NORTH CAROLINA JOURNAL of
LAW & TECHNOLOGY
Volume 27, Issue 3 2026

ARTICLE

THE THIRD-PARTY PRIVACY PROBLEM

David Sella-Villa†

You stand on a city street corner, and a driverless robotaxi crosses the road in front of you. To operate safely, the robotaxi identifies you as a person, tracks your movements, determines your relative location, and stores data about you. What are your privacy interests in these data?

This Article examines the "third-party privacy problem"—a phenomenon where technologies collect personal data from individuals who are neither users nor direct participants in a service. This concept merits further definition and exploration, especially as technologies like artificial intelligence systems process more data from more people. The one-to-one relationship at the heart of most privacy laws fails to capture all the privacy interests of third parties.

This Article explores the third-party privacy problem in the frame of European Union ("EU") law, using data collected by vehicles' externally facing sensors as a case study. The EU's privacy and AI laws are among the most comprehensive in the world. If third parties' privacy interests can be

† Assistant Professor of Law, University of South Carolina Joseph F. Rice School of Law, CIPP/E, FIP. A special thank you to Helen Nissenbaum and Matt Franchi for their deep engagement with the piece and citing to it in their forthcoming work. Many thanks to Derek Black, Adair Boroughs, Irene Calboli, Alessandra Calvi, Jeff Bellin, Jan de Bruyne, César Augusto Fontanillo López, Laura Lane-Steele, Fernanda Nicola, Joseph Seiner, Ned Snow, Peter Swire, Etienne Toussaint, Charlie Trumbull, Bryant Walker Smith, Clint Wallace, and Madalyn Wasilczuk for their generous and thoughtful feedback. I benefitted from the opportunity to present this project at the 2024 Privacy Law Scholars Conference—Europe, the AALS European Law Section New Scholarship in EU Law session, the Democracy Works in Progress Conference and the 2025 Privacy Law Scholars Conference.

recognized and protected in the EU, it indicates that privacy and AI laws can work together to protect third-party data privacy. The Article finds these protections lacking and calls into question the role of privacy and AI law in safeguarding third parties.

Table of Contents

I. Introduction

You stand on a city street corner, and a driverless robotaxi crosses the road in front of you. Looking past the dizzying array of sensors and cameras, you notice that no one is in the vehicle. To operate safely, the robotaxi used artificial intelligence ("AI") to identify that you are a person (rather than a mailbox or a lamppost), track your movements for a short period of time, determined your proximity to the robotaxi, and locate you as being on the sidewalk rather than the street. It then stored some of this information. Later, these data will be used to train future robotaxi fleets. Absent a human occupant, these data likely implicate no driver or passenger privacy interests. But what about you, as a third party: what are your privacy interests in these data?[1]

One might argue that your presence in a public place diminishes your privacy expectations altogether.[2] This might be true if the encounter with the robotaxi (or any other vehicle with externally facing sensors)[3] were akin to the human driver making similar

---

1. Though cognizant that privacy and data protection interests have distinct bases in several legal systems, this Article will use the terms *privacy* and *data protection* interchangeably. *See* Michael Veale, *Some Commonly-Held but Shaky Assumptions About Data, Privacy and Power*, *in* Research Handbook on Competition Law and Data Privacy 3–7 (Maria Ioannidou & Despoina Mantzari eds., 2025) (arguing that in practice, privacy and data protection are "entwined" concepts). Additionally, this Article uses the term "third party" in relation to privacy interests, this Article does not discuss the third-party doctrine found in U.S. Fourth Amendment jurisprudence. *See infra* note 25.
2. Cara Bloom & Josiah Emery, *Privacy Expectations for Human-Autonomous Vehicle Interactions*, 31 IEEE 1647, 1647 (2022).
3. The term "vehicles," as used in this Article, refers exclusively to terrestrial vehicles intended for use on public roadways. This excludes aircraft and watercraft. These include passenger cars, vans, delivery bots, light trucks, heavy trucks, shuttles, and buses—including those used as part of public transportation systems. But conveyances that operate exclusively on closed test tracks and other non-public environments, like Kodiak's automated trucks in use on private property, would not meet this definition of "vehicle." David Taube, *Kodiak, Atlas Energy Solutions Ramp Up Self-Driving Trucks in Texas*, TruckingDive (July 24, 2024), https://www.truckingdive.com/news/atlas-energy-solutions-kodiak-robotics-driverless-frac-sand-deliveries/722066 [https://perma.cc/HY97-BAXE]. "Automated vehicles" refer to said vehicles that have a feature which meets at least Level 0 of the Society of Automotive Engineers standard SAE J3016 for

footnote continued on next page

observations—those that are merely "ephemeral."[4] But the moment data about third parties are used beyond sensing the environment to facilitate immediate safe-driving needs,[5] these data potentially implicates the privacy interests of third parties.[6]

In the European Union ("EU"), which has some of the world's most stringent data protection laws, some scholars have gone so far as to say that "data protection law would normally not apply" to third parties in these circumstances.[7] Third parties may not be identifiable in these data sets and certain data collections from public spaces might

---

driving automation. SOC'Y OF AUTO. ENG'GS, J3016-202104, TAXONOMY AND DEFINITIONS FOR TERMS RELATED TO DRIVING AUTOMATION SYSTEMS FOR ON-ROAD MOTOR VEHICLES 4 (Apr. 2021), https://www.sae.org/standards/content/j3016_202104/ [https://perma.cc/H7TH-TGUU].

4. Matt Franchi et al., *Privacy of Groups in Dense Street Imagery*, *in* ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (FACCT) '25 at 2880 (2025).

5. Bloom & Emery, *supra* note 2, at 1647; Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 915, 945–46 (2017); Livia Aulino et al., *Consideration of Privacy Aspects in the Area of Highly Automated Driving. An Intention Recognition Use Case*, 2 EUR. J. PRIVACY L. & TECHS. 252, 263 (2020); *Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related* Applications, EUR. DATA PROT. BD. 5 (Mar. 9, 2021) [hereinafter EDPB CONNECTED VEHICLES],https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connectenected_vehicles_v2.0_adopted_en.pdf [https://perma.cc/MS3H-G3MQ].

6. *See, e.g.*, Roeland de Bruin, *Autonomous Intelligent Cars on the European Intersection of Liability and Privacy: Regulatory Challenges and the Road Ahead*, 7 EUR. J. RISK REG. 485, 485–86, 495 (2016); Philipp Hacker, *Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things*, 7 INT'L DATA PRIV. L. 266, 268, 273 (2017); *cf.* Jason Koebler, *LAPD Publishes Crime Footage It Got from a Waymo Driverless Car*, 404 MEDIA (Apr 16, 2025, at 15:34 ET), https://www.404media.co/lapd-publishes-crime-footage-it-got-from-a-waymo-driverless-car/ [https://perma.cc/T3Y2-VAJB] (discussing internal policies intended to protect the privacy interests of people observed by Waymo's in response to data requests).

7. Inge Graef & Bart van der Sloot, *Collective Data Harms at the Crossroads of Data Protection and Competition Law: Moving Beyond Individual Empowerment*, 33 EUR. BUS. L. REV. 513, 513–14 (2022) (citing Maša Galič & Raphaël Gellert, *Data Protection Law Beyond Identifiability? Atmospheric Profiles, Nudging and the Stratumseind Living Lab*, 40 COMP. L. & SEC. REV., 2021).

inherently avoid certain privacy protections.[8] More commonly, the literature examining automated vehicle sensor systems notes that while third party privacy is likely an issue, scholars have not assessed the question directly.[9] Professor Philipp Hacker explained that one of the world's most stringent privacy laws, the European Union's General Data Protection Regulation ("GDPR"), provides legal bases, other than consent, for the processing of third party data in the driving context.[10] But this analysis left an important antecedent issue unexamined—do data collected about third parties by vehicles meet the definition of "personal data" under privacy laws?

---

8. *See id.*

9. Hacker, *supra* note 6, at 267–68, 273 ("The collection of data on traffic participants outside of [vehicles] raises intricate questions of the legality of processing their data absent consent. . . . The pressing data protection issues of this type of [vehicle] powered third party surveillance . . . transcend the scope of this article."); Ioannis Krontiris et al., *Autonomous Vehicles: Data Protection and Ethical Considerations*, *in* PROCEEDINGS OF THE CSCS 2020: ACM COMPUTER SCIENCE IN CARS SYMPOSIUM 2 (Dec. 2020), https://orbilu.uni.lu/bitstream/10993/50095/1 [https://perma.cc/AHQ3-KKB5] ("The situation regarding legal protections for pedestrians and other traffic participants against the capture and use of images taken by AVs is—at best—unclear."); Rastislav Funta, *Automated Driving and Data Protection: Some Remarks on Fundamental Rights and Privacy*, 13 KRYTYKA PRAWA [CRITICISM OF THE LAW] 106, 113 (2021); Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1179–80 (2012); *see also* de Bruin, *supra* note 6, at 498 (citation omitted); Franchi et al., *supra* note 4, at 2875 (when discussing their work on dashcams that create dense street imagery, noting "that this work does not address the potential identifiability of individuals"); *cf.* Michael Veale, *Denied by Design? Data Access Rights in Encrypted Infrastructures*, *in* RESEARCH ACCESS TO DIGITAL INFRASTRUCTURE 10–11 (Jef Ausloos & Siddharth P. de Souza eds., 2023) ("The extent to which orchestrating data controllers should be obliged to consider whether the data collected by an individual using their own device could be used to reidentify those around them in the future is unclear."). For brief discussion of this issue in the U.S. context, see Bryant Walker Smith & Matthew T. Wansley, *Regulating Robotaxi*, 99 S. CAL. L. REV. *44–47 (Forthcoming 2026).

10. Hacker, *supra* note 6, at 274–75 ("These [legal bases] . . . present further avenues for companies to defend data processing of . . . other traffic participants if the profiles contribute to . . . traffic security, or . . . to interests of the controller to improve fleet learning and algorithmic precision.").

Most data privacy laws, including those in the EU, only apply protections to "personal data." Generally, they define personal data broadly as "any information relating to an identified or identifiable natural person."[11] When applying this definition, the focus has been on just how identifiable any given third party might be to the entity holding the information in question.[12] Identification of a person's group membership, or other collective classifications, typically has not been enough to meet the definition of "personal data."[13] Data from external sensor systems allow vehicle manufacturers, providers of automated driving systems, regulators, researchers, other market participants, and law enforcement to readily identify groups, but not necessarily individual people.[14] These group classifications facilitate decisions that affect the rights and interests of third parties, and privacy law offers these people little recourse.[15] In short, even without individual identification of third parties, data collected from external sensors on vehicles affects the privacy interests of third parties.

This gap in legal protections has enabled vehicles equipped with extensive external sensors, including automated vehicles, to develop with little social resistance from people observed by said vehicles.[16]

---

11. Regulation 2016/679, art. 4(1), 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), 2016 (O.J. L 119) [hereinafter GDPR]; CAL. CIV. CODE § 1798.140(v)(1) (West 2025).

12. *See infra* Part III.B.

13. *See* Graef & van der Sloot, *supra* note 7, at 518 (citations omitted). This statement, however, rests on assumptions about the state of "identifiability" jurisprudence. For a discussion of this issue, see *infra* Part III.B.

14. *E.g.*, Franchi et al., *supra* note 4, at 2881; Tahiya Chowdhury et al., *Towards Sensing Urban-Scale COVID-19 Policy Compliance in New York City*, *in* BUILDSYS '21: PROCEEDINGS OF THE 8TH ACM INTERNATIONAL CONFERENCE ON SYSTEMS FOR ENERGY-EFFICIENT BUILDINGS, CITIES, AND TRANSPORTATION 353, 353 (2021).

15. *See infra* Part II.C.

16. de Bruin, *supra* note 6, at 488, 499 (citations omitted) (describing the privacy regime as a system for facilitating trade because it "contributes to consumer trust, and therefore acceptance of [vehicles with externally facing sensors]."). People who drive to earn a living, however, have resisted increased automation of vehicles. *See* KAREN LEVY, DATA DRIVEN: TRUCKERS,

footnote continued on next page

External sensor data have been "used to the maximum technologically and legally possible, by the companies developing [automated vehicles]." [17] These developers have, in effect, been able to "leverage[] political economic factors such as . . . favourable legal frameworks . . . [including] data protection."[18] In short, privacy law has not emerged as a means of resisting the proliferation of data collection via vehicles. Data collection about third parties can proceed largely unimpeded, "shift[ing]. . . 'reasonable expectations' of . . . privacy in public spaces."[19] Increasingly, third parties face the impossible choice of either protecting their privacy or "opt[ing] out of public space[s]."[20]

Interestingly, providers of vehicles equipped with externally facing sensors that seek to preserve third party privacy interests face a comparable dilemma. Designing and deploying regulatorily-compliant and safe vehicles requires collecting, processing, and sharing vast amounts of data.[21] Privacy law defers to regulatory and safety needs, offering almost no limitations on the collection, retention, or further sharing of data about third parties.[22] Removing relevant characteristics about third parties from sensor data undermines the efficacy of vehicle

---

Technology, and the New Workplace Surveillance (2022); Joseph Seiner & Jeffrey Hirsch, *A Modern Union for the Modern Economy*, 86 Fordham L. Rev. 1727 *passim* (2018).

17. Hacker, *supra* note 6, at 268 (citing A. Cole, *How Artificial Intelligence Will Make the IoT*, IT Business Edge Blog (Mar. 15, 2017), http://www.itbusinessedge.com/blogs/infrastructure/how-artificial-intelligence-will-make-the-iot.html [https://perma.cc/4X33-ZR6F].

18. Jennifer Cobbe et al., *Understanding Accountability in Algorithmic Supply Chains*, *in* FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency 1186, 1189 (2023); *accord.* Julie Cohen, Between Truth and Power: The Legal Construction of Information Capitalism (2019).

19. Franchi et al., *supra* note 4, at 2883 (citing Julia Lane et al., Privacy, Big Data, and the Public Good: Frameworks for Engagement (2014)).

20. *Id.* at 10 (citing Ben Green, The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future (2019)).

21. *See infra* Part IV.B.

22. *See infra* Part IV.C.; *cf.* Jennifer Cobbe & Jatinder Singh, Data Protection Doesn't Work: Oversight Failure in Data Processing Figurations 17 (June 14, 2023) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4437133 [https://perma.cc/B84Q-PQCV].

safety systems.[23] Absent some form of legal protection for third parties, a vehicle manufacturer who seeks to protect third-party privacy interests must avoid collecting information in the first place. Vehicle providers must decide whether to develop compliant, safe vehicles that rely on external sensor data, or to protect third-party privacy interests. Third party privacy protection, sits in direct conflict with technological progress.[24]

Vehicles with externally facing sensors highlight a broader phenomenon at the intersection of technological capabilities, legal structures, and third-party privacy interests. This Article calls this phenomenon the "third-party privacy problem."[25] Another example arises in the hiring context. Rules governing anti-discrimination testing of AI tools potentially require the processing of data from non-consenting, non-applicants (third parties).[26] Neither the privacy laws nor the burgeoning AI laws offer these third parties much recourse.[27] A further example potentially arises from law firm use of AI systems. AI systems that process all the firm's data may run afoul of the data protection interests of former clients (who are third parties in these circumstances), potentially violating the lawyers' rules of professional conduct.[28]

---

23. *E.g.*, Franchi et al., *supra* note 4, at 2882.

24. *Cf.* Salomé Viljoen, *An Argument for Positive Political Theories of Data Governance*, 6 GEO. L. TECH. REV. 464, 468 (2022) ("Instead of developing legal responses primarily equipped to abolish or unmake data relations, positive legal theories of data governance aim to develop legal responses to equalize and democratize the data relations that will constitute digital social life.").

25. Commentators generously suggested alternative names for this phenomenon, including "bystander privacy" or "collateral privacy." While these names are evocative, they suggest an accidental collection of third-party data. As explained in Part II, *infra*, some combination of technological capabilities and legal standards make collection and further processing of third-party data a necessary result. Accordingly, I have chosen a label that, hopefully, better captures some degree of intentionality inherent in these techno-legal systems. *See infra* Part V.B.

26. *See* Colorado Artificial Intelligence (AI) Act, COLO. REV. STAT. ANN. §§ 6-1-1701(1)(a), 1703(2)(a) & 1703(4)(a)(III) (West 2025).

27. *See* David Sella-Villa, *Privacy and AI Law in Conflict* (draft on file with author).

28. *See* David Sella-Villa, *Disloyalty by AI* (draft on file with author).

As AI tools proliferate, this phenomenon will likely arise in other contexts.[29] Will AI note takers draw new attention to the intersection of disability accommodations and the privacy interests of fellow students and employees?[30] Will wearable devices recognize patterns in other people's behavior as part of improving the user's service experience?[31] If the third-party privacy problem can be defined carefully, it is possible to assess the efficacy of potential solutions.[32] Regarding data from vehicle's externally facing safety systems, the EU's Artificial Intelligence Act ("AI Act") offers one such intervention.

Enacted in 2024, the AI Act marks an inflection point in third-party privacy.[33] Under the AI Act, vehicle safety systems and their external sensors qualify as "high-risk AIs."[34] As such, the AI Act potentially subjects them to data governance requirements beyond the privacy protections enshrined in the GDPR.[35] Unlike GDPR's focus on

---

29. *E.g.*, Gabriela Gura et al., *Privacy & XR*, *in* GOVERNING XR 46, 48 (Michael Karanicolas et al. eds., 2024) (discussing potential privacy issues presented by extended reality ("XR") systems, including "bystander effects").

30. *See, e.g.*, Peter W. Cardon et al., *Recorded Business Meetings and AI Algorithmic Tools: Negotiating Privacy Concerns, Psychological Safety, and Control*, 60 INT'L J. BUS. COMMC'N 1095, 1095 (2021).

31. *See, e.g.*, Zahra Takhshid, *Wearable AI, Bystander Notice, and the Question of Privacy Frictions*, 104 B.U. L. REV. 1087 (2024).

32. Ryan Calo, *The Scale and the Reactor*, *in* LAW AND TECHNOLOGY: A METHODICAL APPROACH 55 (2025) ("We are ready—nay, delighted—to describe the levers of power in detail and to proscribe precise solutions to the problems we identify. Legal academics expect to say what society should do and how."). *See generally* JULIE COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY (2012) (discussing the pragmatism of the U.S. legal tradition).

33. Regulation 2024/1689 of the European Parliament and Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations, 2024 O.J. L 2024/1689 [hereinafter EU AI Act].

34. *Id.* art. 6(1), Annex I Part B. For a fuller explanation of the different classifications of AI system under the AI Act and their respective data governance controls see *infra* Part III.A. Part III describes more precisely which safety systems in vehicles fall under the EU AI Act.

35. EU AI Act, *supra* note 33, art. 2(7), recitals 10, 27, 67, 69, 70, 122; *see infra* Part III.B. The advent of big data has pulled much privacy scholarship towards discussions of related concepts like "data governance." *See* María P. Ángel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*,

footnote continued on next page

data subjects' individual interests in data privacy,[36] the AI Act aims to account for the interests of a wider range of parties.[37] Providers of high-risk AIs must identify and analyze "the known and the reasonably foreseeable risks that . . . high-risk AI[s] can pose to . . . fundamental rights . . . ."[38] Under the EU Charter of Fundamental Rights, "*everyone*" enjoys "the right to respect for his or her private and family life, home and communications," and "the right to the protection of personal data concerning him or her."[39] Accordingly, providers of vehicle safety systems should consider the privacy and data protection of all people potentially impacted by their high-risk AI systems. If the AI Act proves unequal to the task of protecting third-party privacy interests, then practical and theoretical consequences follow. Practically, third parties in jurisdictions with less robust AI regulations enjoy even fewer safeguards. Theoretically, the entire enterprise of protecting privacy through the exercise of individual rights may be incapable of addressing the third-party consequences of AI's rapid proliferation.

So, does the AI Act do enough to address the third-party privacy problem? This Article seeks to address part of that question. Part II conceptualizes the third-party privacy problem as a particular

---

124 COLUM. L. REV. 507 (2024). This shift is not without its critiques. *See id.*; *see also* Jeffrey Bellin, *Pure Privacy*, 116 NW. U. L. REV. 463 (2021). This Article seeks to present the third-party privacy problem as a concept that may require broader interventions, like data governance, to address the privacy interests of third parties. *See infra* Parts III & V. As such, the concept of third-party privacy problems offers a path towards reconciliation between the entrenched principles in privacy laws and the more expansive theoretical developments that shape possible reforms. *Compare* Margot E. Kaminski, *The Case for Data Privacy Rights (or, Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385 (2022) (arguing that data privacy rights can play an important role), *with* Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975 (2023) (critiquing the limitations of data privacy rights).

36. *E.g.*, Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 425 (2018); Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 38 (2021); Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 578 (2021).

37. *See infra* Part III.

38. EU AI Act, *supra* note 33, art. 9(2)(a); *acorrd. id.* recital 65.

39. Charter of Fundamental Rights of the European Union arts. 7, 8, 2000 O.J. C364/10 (emphasis added) [hereinafter Charter of Rights].

interplay between law and technology. This distinguishes the third-party privacy problem from other theories of collective or group privacy, sometimes referred to as inferential privacy. Part III summarizes the AI Act and explains how its data governance provisions go beyond the requirements of privacy law. In addition to obligations for providers of AI systems, the AI Act also calls for policymakers to incorporate data governance practices into existing regulatory systems—a process of adopting delegated acts. This Article argues that the AI Act's combination of data governance and adoption of delegated acts establishes the high-water mark of possible solutions to the third-party privacy problem.

Part IV offers a case study of vehicles' externally facing sensors and examines the efficacy of the AI Act's data governance tools. It describes the vehicle technologies that most directly impact third-party privacy. Part V evaluates the AI Act's data governance framework for its ability to address the privacy interests of third parties. This Part offers an account of third-party privacy that is missing from the literature on increased vehicle automation. The data governance requirements of the AI Act, however, create a privacy rights cliff for third parties. If the AI Act can address the third-party privacy problem, it will be through the delegated acts.

II. Defining the Third-Party Privacy Problem

Three sections comprise this Part of the Article. The first Section explains the key concepts necessary for defining the third-party privacy problem. Applying those concepts, the second Section defines the third-party privacy problem and highlights its key features. The last Section situates the third-party privacy problem in relation to other conceptions of privacy harms.

A. Key Concepts

The third-party privacy problem emerges from the interaction of a series of interrelated concepts. The names of these concepts may correspond to common terms in privacy law. But the concepts explained here, and their homonyms in EU privacy law, do not align perfectly. The first key term, *personal data*, is a case in point.

The concept of personal data, as used in this Article, is *information processed from and about an identified or identifiable person*. Processing retains its rangy definition—any action undertaken with data—used in most privacy laws.[40] But in other ways, this conception of personal data is both narrower and broader than most legal interpretations of the term "personal data."[41] By focusing on data processed both *from and about* a person, the definition narrows the scope of data processing practices to those where the person interacts with a given data-collection or data-generation technology. "Identifiability," as used here, does not limit consideration to the data processing practices of the party that collects or generates the data. Rather, it considers how all parties that might receive information from and about a person can use it to identify the person in question. This expands the scope of identifiability beyond the moment of data collection to any moment of identification at a later time.[42]

The party with legal agency and technological capabilities to process the personal data is the data *controller*.[43] The natural person in question is a *data subject*. Controllers process data from three categories of data subjects: first parties, second parties, and third parties. A *first party* has a direct relationship with the controller in the present moment. Among all the possible data subjects, the first party has the most recognized priority of interests in the exercise of some control over the data processing either directly or by consenting to the controller's data processing arrangement. Ideally, the first party enjoys the broadest application of rights under EU privacy law. A *second party* does not have a direct relationship with the controller but has a relationship with the first party in the present moment, independent

40. *E.g.*, GDPR, *supra* note 11, art. 4(2); CAL. CIV. CODE § 1798.140(z) (West 2025).

41. Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 406 n.226 (2022) (deviating from the definition of personal data proffered in privacy laws in her influential piece); *see also infra* Part III.B (incorporating language from the AI Act into the interpretation of personal data under GDPR).

42. *See infra* Parts III.B, V.B.1.b, V.B.2.b & V.C

43. *E.g.*, GDPR, *supra* note 11, art. 4(7) (using the term "controller"); CAL. CIV. CODE § 1798.100(a) (West 2025) (referring to "[a] business that *controls* the collection of a consumer's personal information") (emphasis added).

of the data processing activity.[44] An example might include the passenger in a vehicle.[45] The driver, as a first party, may engage with any number of controllers as part of the driving experience. The passenger may have their personal data processed, such as the determination of their geospatial location, because of the driver's activities. But the passenger may advocate for their privacy interests via their relationship with the driver, but their data privacy interests will be subordinate to those of the driver.[46]

A *third party*, at the present moment, may have no ability to direct the data processing activity, either via a relationship with the first

44. "[P]ersonal information" combines first parties and second parties when they are members of the same "household." CAL. CIV. CODE § 1798.140(v)(1) (West 2025) (stating "information that . . . could reasonably be linked . . . with a particular consumer *or household*") (emphasis added). The definition of "second party" used here differs from the meaning of the term in other data privacy-related fields. In the Fourth Amendment context, *see* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 164 (2008) ("[T]hese are cases in which the ISP, as recipient of an intended communication, acts as a 'second party' rather than a third party to a communication between two others."). In the adtech context, see Paloma Fuentes Santos et al., *Adapting Digital Marketing Strategies for a Cookieless Future: Challenges and Opportunities*, 30 FIRST MONDAY, no. 6, at 9 (June 2, 2025) ("Second-party data are obtained through legally explicit and consented partnership agreements.").

45. In this example, this is not a vehicle for hire or a commercial vehicle.

46. Though there are many nuances and unresolved issues in the application of privacy law in the context of this relationship, this Article does not aim to address those issues directly. At least in the vehicle context, some studies have made inroads on some of these issues. *E.g.*, *Study on the Social Dimension of the Future EU Transport System Regarding Users and Passengers*, EUR. COMM'N, (Aug. 2022) [hereinafter COMM'N STUDY], https://op.europa.eu/en/publication-detail/-/publication/a6cf3c66-34a9-11ed-8b77-01aa75ed71a1 [https://perma.cc/6NM5-YWSD]; Funta, *supra* note 9, at 113. *See generally* Claire Levallois-Barth & Jonathan Keller, *Analyse d'Impact Relative à la Protection des Données: Le Cas des Voitures Connectées* [Data Protection Impact Assessment: The Case of Connected Cars], INSTITUT MINES-TÉLÉCOM (Nov. 2021), https://cvpip.wp.imt.fr/files/2021/11/FINALRapportRechercheC3S_AIPD_VoituresConnectees_nov2021.pdf [https://perma.cc/Q2RA-LSVX] (examining passengers' data protection rights in connected taxis).

party or the controller.[47] Or, the third party may have direct relationship with the first party or the controller, but their rights are subordinate and therefore cannot direct the data processing activity to reflect their privacy interests.[48] Yet, a third party's personal data is processed incident to the present relationship between the first party and the controller. Further, once either a second party or a third party establishes a direct relationship with the controller that allows them priority of influence in the data processing relationship, they become a first party.[49] The processing of third-party data occurs because of a combination of *technological capabilities* and *legal standards*.[50]

---

47. Save, of course, general duties to all people, such as might be established under a tort regime or potentially, a comprehensive privacy rights regime. *See infra* Part V.C. Additionally, though the construction here bears similarities to the rights and interests of third parties under contract law, this Article uses the term in a different way.

48. This scenario arises in other contexts.

49. *See, e.g.*, CAL. CIV. CODE §§ 1798.100(b) & 1798.140(ai)(1) (West 2025). This reclassification of third parties as first parties is what distinguishes aerial drones, video doorbells, and surveillance cameras from other technologies that present the third-party privacy problem. In most instances, aerial drones and surveillance cameras operate with the intent of observing the people who come within their field of vision. Accordingly, the observed people are first parties under this classification system. Though their rights may be more limited, they are nonetheless recognized under privacy law. *See* David Sella-Villa, *Drones and Data: A Limited Impact on Privacy*, 55 U. RICH. L. REV. 991 (2021). Externally facing cameras in vehicles, like dashcams, that do not inform vehicle safety systems also collect first party data. *See* Tim Gruchmann & Amer Jazairy, *Big Brother Is Watching You: Examining Truck Drivers' Acceptance of Road Facing Dashcams*, 111 TRANSP. RSCH. PT. F: PSYCH. & BEHAV. 316 (2025), https://www.sciencedirect.com/science/article/pii/S136984782500107X [https://perma.cc/RD2R-8F64].

50. The concepts behind these terms draw from an extensive literature studying the interaction between technological designs, organizational practices, and legal requirements. *E.g.*, Mireille Hildebrandt, *Law as an Affordance: The Devil Is in the Vanishing Point(s)*, 4 CRITICAL ANALYSIS L. 116 (2017); COHEN, *supra* note 18; Sebastian Benthall et al., *Contextual Integrity Through the Lens of Computer Science*, 2 FOUNDS. & TRENDS IN PRIV. & SEC. 1 (2017); *see also Programmable Infrastructures Project*, TUDELFT https://www.tudelft.nl/en/tpm/our-faculty/departments/multi-actor-systems/research/projects/programable-infrastructures-project [https://perma.cc/H7GR-C4E2] (applying related concepts to examinations of specific technologies). It appears that scholars in this space

footnote continued on next page

Technological capabilities encompass engineering design features *and* organizational practices[51] that enable the processing of data from and about third parties.[52] For example, Google developed the ability to train a facial recognition system from photos on the internet, but elected not to do so.[53] Under this definition, therefore, Google did not have the technological capabilities that Clearview AI deploys in its facial recognition systems.[54]

Legal standards are legally enforceable prescriptions or proscriptions for certain data processing practices.[55] These standards can take many forms, such as statutes, regulations, contract provisions, or defenses under certain liability regimes.[56] While legal standards and technological capabilities are causally entwined,[57] these terms focus on

---

have not generated a standardized vocabulary around these concepts. *Compare* Laurence Diver, *Law as a User: Design, Affordance, and the Technological Mediation of Norms*, 15 SCRIPTED 4 (2018) (discussing the idea of "affordances"), *with* Cobbe & Singh, *supra* note 22 (discussing the idea of "figurations"). Accordingly, the terms used in this Article are meant to reference this literature generally without adopting any particular nomenclature.

51. *E.g.*, Seda Gürses & Joris van Hoboken, *Privacy After the Agile Turn*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 579 (Evan Selinger et al. eds., 2017); Michael Veale, *Rights for Those Who Unwillingly, Unknowingly and Unidentifiably Compute!*, CTR. OPEN SCI. (Aug. 1, 2023), https://doi.org/10.31235/osf.io/4ugxd [https://perma.cc/EN34-L27Q].

52. Cobbe et al., *supra* note 18, at 1189 (citations omitted) "[technological capabilities] are not objective properties of technologies, but depend on context and perspective." In this Article, accordingly, processing data from and about third parties provides the necessary "context and perspective."

53. KASHMIR HILL, YOUR FACE BELONGS TO US: A SECRETIVE STARTUP'S QUEST TO END PRIVACY AS WE KNOW IT 99–110 (2023).

54. *Id.* at ix–x, 94.

55. *E.g.*, Ryan Calo, *Can Americans Resist Surveillance?*, 83 U. CHI. L. REV. 23 (2016); Agathe Balayn & Seda Gürses, *Misguided: AI Regulation Needs a Shift in Focus*, 13 INTERNET POL'Y REV. (SPECIAL ISSUE) 3 (Sep. 30, 2024), https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796 [https://perma.cc/X9GR-TEBU].

56. *See infra* Part IV.B.

57. *E.g.*, Blagovesta Kostova, Seda Gürses & Carmela Troncoso, *Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy by Design*, CORNELL U. ARXIV (July 16, 2020, at 15:29 ET), https://arxiv.org/abs/2007.08613 [https://perma.cc/5E5J-VYFW]; Alessandra

footnote continued on next page

different sets of actors. Technical capabilities tend to address the choices that controllers make, even when constrained by legal standards.[58] Legal standards look to outputs from policymakers—legislative bodies, regulators, courts, standard setting bodies—even as these actors develop responses to technical capabilities.[59]

Lastly, the term *privacy problem*, though inclusive of, captures more than the concepts of privacy harm or violations of a legal standard.[60] This is because privacy rights or interests are often subordinate to other rights.[61] Accordingly, in certain circumstances, preserving someone's life may require impinging on their privacy interests.[62]

Calvi et al., *The Unfair Side of Privacy Enhancing Technologies: Addressing the Trade-Offs Between PETs and Fairness*, 2024 ASS'N COMPUTING MACH. CONF. ON FAIRNESS, ACCOUNTABILITY, & TRANSPARENCY (FACCT) 2047 (2024), https://doi.org/10.1145/3630106.3659024 [https://perma.cc/XZ8V-7C69 (staff-uploaded)]

58. de Bruin, *supra* note 6, at 488 ("In a qualitative way, it is *inter alia* observed that the allocation of risks concerning (the results of) innovation through liability legislation can provide significant incentives or disincentives for innovation depending on the way these are regulated."); *e.g.*, Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Humans in the Loop*, 76 VAND. L. REV. 429, 437 (2023) ("Tort rules, though not intended to affect the design or operation of … [certain vehicle safety systems], profoundly shape . . . [their] dynamics.").

59. *See generally* Gregory C. Shaffer & Mark A. Pollack, *Hard vs. Soft Law: Alternatives, Complements and Antagonists in International Governance*, 94 MINN. L. REV. 707 (2010) (discussing multiple sources of legal standards with varying degrees of enforceability); Margot Kaminski, *Regulating the Risks of AI*, 103 B.U. L. REV. 1347 (2023) (discussing various policy responses to AI's changing capabilities).

60. *See generally* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) (describing privacy harms legally recognized under U.S. law); Bert-Jaap Koops et al., *A Typology of Privacy*, 38 U. PA. J. INT'L L. 483 (2017) (enumerating privacy interests rooted in several legal traditions).

61. *See* Paul de Hert & Serge Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *in* PRIVACY AND THE CRIMINAL LAW 74–76 (Erik Claes et al. eds., 2006) ("Actually, not a single aspect of privacy takes absolute precedence over other rights and interests.").

62. *See infra* Part V.A (discussing kinetic safety).

Though justified, that impingement could still be considered a privacy problem.[63]

B. The Third-Party Privacy Problem

The third-party privacy problem arises from two conditions:

> 1) a controller has the technological capabilities to collect and retain third-party personal data, and
>
> 2) legal standards at least incentivize, if not require, the controller to further process third-party personal data.

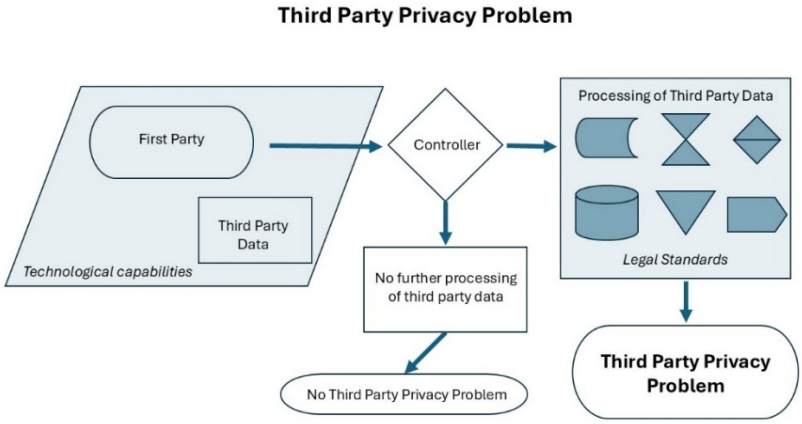

Figure 1

The third-party privacy problem emerges from a particular structure of data flows among the controller, the first party, and the third party. This structure reflects a specific "relational" quality of data described by Professor Salomé Viljoen. According to Professor Viljoen, data structure social relations along two axes.[64] In the context of the third-party privacy problem, a vertical relationship exists between the first party and the data controller.[65] A horizontal

63. *Accord Problem*, OXFORD ENGLISH DICTIONARY (3d ed. 2007), https://www.oed.com/dictionary/problem_n?tab=meaning_and_use#28477799 [https://perma.cc/8GEG-75LF] ("3.a. A difficult or demanding question; (now, more usually) a matter or situation regarded as unwelcome, harmful, or wrong and needing to be overcome; a difficulty.").

64. Viljoen, *supra* note 36, at 607.

65. *Id.*

relationship exists between and among data subjects, such as between the first and third parties. Moreover, "[t]his horizontal relation, or data relation, reflects the notion that data collected from one person can almost never be said to be truly about one person."[66]

Technological capabilities organize these relationships. Externally facing sensors that support vehicle safety systems illustrate that the controller processes data along both axes of relation simultaneously. Data processing in the vertical relationship (between the human driver and the vehicle safety systems) is derived from data about horizontal relationships (between the vehicle the human driver occupies and all other data subjects on or along the roadway). In other words, the technology structures the relationship among the parties such that the controller can only process data in service of the first party by processing third-party data.[67]

These data processing activities also stem from a legal foundation. The technological capabilities of the third-party problem challenge the human-centric paradigm, that a human is watching another human, at the heart of privacy laws.[68] When a first party hails a robocab, submits a resume to an applicant management system, or uploads documents to a law firm's web portal, they initiate a series of data processing practices that were once conducted primarily by humans. The laws that enable these data-driven transactions also share the same assumption that a human is watching another human.[69] As Professor Yafit Lev-Aretz explains, this paradigm of privacy law brings observation and judgment together.[70] Accordingly, the law says that if

66. Rebecca Hamilton, *Seventh Annual Detlev F. Vagts Roundtable on Transnational Law: Transnational Regulation of the Platform Economy*, 116 AM. SOC. INT. L. PROC. 122 (2022) [hereinafter *Detlev Vagts Roundtable*], (quoting Prof. Viljoen).

67. This is maybe even more true when the first party fails to be in spatial proximity to the third party. This occurs in the scenario described in the introduction—the robotaxi has no occupants. *See* Bloom & Emery, *supra* note 2, at 1647 (describing "many-to-many robotic surveillance, exemplified by robotic fleets of autonomous taxis or delivery drones where many robots collect data on many different people").

68. Yafit Lev-Aretz, *"Nobody Is Watching Me": Towards Human-Centric Privacy and Humanless Information Protection*, 26 VA. J.L. & TECH., 1, 2 (2022).

69. *Id.*

70. *Id.* at 4.

you allow observation, you allow judgment.[71] In these examples, a human controller's observations of third parties resulted in either fleeting judgments or the controller treated judgments of third parties as they might treat judgments of first parties.[72] For example, a human taxi driver quickly notes that a pedestrian is on the sidewalk. If no incident occurs, the observation and judgment are fleeting and unremarkable. If the pedestrian and another vehicle collide, that human taxi driver may now be a witness who must recall and recount the incident and offer insights as to who might have been at fault.

Now, *humanless* forms are watching.[73] Consistent with applicable legal standards, those humanless forms are also at least recording their observations.[74] Humanless machine observation still creates observation, but delays judgment.[75] This speaks to the legal dimension of the third-party privacy problem. Third parties have no opportunity to affect the initial observation—the collection of data from and about them. And the law enables later judgments.

C. *The Third-Party Privacy Problem & Other Conceptions of Privacy Harms*

In efforts to critique and improve privacy law, scholars have described and categorized privacy harms.[76] Harms arise from a

---

71. *Id.* at 4-5.

72. Interestingly, differential privacy, a data science privacy-preserving technique that injects statistical "noise" into shared data sets, when combined with a "fleeting" time domain, may also make future judgments less notable. *See* Sujin Cai et al., *A Trajectory Released Scheme for the Internet of Vehicles Based on Differential Privacy*, 23 IEEE TRANSACTIONS ON INTELLIGENT TRANSP. SYS. 16534, 16537 (Sep. 2022) ("Unfortunately, the time dimension introduction will make the data sparser, which is hard to withstand the injected noise, decreasing the worth of the released data.").

73. Lev-Aretz, *supra* note 68, at 2 ("Technology, however, has created a new form of observation - one that is *humanless*.") (emphasis in the original).

74. *See infra* Part V.B.

75. *See* Lev-Aretz, *supra* note 68, at 6–10.

76. This body of scholarship is too long to summarize here. For examples of notable contributions on individual privacy harms, see Citron & Solove, *supra* note 60; Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J.1039 (2018). For examples of notable contributions on societal privacy harms see Viljoen, *supra* note 36; Jack M. Balkin, *Free Speech in the*

footnote continued on next page

"thwarting of an interest."[77] Though important nuances exist within the field, Professor Nathalie Smuha offers an overview that distinguishes among the interests of an individual, a collective, and a society.[78] Individual privacy interests arise in a variety of contexts.[79] Some privacy laws are of general applicability.[80] Some privacy laws are sectoral.[81] Some laws address privacy issues incident to circumstances that are generally not considered "private," like court proceedings.[82] Privacy laws generally attempt to offer protections for those individual interests while balancing other relevant considerations.[83] The technological mechanisms that enable individual privacy harms also injure the interests of society as a whole.[84] Mass impingement of

Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 U.C. DAVIS L. REV. 1149 (2018); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1997). For a discussion of collective privacy harms, see *infra* notes 88–96 and accompanying text.

77. Nathanlie A. Smuha, *Beyond the Individual: Governing AI's Societal Harm*, 10 INTERNET POL'Y REV. 1, 4 (2021) (citing 1 JOEL FEINBERG, THE MORAL LIMITS OF THE CRIMINAL LAW—HARM TO OTHERS ch. 1 (1987)), https://policyreview.info/articles/analysis/beyond-individual-governing-ais-societal-harm [https://perma.cc/C75W-27XX].

78. *Id.* at 5.

79. The contextual scope of privacy laws reflects the commonality of those privacy interests. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009) (explaining the theory of contextual integrity).

80. *See* GDPR, *supra* note 10.

81. *E.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.); Currency and Foreign Transactions Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-1959 and 31 U.S.C. §§ 5311-5332); Fair Credit Reporting Act, Pub. L. No. 91-508, tit. VI, 84 Stat. 1114, 1127 (1970) (codified as amended at 15 U.S.C. §§ 1681–1681x).

82. *See generally* Lior Jacob Strahilevitz, *Pseudonymous Litigation*, 77 U. CHI. L. REV. 1239 (2010) (discussing court rules that protect privacy during litigation).

83. "Actually, not a single aspect of privacy takes absolute precedence over other rights and interests." De Hert & Gutwirth, *supra* note 61, at 74.

84. Viljoen, *supra* note 36.

individual privacy interests frustrates societal attempts at realizing common objectives, such as equality, democracy, and the rule of law.[85]

Collective harms recognize the thwarting of defined interests common to groups, potentially smaller in size than society as a whole.[86] Professors Inge Graef and Bart van der Sloot use the term *collective data harms* to refer to "harms to the interests of a group of individuals resulting from the collection or use of data having effects beyond the level of the individual and outside the individual's control."[87]

The third-party privacy problem shares features with individual privacy harms and collective privacy harms, but is distinct from both.[88] The remainder of this Section describes the concept of collective privacy harms more fully, identifies the distinctive features of the third-party privacy problem, and highlights areas of conceptual overlap.

Scholarship on collective privacy[89] has revealed two interrelated concepts. One idea recognizes that collectives have common privacy interests beyond those of individual members that may need to be protected from outside interference.[90] Another version of collective privacy focuses on "'deindividualization of the person,' where judgments about individuals are based on group characteristics rather

---

85. *E.g.*, Smuha, *supra* note 78, at 6–12; Viljoen, *supra* note 36.

86. *E.g.*, Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985 (2022).

87. Graef & van der Sloot, *supra* note 7, at 514 (emphasis added).

88. David Sella-Villa, *Towards a Political Economy of Third Party Privacy* (forthcoming) (on file with author) [hereinafter Sella-Villa, Political Economy of Third Party Privacy] (exploring the societal harms of the third-party privacy problem).

89. Others refer to this concept as "group," "categorical," or "relational" privacy. *E.g.*, GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES (Linnet Taylor et al. eds., 2017) [hereinafter GROUP PRIVACY]; Anton Vedder, *KDD: The Challenge to Individualism*, 4 ETHICS & INFO. TECH. 275, 278 (Dec. 1999) (referring to "collective privacy"); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EURO. DATA PROT. L. REV. 492, 494 n.9 (2020). The use of the term "collective privacy" in this Article simply borrows from Professor Smuha's framing. Smuha, *supra* note 78, at 5.

90. *See* GROUP PRIVACY, *supra* note 89; Michele Loi & Markus Christen, *Two Concepts of Group Privacy*, 33 PHIL. & TECH. 207, 210–18 (2020).

than individual merits."[91] Modern data technologies have facilitated the explosion of the latter collective privacy phenomenon because it enables inferences or clustering that reveal features shared by individuals, but individuals have no control over the creation or use of those judgments.[92] Many scholars refer to this aspect of collective privacy harms as "inferential privacy."[93]

Inferential privacy shares structural features with the third-party privacy problem. Using the language of the third-party privacy problem, inferential privacy results from the processing of first party data (and potentially second party data) to reveal information about third parties.[94] Inferential privacy corresponds to the horizontal data relations described by Professor Viljoen.[95] Further, Professor Alicia Solow-Niederman conceives of inferential privacy as a triangle.[96] Using the language of the third-party privacy problem, the corners of Professor Solow-Niederman's triangle include the first party, the

91. Franchi et al., *supra* note 4, at 2879 (quoting Vedder, *supra* note 89).

92. A capacious body of literature explores these concepts. For an analysis of modern data technologies and how they have facilitated the collective privacy phenomenon, see GROUP PRIVACY, *supra* note 89; Mireille Hildebrandt, *Defining Profiling: A New Type of Knowledge?*, *in* PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINARY PERSPECTIVES 17, 29–30 (Mireille Hildebrandt & Serge Gutwirth eds., 2008); Richards & Hartzog, *supra* note 89, at 494 n.9; JULIE E. COHEN, *How (Not) to Write a Privacy Law*, COLUM. UNIV. KNIGHT FIRST AMEND. INST. 4 (2020) https://s3.amazonaws.com/kfai-documents/documents/306f33954a/3.23.2021-Cohen.pdf [https://perma.cc/C2N4-8MHL] (critiquing privacy law's reliance on "[a]tomistic, post hoc assertions of individual control rights" that "cannot meaningfully discipline networked processes that operate at scale").

93. *E.g.*, Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 692 n.83 (2016); Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555, 577 n.81 (2020); Tiffany C. Li, *Algorithmic Destruction*, 75 SMU L. REV. 479, 492–93 (2022); Maria Lilla Montagnani & Mark Verstraete, *What Makes Data Personal?*, 56 U.C. DAVIS L. REV. 1165, 1221 (2023) (citing Joe O'Callaghan, *Inferential Privacy and Artificial Intelligence - A New Frontier?*, 11 J.L. & ECON. REGUL. 72, 72 (2018)). *But see* Mark Hanin, *Privacy Rights Forfeiture*, 22 J. ETHICS & SOC. PHIL. 239, 240 (2022) (using the term "inferential privacy" to refer to an individual privacy right).

94. *See* Figure 2.

95. Viljoen, supra note 36, at 607–13.

96. Solow-Niederman, *supra* note 41, at 367, 400, 406, 410–11.

controller, and the party conducting further processing of first-party data.

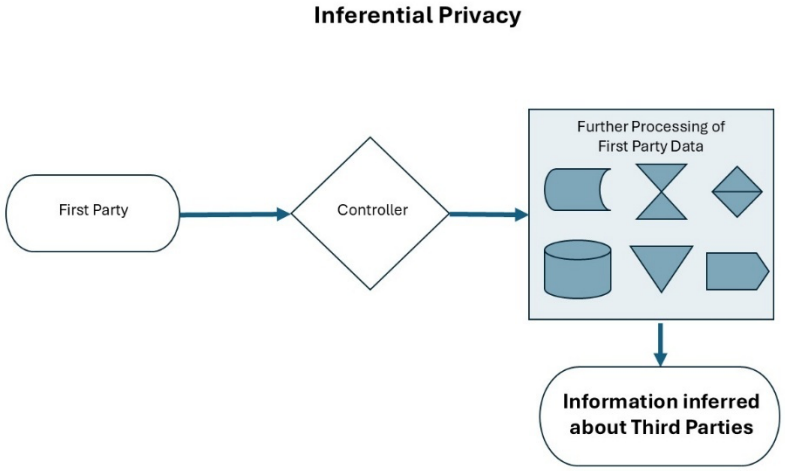

Figure 2

The third-party privacy problem differs from inferential privacy on a structural level in that the initial processing includes personal data from third parties. With inferential privacy, however, third-party personal data only emerges after first-party data are processed. Therefore, the third-party privacy problem effectively includes at least one extra dimension of data processing.[97]

---

97. At the University of Richmond Journal of Law and Technology 31st Annual Symposium on February 28, 2025, on the panel entitled *Constitutional Concerns in the Tech Era*, Professor Margaret Hu expanded on the concept of the triangle in inferential privacy to include a fourth party—technology. She conceptualized the relationships as a square. Margaret Hu, Prof. at Wm. & Mary Sch. of L., Address at the 31st Annual University of Richmond Journal of Law and Technology Symposium: Balancing Innovation and Oversight (Feb. 28, 2025). *Cf.* Margaret Hu et al., *National Security and Federalizing Data Privacy Infrastructure for AI Governance*, 92 FORDHAM L. REV. 1829 (2024) (discussing each of these elements but not describing them as a square). The third-party privacy problem includes all the same elements as Professor Hu's square but starts with third party data as a sufficient condition of the initial data processing. Accordingly, this more dynamic relationship is best described by the shape called a "hypercube" or a "tesseract." L. Sue Baugh, *Tesseract*, ENCYCLOPEDIA BRITTANICA (Dec 23, 2024), https://www.britannica.com/science/tesseract [https://perma.cc/97ME-

footnote continued on next page

Controller choice also serves to distinguish inferential privacy and the third-party privacy problem. Inferential privacy tends to assume that controllers choose to process data to gain insights into third parties. For example, Professor Kirsten Martin explains that "[d]igital platforms have become imaginative in how to collect and create new types of data, as well as how to use, share, and exploit consumer data in facilitating transactions."[98] It is difficult to realize inferential privacy harms without these "new types of data."[99] Later processing is a sufficient condition of inferential privacy. Accordingly, inferential privacy harms stem from controllers' design and data processing choices.

The third-party privacy problem challenges the notion of controller choice as the main reason that data are being collected from and about third parties.[100] Importantly, legal standards drive both

---

SB9Q]. For those familiar with the tesseract in Marvel Comics, that object contains the Space Stone which allows its holder to collapse the distances of space through portals and wormholes. *Space Stone*, MARVEL CINEMATIC UNIVERSE WIKI, https://marvelcinematicuniverse.fandom.com/wiki/Space_Stone#Capabilities [https://perma.cc/5KVN-CVRR]. Though the technologies that present the third-party privacy problem do not create portals through spacetime, per se, these technologies and the legal standards guiding their use can be understood to collapse the distinction between first party privacy and inferential privacy by linking initial data collection to later processing.

98. Kirsten Martin, *Platforms, Privacy, and the Honeypot Problem*, 37 HARV. J.L. & TECH. 1087, 1089–90 (2023).

99. *Id.* at 1090; *see* COHEN, *supra* note 18.

100. An episode from Kristina Batistič's study of a smart parking system illustrates both the technological design and later processing choices that the city of Frederiksberg, Denmark exercised:

> [T]he discussion on treatment of non-hit scans, scans of licence plates that are not needed for the purpose they were scanned for (in our project that would be the vehicles that have properly paid their parking fee). It opens the question of whether those records should be redacted, or anonymized, where redaction means deleting them from the database. In case of redacting, we have loss of data that we can use for analysis, so the database significantly loses on its usefulness. However, in case of anonymizing (here it

footnote continued on next page

technological design choices and the later processing of data from and about third parties. Therefore, the third-party privacy problem arises from the confluence of technological features that capture third-party data and legal incentives that necessitate the further processing of those data.[101] In other words, controller choice plays less of a role in the third-party privacy problem.

As a result, inferential privacy harms and the third-party privacy problem affect controllers' compliance strategies. Controllers under both sets of circumstances can practice data minimization by limiting the data they collect and generate to only that which is "adequate, relevant, and limited to what is necessary."[102] Controllers creating inferential privacy harms might even go so far as to sidestep privacy law compliance issues by structuring data processing in a way that avoids altogether the creation of personal data—a process some scholars call "regulatory avoidance."[103] However, regulatory avoidance is not a legally or technologically viable option for controllers subject to the third-party privacy problem. Both the technology and the legal incentives drive the processing of third-party personal data.

These distinctions also differentiate between the concept of collective classification created by inferential privacy and the collection of data from third parties involved in the third-party

---

> is suggested that the license place is simply randomly changed), we risk re-identification.

Kristina Batistič, Privacy in Smart Parking 4 (Apr. 14, 2020) (Master's thesis, KTH Royal Institute of Technology & Technical University of Denmark) (Google Scholar). Frederiksberg was not legally required not legally incentivized to retain the third-party data and so could choose how it managed third party data. Its smart parking system, therefore, is not an example of the third-party privacy problem.

101. *E.g.*, Gürses & van Hoboken, *supra* note 51, at 595.

102. GDPR, *supra* note 11, art. 5(1)(c); *see* Anuj Puri, *A Theory of Group Privacy*, 30 CORNELL J.L. & PUB. POL'Y 477, 535–36 (Spring 2021).

103. Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 157 (2016) ("The challenge of sorting out regulatory avoidance from innovation is at the core of debates about the regulation of new business models . . . ."); *see* Helen Nissenbaum, Katherine Strandburg & Salome Viljoen, *The Great Regulatory Dodge*, 37 HARV. J.L. & TECH. 1231, 1238 (2023); Damian George et al., *GDPR Bypass by Design? Transient Processing of Data Under the GDPR*, 9 INT'L DATA PRIV. L. 285, 286 (2019).

privacy problem. In the latter context, the third parties are not a group per se. Rather, they are multiple individuals' data that are processed. Because of common characteristics, it may be possible to assign group attributes to them, but the circumstances of the initial data processing do not require it.[104] An example from automated driving illustrates this distinction. Imagine an automated vehicle traveling in the middle of the night passes only one third party—a pedestrian. To avoid colliding with the pedestrian, data from and about her had to be collected.[105] This example also represents an instance of the third-party privacy problem. From the data collected about the pedestrian, it may be possible to glean information about people with similar characteristics, related or unrelated to her presence on the roadway—an instance of inferential privacy. [106]

The boundaries of the definition of a "collective" may be set by computational abilities and the limits of data scientists' imaginations. Third parties, however, are potentially identifiable individuals from whom data are being processed. The above example demonstrates that a grouping can be formed by processing data from and about third parties—all potential pedestrians. Data from the collective can help generate data about first parties, like human drivers of vehicles. However, absent deliberate inquiries and additional information, it would be exceedingly difficult to derive personal data about individual third parties from first party data.

By focusing on individual third parties, the third-party privacy problem does not need to define collective privacy interests. Later data processing helps create the collective or group identity implicated by inferential privacy.[107] But identifying the third-party privacy problem does not require establishment of a collective or group identity.

104. *E.g.*, Franchi et al., *supra* note 4, at 2880.

105. *See infra* Part V; Franchi et al., *supra* note 4, at 2880.

106. For information on these practices see Helen Nissenbaum, *Contextual Integrity Up and Down the Data Food Chain*, 20 THEORETICAL INQUIRIES L. 221, 240 (2019); Franchi et al, *supra* note 4, at 2881.

107. Bart van der Sloot, *Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation*, 4 INT'L DATA PRIV. L. 307, 322 (2014); *see* Clauda Diaz et al., *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923, 941–42 (2013); Solow-Niederman, *supra* note 41, at 361–62.

Scholars and policy makers have struggled with the legal and moral quandaries raised by the concept of "group rights."[108] Simply put, collective rights are murky.[109] Thus, the third-party privacy problem avoids these issues. It effectively identifies a subset of first parties whose privacy interests may be inadequately protected.[110]

Despite these differences, the third-party privacy problem and inferential privacy harms share some important commonalities. Privacy law's focus on individual, first-party privacy, creates the legal environment in which "no individual—not even a sophisticated consumer—can fully protect herself."[111] For both the third-party privacy problem and inferential privacy harms, "[t]he result is a technologically driven decision-making process that seems to defy interrogation, analysis, and accountability."[112] Relative to privacy law, third parties and the people implicated by inferential privacy "become[] growingly humanless."[113]

"Data processing may respect the data subject's rights, but harm other people or society generally. Addressing these effects requires normative frameworks which center collective interests and democratic control."[114] The conditions that give rise to the third-party privacy problem span the conceptions of individual and collective privacy harms. However, addressing the third-party privacy problem

108. *E.g.*, Asaf Lubin, *Collective Data Rights and Their Possible Abuse*, 95 TEMP. L. REV. 661, 667–70 (2023) (using critiques of collective human rights to anticipate the potential drawbacks of collective data rights); *see generally* Peter Jones, *Group Rights*, Stanford Encyclopedia of Philosophy (Edward N. Zalta & Uri Nodelman eds., 2022), https://plato.stanford.edu/entries/rights-group/ [https://perma.cc/P5XS-MTPN] (describing group rights).

109. Lubin, *supra* note 108, at 669.

110. *See infra* Part IV.C.

111. Graef & van der Sloot, *supra* note 7, at 514; *see* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–82 (2013); Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 594 (2024).

112. Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 FORDHAM L. REV. 613, 614 (2019).

113. Lev-Aretz, *supra* note 68, at 6.

114. Rachel Griffin, *Rethinking Rights in Social Media Governance: Human Rights, Ideology and Inequality*, 2 EUR. L. OPEN 30, 41 (2023).

may not require "cent[ering] collective interests."[115] Solutions can strike a balance between technological capabilities and legal requirements. But creating legal mechanisms that directly intervene with data processing practices can give a third party—as an individual—voice and influence to advocate for their interests. Those same mechanisms may also be used to advocate for the interests of collectives affected by similar data processing practices.[116]

Novel approaches must start outside of privacy law's framework. Consider how the conceptualization of third party used here differs from the term "third party" found in certain data privacy laws.[117] Under both CCPA and GDPR, a third party is a later-stage data processor.[118] This suggests that these laws, and all the laws influenced by them,[119] structure a direct relationship between a data subject and a controller,[120] giving the data subject with the most direct relationship priority of interest over other the privacy rights of other data subjects. Later, "third parties" can touch the data subject's data.[121] The concept of third-party privacy used here draws attention to people that prominent privacy laws literally do not name—data subjects with subordinate privacy interests. As such, the interests of third parties are not fully realized under existing privacy law. At least in the EU, the AI Act might address the privacy interests of third parties. The next Part explains how.

---

115. *Id.*

116. *See, e.g.*, Artur Pericles L. Monteiro, *Countervailing Platform Power*, 41 BERKLEY TECH. L. J. (forthcoming 2026); *cf.* Daniel Solove & Woodrow Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 B.U. L. REV. 1021, 1026–29 (2024) (arguing how privacy law's primary goal regarding personal data should be oriented around societal structure rather than individual control).

117. *See* Waldman, *supra* note 112, at 620 ("Language, Foucault argued, shapes our understanding and perceptions of legitimacy and legality.") (citations omitted).

118. GDPR, supra note 11, art. 4(10); CAL. CIV. CODE § 1798.140(ai) (West 2025).

119. Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021).

120. Or "joint controllers." *See* GDPR, *supra* note 11, art. 26(1). *But see*, David Sella-Villa & Michael E. Hodgson, *Privacy in the Age of Active Sensors*, 92 UMKC L. REV. 67, 117–19 (2023) (discussing limited notice requirements to third parties).

121. GDPR, *supra* note 11, art. 4(10); CAL. CIV. CODE § 1798.140(ai) (West 2025).

III. The EU AI Act: Opportunities to Address the Third-Party Privacy Problem

The AI Act currently offers the best legal mechanisms to address the third-party privacy problem. To that end, this Part starts with a general overview of the AI Act. Then, it explains how the protections for privacy and data protection under the AI Act are broader than those offered by the EU's main privacy law: the GDPR. The Part concludes by arguing why the AI Act represents the highwater mark for laws that can address the third-party privacy problem.

A. Overview of the AI Act

Enacted in 2024, the AI Act aims "to improve the functioning of the [European Union's] internal market by laying down a uniform legal framework . . . for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems)."[122] It approaches this enormous (and ever growing)[123] task by categorizing AI systems according to the level of risk they present "to public interests and fundamental rights," including risks to privacy and data protection.[124] The four risk categories for AI systems are: unacceptable risk, high-risk, limited risk, and minimal risk.[125]

The AI Act prohibits AI systems that present unacceptable levels of risk to "fundamental rights, health and safety and . . . democratic control."[126] Some prohibited AI systems process data in ways that leave people susceptible to manipulation. The AI Act prohibits systems that conduct subliminal messaging, distort the behavior of vulnerable populations, assign social scores in certain contexts, or infer emotions

---

122. EU AI Act, *supra* note 33, recital 1.

123. Alex Singla et al., *The State of AI: How Organizations Are Rewiring to Capture Value*, McKinsey & Co. (Mar. 12, 2025), https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai [https://perma.cc/X7NF-BUSR].

124. EU AI Act, *supra* note 33, recital 5; *see* Charter of Rights, *supra* note 39, arts. 7, 8.1.

125. Lucilla Sioli, *A European Strategy for Artificial Intelligence,* slide 7 (Apr. 23, 2021), https://www.ceps.eu/wp-content/uploads/2021/04/AI-Presentation-CEPS-Webinar-L.-Sioli-23.4.21.pdf [https://perma.cc/ET2E-FFWE] (discussing the EU's approach in the design of the AI Act).

126. EU AI Act, *supra* note 33, recital 20.

in educational and workplace settings.[127] Other prohibited systems use AI to create unacceptable levels of surveillance. These prohibited AI systems include risk-of-crime scoring, compiling facial recognition databases through untargeted scraping, biometric systems inferring sensitive attributes, and real-time biometric identification in public, with certain limited law enforcement exceptions.[128]

Under the AI Act, general-purpose AI systems, like ChatGPT and other large language models,[129] present a limited risk.[130] Depending on certain technical and design features,[131] deployers of these systems may have to provide notice to users that they are interacting with an AI system, comply with EU copyright laws, publish summaries of the content used to train the AI system, provide instructions for its use, conduct risk assessments, and provide cybersecurity protections.[132] Regulation of high-risk AI systems constitutes the bulk of the AI Act, and are discussed in detail below. Some AI systems that present minimal risk may not be regulated under the AI Act.[133]

High-risk AI systems fall into two categories: AI safety systems in products that undergo "third-party conformity assessments"[134] or AI systems listed under Annex III of AI Act.[135] Annex III includes, *inter alia*, AI systems used as part of permitted biometrics, critical infrastructure, education and vocational training, essential private

127. *Id.* art. 5(1)(a)–(c) & (f).

128. *Id.* art. 5(1)(d), (e), (g), (h) & 5(2)–(8).

129. In an effort to extend the AI Act's coverage to include the large language models (LLMs) that experienced a sudden rise in use since 2023, the provisions governing general-purpose AI systems were a "last minute" addition to the AI Act. Alessandro Mantelero, *The AI Act: A Realpolitik Compromise and the Need to Look Forward*, *in* DIGITAL CONSTITUTIONALISM 311, 316 (Spiros Simitis & Indra Spiecker genannt Döhmann eds., 1st ed. 2025), https://doi.org/10.5771/9783748938644-311 [https://perma.cc/KP7Q-9WWL].

130. EU AI Act, *supra* note 33, arts. 3(63), 53; *see* Sioli, *supra* note 125.

131. EU AI Act, *supra* note 33, arts. 50(1), 51, 53(2).

132. *Id.* arts. 50(1), 53(1) & 55(1).

133. *Id.* art. 50(2); *see* Sioli, *supra* note 125, slide 7; Theodore Christakis & Theodoros Karathanasis, *Tools for Navigating the EU AI Act: (2) Visualisation Pyramid*, MIAI GRENOBLE ALPES (Mar. 7, 2024), https://ai-regulation.com/visualisation-pyramid/ [https://perma.cc/W7KJ-49SC].

134. EU AI Act, *supra* note 33, art. 6(1).

135. *Id.* art. 6(2).

services and essential public services, and administration of justice and democratic processes.[136] At the core of their obligations under the AI Act, providers of high-risk AI systems must implement a risk management system.[137] "The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating."[138]

The "entire lifecycle of a high-risk AI system" starts pre-deployment.[139] Some pre-deployment obligations for high-risk AI systems include fundamental rights analyses, testing and governance of training data, implementing human oversight, and generating extensive documentation.[140] Post deployment, the provider must undertake corrective action to bring a high-risk AI system into conformity with the AI Act and provide necessary information to the appropriate market surveillance authorities.[141] Additionally, other parties along the "AI value chain"—distributors, importers, and other third parties—share many similar obligations.[142]

In the coming years, a growing number of AI systems will likely have to meet the requirements for high-risk AI systems under the AI Act. The AI Act includes a procedure for "amend[ing] the list set out in Annex III,"[143] allowing new AI systems to be incorporated. Additionally, though the AI Act exempts some safety systems from all the requirements for high-risk AI systems,[144] the rules governing conformity assessments for AI safety systems will be updated to "take[] into account" the AI Act's risk management requirements.[145]

---

136. *Id.* Annex III.
137. *Id.* art. (9)(1).
138. *Id.* art. (9)(2).
139. *Id.*
140. *Id.* arts. 10–19, 27.
141. *Id.* arts. 20, 28.
142. *Id.* art. 25.
143. *Id.* art. 112(1).
144. *Id.* art. 2(2).
145. *Id.* arts. 102–09.

B. The AI Act and Third-Party Privacy

As discussed above, the GDPR, the EU's primary privacy legislation, does not have a mechanism to realize the full complement of privacy interests of third parties.[146] Though "data subjects" under the GDPR,[147] the third-party privacy problem highlights the fact these people do not have a direct relationship with the controller.[148] The lack of a direct relationship contributes to the later processing of third-party data while taking little account of third-party privacy interests.[149] The AI Act takes important steps to recognizing the privacy interests of third parties.

Under the AI Act, controllers deploying technologies classified as high-risk AIs must implement a comprehensive risk management system "as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating."[150] This risk management system includes at least three features that may capture the privacy interests of third parties.[151]

One feature requires that controllers who deploy high-risk AIs must "identif[y] and analy[ze] . . . the known and the reasonably

146. *See supra* text accompanying notes 16–20, 117–120; *see* Cobbe & Singh, *supra* note 22, at 4–5; *infra* Part V.C.

147. GDPR, *supra* note 11, art. 4(1).

148. *See supra* Part II.A.

149. *See supra* Part II.

150. EU AI Act, *supra* note 33, art. (9)(2).

151. The AI Act's risk management system includes many more provisions than are discussed here. *See id.* arts. 8–49. This discussion focuses on those provisions that are most directly applicable to the third-party privacy problem. These provisions of the AI Act's risk management system may evince what Professors Seda Gürses and Joris van Hoboken describe in their seminal piece, *Privacy After the Agile Turn*. Gürses & van Hoboken, *supra* note 51. They argue that "[d]ata privacy regimes rarely attend to the conditions of production, nor do they easily address the implications of users being enlisted as labor in the production of services through the process of capture." *Id.* at 580–81. The AI's Act risk management requirements for high-risk AI systems seem to attempt exactly that. As such, these risk management requirements may represent a "paradigmatic transformation[] in the production of digital functionality . . . [that] change[s] the conditions of privacy governance." *Id.* at 579. But as compared to the negative effects of agile production that they describe, the AI Act may be a turn for the better.

foreseeable risks that the high-risk AI system can pose to . . . fundamental rights when the high-risk AI system is used in accordance with its intended purpose."[152] The AI Act does not limit this analysis to first parties. Rather the AI Act "applies to . . . affected persons that are located in the [EU].[153] Therefore, the risk management system requires an analysis of how the high-risk AI system might present risks to the fundamental rights of affected persons.

The EU Charter of Fundamental Rights enshrines the fundamental rights of people located in the EU.[154] With privacy and data protection, "*everyone*" enjoys "the right to respect for his or her private and family life, home and communications," and "the right to the protection of personal data concerning him or her."[155] Accordingly, if a high-risk AI system processes information about a third party's "private and family life, home and communications" or otherwise generates "personal data,"[156] that third party becomes an affected person. The controller deploying that high-risk AI system must identify and analyze the risk.[157]

The reference to fundamental rights in the AI Act's risk management system may have intended to enable broader privacy and data protections than those afforded by the GDPR.[158] Third party

152. EU AI Act, *supra* note 33, art. (9)(2)(a).

153. *Id.* art. (2)(1)(g).

154. *Id.* recital 1. These protections potentially extend to people located outside of the European Union. *See* Press Release, No. 37/2020, To the Judgment of the First Senate of 19 May 2020, 1 BvR 2835/17, Federal Intelligence Service—Foreign Surveillance (May 19, 2020), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html [https://perma.cc/79KC-XG3J]

155. Charter of Rights, *supra* note 39, arts. 7, 8.1 (emphasis added).

156. *Id.* arts. 7, 8.1.

157. EU AI Act, *supra* note 33, art. (9)(2)(a).

158. *Compare id.* recital 1 ("The purpose of this Regulation is . . . to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union."), *with id.* recital 10 ("The fundamental right to the protection of personal data is safeguarded in particular by [GDPR and two other data protection regulations]."). Applying the language of the third-party privacy problem, as a legal standard, the Charter of Fundamental Rights enjoys a broader set of

footnote continued on next page

privacy, therefore, could find legal grounding in a fundamental rights analysis that differs from the GDPR.[159] But even within the more limited interpretations of privacy and data protections offered by the GDPR, the AI Act suggests readings of GDPR jurisprudence that may still capture the privacy interests of third parties.[160]

The GDPR's applicability to third party privacy hinges on the definition of personal data.[161] The GDPR has an expansive definition of personal data[162]: "[A]ny information relating to an identified or identifiable natural person."[163] As the EU's General Court commented in the *Nowak* case, the term "'any information' . . . reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information."[164] "In respect of the second element, data can be said to relate to a natural person if it is about the relevant person."[165] With such broad coverage, the data that high-risk

affordances than GDPR. *See* Calo, *supra* note 55; *accord* Cobbe & Singh, *supra* note 22, at 17.

159. *See* Kaminski, *supra* note 35, at 386 ("Individual rights are not sufficient by themselves, but they are necessary for data privacy."). *But see* EU AI Act, *supra* note 33, recital 10 ("[The AI Act] does not seek to affect the application of existing Union law governing the processing of personal data. . . . It also does not affect the obligations of providers and deployers of AI systems in their role as data controllers or processors stemming from Union or national law on the protection of personal data in so far as the design, the development or the use of AI systems involves the processing of personal data.").

160. *But cf.* Graef & van der Sloot, *supra* note 7, at 518 ("History of ECJ Privacy Jurisprudence does not allow collective/class claims.") (citations omitted).

161. Montagnani & Verstraete, *supra* note 93, at 1178 (citations omitted).

162. *See* Nadezhda Purtova, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, 10 L., INNOVATION & TECH. 40, 41 (2018). *But see* César Augusto Fontanillo López, *Against Biometric Identifiability. Part I: The Law of What Is Reasonably Likely*, 11 EUR. DATA PRO. L. REV. 465 (2026) (arguing for a narrower interpretation of GDPR's definition of personal data).

163. GDPR, *supra* note 11, art. 4(1); *see* Montagnani & Verstraete, *supra* note 93, at 1177–80.

164. Nowak v. Data Prot. Comm'r, Case C-434/16, 2017, ¶ 34, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CN0434&qid=1775429466487 [https://perma.cc/GN4X-9VK9].

165. Emmanuel Salami, *Balancing Competing Interests in the Reidentification of AI-Generated Data*, 8 EUR. DATA PROT. L. REV. 362, 369 (2022) (citing Article 29

footnote continued on next page

AI systems collect from and generate about third parties likely qualify as "any information relating to" a third party.[166]

The identifiability element of the GDPR's definition of personal data may present an issue for third parties. Data are considered anonymous or non-personal when they cannot identify a natural person.[167] AI systems (but not necessarily high-risk AI systems) make identification easier, such that the distinction between personal data and anonymous or non-personal data may become "obscured."[168] GDPR jurisprudence, however, does not consider the question of identifiability in an absolute or theoretical sense.[169] Rather, the *Breyer* case presents the question of identifiability as a relative one—the Court of Justice of the European Union ("CJEU") focused on the abilities of the party holding the data to identify natural persons.[170] "In *Breyer*, . . . the CJEU ruled that identification would not be reasonably likely if it was 'prohibited by law or practically impossible' due to 'a

Working Party, "Opinion 04/2007 on the concept of personal data" (WP 136) 01248/07/EN, 9–12).

166. GDPR, *supra* note 11, art. 4(1).

167. GDPR, *supra* note 11, recital 26; Salami, *supra* note 165, at 370.

168. Salami, *supra* note 165, at 370 (citing Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1723 (2010)); *accord.* Franchi et al, *supra* note 4, at 2878 ("The privacy conceptions most susceptible to erosion by AI's inferential power are likely those grounded exclusively in categorical distinctions."); *see* Salami, *supra* note 165, at 371.

169. *See* Purtova, *supra* note 162; *cf.* Theodore Christakis, *The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach*, Ctr. for Info. Pol'y Leadership 60 (Feb. 2024), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_zero_risk_fallacy_-_t.christakis_feb24.pdf [https://perma.cc/V7HP-8VF5] ("While some of the GDPR articles, especially respect of the principles concerning processing of personal data under Article 5, are formulated in absolute terms, and must be protected under any circumstances, the whole logic of the GDPR revolves around imposing a 'risk-based accountability principle' on data controllers."). *But see* Michèle Finck & Frank Pallas, *They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data Under the GDPR*, 10 Int'l Data Privacy L. 11 (2020) (discussing conflicting interpretations of the risk-based approach to identifiability).

170. Breyer v. Bundesrepublik Deutschland, Case C-582/14, 2016, ¶ 43, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582 [https://perma.cc/978R-GFS8].

disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.'"[171] Accordingly, the party sharing data must consider its audience.

When a party shares information with the intention that it be made available to the general public, the EU General Court's ruling in *OC* arguably narrows the test of reasonable likelihood of identification.[172] In *OC,* the European Anti-Fraud Office issued an anonymized press release about an investigation into a scientist's allegedly fraudulent use of EU grant funds, which later proved to be incorrect.[173] Based on that press release, a journalist specializing in science reporting quickly identified the scientist in question.[174] In other words, it was not practically impossible for the specialized journalist to reidentify the scientist. Despite the journalist's reidentification of the scientist based on his knowledge, combined with the press release, the General Court ruled that the press release did not constitute personal data because the journalist should not be considered an "average reader."[175]

For data released to a specific party, the EU's General Court clarified the importance of a fact-dependent analysis in the *SRB* case.[176]

---

171. Bryce Clayton Newell et al., *Regulating the Data Market: The Material Scope of American Consumer Data Privacy Law*, 45 U. PA. J. INT'L L. 1055, 1095 (2024) (citing *Breyer*, Case C-582/14, ¶ 43).

172. Though this decision was appealed, the points of law discussed here were not overturned on appeal., OC v. European Commission, Case C-479/22, 2024, ¶90, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0479 [https://perma.cc/2LNY-QHS4].

173. OC v. European Commission, Case T-384/20, 2022, ¶ 8 (translated from French), https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex:62020TJ0384 [https://perma.cc/84UT-WFGH]. The allegation was later found to be erroneous by determination of a Greek court. Efeteio Thessalonikis [Thessaloniki Court of Appeals] 1042/2025 (Gr.) (June 3, 2025) (decision and translation on file with author).

174. *Id.* ¶¶ 74–80.

175. *Id.* ¶ 76 ("Le journaliste . . . ne saurait être considéré comme *un lecteur moyen*." ["The journalist . . . cannot be considered *an average reader*."]) (emphasis added).

176. Iain Nash et al., *Legal Issues in Reconciling Data Protection, AI, and Cybersecurity Under EU Law*, 89 MO. L. REV. 871, 885–86 (2024).

In that case, the court specified that a party transmitting information needed to consider at least two factors:

> [W]hether the possibility of combining the [transmitted] information . . . with the additional information held by [the transmitting party] . . . constituted a means likely reasonably to be used by [the receiving party] to identify [people] and whether the [receiving party] . . . had legal means available to it which could in practice enable it to access the additional information necessary to re-identify [a person].[177]

If either of these factors are satisfied, the information could be understood as personal data.

For third parties, the above interpretations of identifiability under GDPR suggest that as long as a controller does not collect specific information that allows third parties to be identified through the efforts of an "average reader," then the controller does not have personal data from or about third parties. Without a controller originally holding their personal data, and impracticality preventing later reidentification, personal data about third parties would not be understood to exist. GDPR, therefore, would not apply to third parties. While identifiability jurisprudence under the GDPR creates a pathway for controllers to practice regulatory avoidance,[178] the AI Act's risk management system has a second feature that potentially engages GDPR protections for third-party data.

The AI risk management system considers "the entire lifecycle of a high-risk AI system."[179] This lifecycle includes "outputs produced by the AI system."[180] If the output of the system includes data about third parties, the provider must consider "the reasonably foreseeable risks" these data can pose to the privacy and data protection rights of third

177. Single Resolution Bd. v. Eur. Data Prot. Supervisor, Case T-557/20, 2023, ¶¶ 104–05, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020TJ0557 [https://perma.cc/ZXK9-Q7LG]

178. *See supra* text accompanying note 103.

179. EU AI Act, *supra* note 33, art. 9(2); *see id.* recitals 6-8.

180. *Id.* art 1(c).

parties.[181] Per the *Breyer* case, that reasonably foreseeable risk to identifiability includes not only the AI system outputs the controller generates, but also other information that the controller can access to identify third parties.[182] For example, when high-risk AI systems capture video imagery of third parties, it is hard to argue that reidentification is not a reasonably foreseeable risk.[183]

In the context of the third-party problem, "the entire lifecycle of a high-risk AI system"[184] includes sharing high-risk AI system outputs about third parties with others.[185] The "reasonably foreseeable risks that the high-risk AI system can pose to . . . fundamental rights" includes the chance that those who receive the data will be able to identify the third parties.[186] If the law requires the controller to share the data with specific parties, the *SRB* case would suggest that the controller must assess each required recipient of the AI system outputs to determine its capabilities to identify third parties.[187] If the controller has obligations to share the data generally, without a specific recipient in mind, then the controller must consider the capabilities of the "average reader" of that data.[188] Under both scenarios, this analysis would include considering the recipient's technical capabilities and the other information available to them.[189]

The AI Act's lifecycle analysis of the data produced by high-risk AI systems may effectively eliminate a GDPR avoidance strategy. With the proliferation of data sets and user-friendly large language

181. *Id.* art. 9(2)(a).

182. *See supra* notes 169–170 and accompanying text.

183. The Dutch Autoriteit Persoonsgegevens [Data Protection Authority], for example, investigated the recording capabilities of the cameras of Tesla vehicles deployed in Sentry mode when the vehicle is parked. *Tesla Makes Camera Settings More Privacy-Friendly Following DPA Investigation*, AUTORITEIT PERSOONSGEGEVENS (Feb. 22, 2023), https://www.autoriteitpersoonsgegevens.nl/en/current/tesla-makes-camera-settings-more-privacy-friendly-following-dpa-investigation [https://perma.cc/87EW-M8XK (staff-uploaded)]; *see infra* note 366 and accompanying text.

184. EU AI Act, *supra* note 33, art. 9(2)(a).

185. *See supra* Part II.B.; *infra* Part V.B.

186. EU AI Act, *supra* note 33, art. 9(2).

187. *See supra* text accompanying note 177.

188. *See supra* text accompanying note 175.

189. *See supra* text accompanying notes 170 and 171.

models,[190] the average person may soon be able to do what computer scientists have achieved for years—combine otherwise anonymous data sets to deanonymize them.[191] But unlike the computer scientists, the average person may not consider all the necessary steps to preserve the anonymity, and therefore the privacy and data protection rights, of third parties.[192]

When interpreting these technical capabilities under the GDPR's identifiability jurisprudence, Dr. Emmanuel Salami has argued that "[o]nce data re(identification) occurs, the party that originally intended to generate the data will be the most appropriate party to be accorded as the data producer."[193] This is consistent with the AI Act's lifecycle analysis. In short, providers of high-risk AI likely must account for the identifiability of third-party data throughout that data's lifecycle. Further, this understanding of the potential privacy and data protection risks to third parties should inform "the adoption of appropriate and targeted risk management measures designed to address the[se] risks."[194] While this may not expand GDPR jurisprudence per se, it creates the opportunity for controllers who deploy high-risk AI systems to address the privacy and data protection interests of third parties.

The AI Act's risk management system does not require a provider to address all possible risks privacy and data protection risks, just those that arise "when the high-risk AI system is used in *accordance with its intended purpose*."[195] In the context of the third-party privacy problem, the controller can establish the intended purpose of the

190. *E.g.*, Ken Kehoe, *How LLMs Will Democratize Exploratory Data Analysis*, MEDIUM (June 9, 2024), https://medium.com/data-science/how-llms-will-democratize-exploratory-data-analysis-70e526e1cfic [https://perma.cc/SGL6-6L8Q].

191. *E.g.*, Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, 2008 IEEE SYMP. ON SEC. & PRIVACY 111, 121 (2008).

192. *See, e.g.*, Sakib Shahriar et al., *A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle*, *in* 11 IEEE ACCESS 61829, 61845–46 (2023); Hannah Brown et al., *What Does it Mean for a Language Model to Preserve Privacy?*, PROCS. OF THE 2022 ACM CONF. ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 2280, 2283–88 (2022).

193. Salami, *supra* text accompanying note 165, at 376; *see supra* text accompanying notes 68–75.

194. EU AI Act, *supra* note 33, art. 9(2)(d).

195. *Id.* art. 9(2)(a) (emphasis added); *accord. id.* art. 9(2)(d).

high-risk AI system, "including the specific context and conditions of use."[196] The scope of a high-risk AI system's intended purpose can limit a controller's inquiries into others that receive outputs from these systems and the capabilities of others to identify third parties based on those data. The controller does not need to address all possible reidentification risks presented by the parties receiving the data outputs of the high-risk AI system—only those risks that arise when these data are used as part of the intended purpose of the high-risk AI system.[197]

The high-risk AI risk management system, however, requires that providers at least consider alternative uses of the outputs of these systems. Providers of high-risk AI systems must also "estimate[e] and evaluat[e]. . . the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and *under conditions of reasonably foreseeable misuse*."[198] This represents the third feature of the AI Act's risk management system that may capture the privacy interests of third parties.

In the context of the third-party privacy problem, inappropriate reidentification of third parties could be a reasonably foreseeable misuse of outputs from a high-risk AI system. However, addressing all possible means of reidentifying third parties based on data outputs from a high-risk AI system is beyond the scope of the AI Act.[199] Further, such a requirement would support an absolute or theoretical interpretation of identifiability in personal data and therefore run

196. *Id.* art. 3(12) (listing the definition of 'intended purpose'). Under the AI Act, a party can engage in activities that qualify it as both a 'provider' and a 'deployer' at the same time. In the context of the third-party privacy problem, the concept of controller does not exclude that possibility. Accordingly, this Article attributes to the controller the ability to establish the intended purpose of a high-risk AI system. *Id.* art. 3(12) (listing the definition of "intended purpose").

197. The intended purpose of the high-risk AI system constrains several other data management requirements under the AI Act. EU AI Act, *supra* note 33, arts. 10(2), 12(2), 19(1), 26(4).

198. *Id.* art. 9(2)(b) (emphasis added).

199. *See id.* art. 9(2)(d); *see also id.* art. 9(5) ("The risk management measures referred to in paragraph 2, point (d), shall be such that the relevant residual risk associated with each hazard, as well as the overall residual risk of the high-risk AI systems is judged to be acceptable.").

contrary to GDPR jurisprudence.[200] Nonetheless, the AI Act requires controllers at least to acknowledge the privacy and data protection risks that misuse of outputs from high-risk AI systems might pose to third parties.[201] The continuous and iterative nature of the risk management system creates opportunities to mitigate those risks, even as AI systems and available data sets evolve.[202]

Taken altogether, these features of the AI Act's risk management system can address the interests of people outside the first-party-to-controller relationship at the heart of GDPR.[203] Through this expansion, the AI Act "combin[es] technical, organizational, and regulatory approaches"[204] to data governance that can capture the privacy and data protection interests of third parties. Though the AI Act might not present the "relational turn" in privacy and data protection that would address inferential privacy,[205] it is potentially a significant step in safeguarding the privacy and data protection interests of third parties.[206] Further, for certain high-risk AI systems, it is only one of the interventions offered by the AI Act.

---

200. *See supra* text accompanying notes 167–177; EU AI Act, *supra* note 33, recital 10.

201. *Cf.* Andrea Vigorito, *Government Access to Privately-Held Data: Business-to-Government Data Sharing: Voluntary and Mandatory Models*, 9 EUR. J. COMPAR. L. & GOVERNANCE 237, 243 (2022) ("[D]ata collection itself creates the general risk of privacy incursions which can jeopardize individuals' dignity and self-determination.").

202. *See* Salami, *supra* note 165, at 373.

203. *See* Veale, *supra* note 9, at 6.

204. Gürses & van Hoboken, *supra* note 51, at 580–81.

205. *See* Richards & Hartzog, *supra* note 89; Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 310, 310 (2020); *see also* Maria Tzanou, *The Future of EU Data Privacy Law: Towards a More Egalitarian Data Privacy*, 7 J. INT'L & COMPAR. L. 449, 464–69 (2020) (arguing that characteristics based on social relationships should receive greater protection under EU data protection law).

206. *See* Luciano Floridi, *On Human Dignity as a Foundation for the Right to Privacy*, 29 PHIL. & TECH. 307, 311 (2016) ("It is the hallmark of being human that we can care beyond our needs and drives. A private life complements a caring life.").

C. The AI Act: The High-Water Mark for Third-Party Privacy Protection

The AI Act distinguishes between two types of high-risk AI systems: AI safety systems in products that undergo "third-party conformity assessments"[207] or AI systems listed under Annex III of the AI Act.[208] Providers of high-risk AI systems that fall under Annex III must implement the risk management system described above along with other requirements.[209] At this time, the providers of high-risk AI safety systems do not necessarily have to implement the risk management system.[210] But the laws establishing the conformity requirements for safety systems must be updated to "take[] into account" the AI Act's risk management system and other data governance requirements.[211] In effect this means that the rules governing the design and conformity assessments of high-risk AI safety systems offer an additional legal mechanism that accounts for the privacy interests of third parties—a process of "adopting delegated acts."[212]

At one level, these delegated acts can ensure that providers of a high-risk AI safety system demonstrate compliance with the AI Act's risk management system as part of establishing conformity for their products.[213] This means analyzing how the high-risk AI safety system affects third party privacy would be a necessary part of placing these products on the market.[214] Requiring and verifying a third-party privacy analysis of the high-risk AI safety system adds an element of

---

207. EU AI Act, *supra* note 33, art. 6(1)(b).

208. *Id.* art. 6(2).

209. *Id.* arts. 8–49.

210. *Compare id.* art. 2(2) ("For AI systems classified as high-risk AI systems in accordance with Article 6(1) related to products covered by the Union harmonisation legislation listed in Section B of Annex I, only Article 6(1), Articles 102 to 109 and Article 112 apply."), *with id.* art. 113(c) ("Article 6(1) and the corresponding obligations in this Regulation shall apply from 2 August 2027.")

211. *See id.* arts. 102-109 & 112; *accord. id.* art. 2(2).

212. *Id.* at 107 & 109; *cf.* Viljoen, *supra* note 24, at 468 ("[P]ositive legal theories of data governance aim to develop legal responses to equalize and democratize the data relations that will constitute digital social life.").

213. *But see* EU AI Act, *supra* note 33, recital 49.

214. *See* Vigorito, *supra* note 201, at 238.

"interrogation, analysis, and accountability" to technologies that present the third-party privacy problem.[215]

The delegated acts have an opportunity to go even further. The "state of the art of AI and AI-related technologies" advances regularly,[216] particularly when it comes to reidentifying third parties.[217] Consistent with the call of the AI Act to "ensur[e] a high level of protection of . . . fundamental rights,"[218] the delegated acts can mandate changes to the design of high-risk AI safety systems themselves. These changes can balance the proper function of the high-risk AI safety systems with the need to minimize the risks these technologies present to the third-party privacy.[219] In short, the adoption of delegated acts creates the opportunity for data governance interventions to address the third-party privacy problem beyond data protection law.[220]

Though several countries have privacy laws modeled off of the GDPR,[221] no other jurisdiction to date has enacted AI legislation as comprehensive and sensitive to the privacy interests of third parties as the EU's AI Act.[222] The AI Act, therefore, represents the high-water mark for third-party privacy protection.

This Part argued that the AI Act currently offers the best set of legal mechanisms to address the third-party privacy problem. But what might that look like in practice? The next two Parts of the Article assess the third-party privacy problem in the context of data collected by externally facing sensors on vehicles and the safety systems that

---

215. Waldman, *supra* note 112, at 614; *accord. id.* at 624.

216. EU AI Act, *supra* note 33, art. 8(1); *accord id.* arts. 102–109.

217. *See supra* text accompanying notes 168, 192 & 202.

218. EU AI Act, *supra* note 33, recital 1.

219. *See* Roxana Vatanparast, *Digital Monetary Constitutionalism: The Democratic Potential of Monetary Pluralism and Polycentric Governance*, 30 IND. J. GLOB. LEGAL STUD., 165, 168 (2023).

220. *See* Gürses & van Hoboken, *supra* note 51, at 580–81.

221. *See* Chander et al., *supra* note 119.

222. *See* IAPP RSCH. & HIGHLIGHTS, GLOBAL AI LAW AND POLICY TRACKER (May 2025), https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf [https://perma.cc/TQK5-W7PP]; Richard Sentinella & Cobun Zweifel-Keegan, *US State AI Governance Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker/#state-ai-governance-law-chart [https://perma.cc/G85F-AQ6Z] (last updated Mar. 3, 2026).

process these data. Part III explains what these technologies are, how they collect data from and about third parties, and how they qualify as high-risk AI safety systems. Using the AI Act's risk management system as a framework, Part IV examines whether the legal mechanisms influencing the flow of data from vehicles' externally facing sensors protect the privacy interests of third parties. Otherwise, this portion of the AI Act falls short of addressing the third-party privacy problem.

IV. VEHICLES' EXTERNALLY FACING SENSORS & THE AI ACT

This Part describes the vehicle technologies that contribute to the third-party privacy problem and shows how they are regulated under the AI Act.

A. Technological Capabilities of Vehicles' Externally Facing Sensors

This Section offers a brief introduction to the externally facing sensors deployed in vehicles.[223] These sensors fall into two broad categories. One set of sensors operate similarly to human senses and simply collect ambient energy.[224] Another set, active sensors, introduce their own energy into the environment and measure its return.[225] The discussion on externally facing sensors explains how these technologies work generally and specifically how vehicle manufacturers deploy them.[226] This Section concludes by explaining

223. The variety of externally facing sensors and the myriad uses of their data are too many to enumerate here. For example, though not discussed here, microphones can play an important role in certain vehicle safety systems. *E.g.*, John Irwin, *Exterior Mic Can Hear Voice Commands*, AUTOMOTIVE NEWS (April 09, 2023, at 00:00 ET), https://www.autonews.com/technology/new-auto-tech-microphones-outside [https://perma.cc/39FH-FLKM].

224. Sella-Villa & Hodgson, *supra* note 120, at 75.

225. *Id.* at 75. There are, of course, sensors systems that feature capabilities of both active and passive sensors. For example, a headlight introduces energy that an electooptical camera of the visible light spectrum can collect.

226. In the context of the third privacy problem, vehicle manufacturers serve as the controller for vehicles because they have the most agency in design and deployment of externally facing sensor systems. If vehicles were to become more "open," then this analysis would need to focus on the party, or even groups of parties, that chose to install or enable the capabilities described

footnote continued on next page

why the data from externally facing vehicle sensors can affect the privacy interests of third parties.

1. Electrooptical Cameras

Electrooptical cameras operate similarly to the human eye, capturing ambient energy in the visible light spectrum. The system of driving—from vehicle design to rules of the road—all assume that the driver meets some minimum standard of eyesight.[227] Drivers determine where to go and where not to go primarily through visual cues on and along the roadway. Externally facing electrooptical cameras on vehicles seek to identify those same cues to inform the driving experience. For example, these cameras help keep a vehicle in its lane, read nearby road signs, and identify when a pedestrian might be approaching the vehicle.[228]

Still using only ambient energy, some electrooptical cameras can observe objects beyond a human's line of sight. By measuring slight changes in light intensity, these cameras can detect and even generate images of items obstructed from view.[229] In other words, some cameras can see around corners.[230] In the vehicle context, this type of externally facing sensor can inform the driving experience by using information about "what lies beyond the next bend or another car."[231] Accordingly,

here. *See* Determann & Perens, *supra* note 5, at 917–18; Balayn & Gürses, *supra* note 55 ("Users . . . may in fact be interacting with dozens of services that, like matryoshka dolls, may comprise further bundles of services.").

227. *E.g.*, Commission Directive 2009/113/EC, 2009 O.J. (L 223) 31.

228. *See infra* Part IV.A.

229. Felix Naser et al., *ShadowCam: Real-Time Detection of Moving Obstacles Behind a Corner for Autonomous Vehicles*, 21ST INT'L CONFERENCE ON INTELLIGENT TRANSP. SYS. (ITSC) 560 (2018), https://sia.mit.edu/wp-content/uploads/2019/02/2018-naser-et-al-itsc.pdf [https://perma.cc/UGB7-ZE6A].

230. *New Camera Can See Around Corners*, MIT TECH. REV. (Jan. 6, 2017), https://www.technologyreview.com/2017/01/06/154704/new-camera-can-see-around-corners/ [https://perma.cc/Z94X-7LBD].

231. Felix Heide et al., *Non-line-of-sight Imaging with Partial Occluders and Surface Normals*, ARXIV (2018), https://arxiv.org/pdf/1711.07134 [https://perma.cc/J9KD-CY3E].

even if a person on the roadway cannot see a third party, the vehicle may still capture an image of them.[232]

2. Active Sensors

Active sensors—radar, lidar, and sonar—all work by emitting short pulses of known quanta of energy into an environment and measuring their return. Lidar systems use near-infrared light waves[233] and radar uses radio waves.[234] Sonar uses sound waves.[235] Therefore, a lidar sensor calculates distance to an object based on how long it takes to send and receive a pulse of light.[236]

Because active sensors emit energy in pulses, they can generate thousands of distance calculations per second.[237] Accordingly, these calculations provide detailed measurements of the environment around the sensor. Additionally, the pulses also push past surfaces that are permeable to the energy,[238] revealing objects beyond perception

---

232. Connected vehicle systems, though not commonly used, offer a means of capturing images via electrooptical cameras of third parties on the roadway visible to one vehicle and sharing it with other vehicles that would not otherwise be able capture such an image at that moment. *See* Rongqiu Song et al., *Digital Roads and Data Ethics: Exploring the Road Users' Perspective*, in 115 TRANSPORTATION RESEARCH PART F: TRAFFIC PSYCHOLOGY & BEHAVIOUR 103330 (2025), https://www.sciencedirect.com/science/article/pii/S1369847825002785. [https://perma.cc/5DFL-SUM3 (staff-uploaded)].

233. *Why Does LiDAR Have a Specific Wavelength? Part. 1*, YELLOWSCAN (July 21, 2020), https://www.yellowscan.com/knowledge/why-does-lidar-have-a-specific-wavelength [https://perma.cc/U2E4-4APX].

234. *How Radar Works*, NAT'L OCEANIC & ATMOSPHERIC ADMIN. (NOAA) [hereinafter NOAA Radar], https://www.noaa.gov/jetstream/doppler/how-radar-works [https://perma.cc/C3UL-DQ55].

235. *What Is Sonar?*, NAT'L OCEANIC & ATMOSPHERIC ADMIN. (NOAA), https://oceanservice.noaa.gov/facts/sonar.html [https://perma.cc/N78M-WJS7].

236. Leah A. Wasser, *The Basics of LiDAR—Light Detection and Ranging—Remote Sensing*, NAT'L ECOLOGICAL OBSERVATORY NETWORK, https://www.neonscience.org/resources/learning-hub/tutorials/lidar-basics [https://perma.cc/7DDX-5DVM] (last updated Apr. 2, 2026).

237. NOAA Radar, *supra* note 234; JAMIE CARTER ET AL., NOAA COASTAL SERVS. CTR., LIDAR 101: AN INTRODUCTION TO LIDAR TECHNOLOGY, DATA, AND APPLICATIONS 3 (Nov. 2012) [hereinafter NOAA LIDAR], https://coast.noaa.gov/data/digitalcoast/pdf/lidar-101.pdf [https://perma.cc/JGA6-9DR6].

238. Sella-Villa & Hodgson, *supra* note 120, at 84, 88 n.189.

from sensors collecting ambient energy (e.g., human eyes and electrooptical cameras). In short, active sensor measurements can generate detailed maps of spaces not readily visible to the human eye.[239]

In the driving context, low visibility and vegetation limit the efficacy of electrooptical cameras.[240] energy emitted by active sensors can push past these types of barriers.[241] This combination of features allows these sensors to play an important role in safety systems.[242] However, these qualities also allow active sensors to process data to generate a rich understanding of the people and places on and along the roadway that complements and augments the capabilities of traditional cameras.[243]

3. *Data from Vehicles' Externally Facing Sensors*

In the vehicle context externally facing sensors generally do not gather information about the environment around the vehicle simply for the sake of data collection.[244] Rather, the information generated informs the operation of a variety of systems in the vehicle. The vehicle systems using externally facing sensors are discussed based on their current rate of use on the roadway.

Object Detection Systems. Certain vehicle safety systems regularly scan the roadway to identify objects that could pose a safety issue.[245] Many of these systems rely on both electrooptical cameras and active sensors to collect information about objects on the road and

---

239. NOAA LIDAR, *supra* note 237, at 13.

240. Sella-Villa & Hodgson, *supra* note 120, at 75, 94.

241. *Id.* at 75.

242. AVENUE21. PLANNING AND POLICY CONSIDERATION FOR AN AGE OF AUTOMATED MOBILITY 407 (Mathias Mitteregger et al. eds., 2023) [hereinafter AVENUE21] ("Examples of key technologies are those that are the backbone of the innovative sensor systems . . . .").

243. *Id.* at 70; *see also* Sella-Villa & Hodgson, *supra* note 120, at 108, 114, 118.

244. At least as a primary purpose anymore. *See* Ron Amadeo, *Google's Street View Cars Are Now Giant, Mobile 3D Scanners* (Sep. 6, 2017, at 15:35 ET), https://arstechnica.com/gadgets/2017/09/googles-street-view-cars-are-now-giant-mobile-3d-scanners/ [https://perma.cc/WG3X-2R8G] (describing how Google Street View car is creating 3D maps of the environment around the car, or data collection for the sake of data collection).

245. Michael Barnard, *Tesla & Google Disagree About LIDAR—Which Is Right?*, CLEANTECHNICA (July 29, 2016), https://cleantechnica.com/2016/07/29/tesla-google-disagree-lidar-right/ [https://perma.cc/DUN3-UHHP].

determine whether they pose a safety risk.[246] Adaptive cruise control, for example, includes an object detection system which identifies that something on the roadway is moving and may calculate its relative speed. Object detection systems can also perform more advanced data processing. Beyond mere detection, they classify and identify the objects in and along the roadway.[247] By identifying the objects, the vehicle safety systems can potentially inform more advanced driving behaviors that promote overall roadway safety.[248] Similar systems offer situational awareness, to either the human driver or vehicle safety features, without specifically classifying all the objects detected.[249]

Localization and Mapping. Externally facing sensors play an important role in helping vehicles with higher degrees of automation understand the location of the vehicle in relation to its surroundings. The process of identifying a vehicle's location on a map is called "localization."[250] To promote safety through redundancy, by having diverse systems perform similar functions, increasingly autonomous vehicles use several sensor systems to conduct localization.[251] In effect, such vehicles have multiple 3-D "maps" stored in their software.[252]

---

246. *See, e.g.*, *True Redundancy*, MOBILEYE, https://www.mobileye.com/technology/true-redundancy/ [https://perma.cc/R8G2-YEFH].

247. *See* Alireza Ghasemieh & Rasha Kashef, *3D Object Detection for Autonomous Driving: Methods, Models, Sensors, Data, and Challenges*, 8 TRANSP. ENG'G 1, 1 (2022).

248. Xiang Jia et al., *Fast and Accurate Object Detector for Autonomous Driving Based on Improved YOLOv5*, 13 SCI. REPS. art no. 9711, at 1 (2023).

249. *See* Jiayao Li et al., *A Segmentation Network for Enhancing Autonomous Driving Scene Understanding Using Skip Connection and Adaptive Weighting*, 15 SCI. REP. 36692 (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12541098/; *see, e.g.*, *Hayden AI Announces Moving Violation Enforcement Solution for Bus Lanes*, HAYDEN AI (May 25, 2023), https://www.hayden.ai/press/moving-violations-bus-lanes-solution [https://perma.cc/MKX9-WSQG].

250. Nefi Alarcon, *DRIVE Labs: How Localization Helps Vehicles Find Their Way*, NVIDIA DEV. TECH. BLOG (Jan. 20, 2020), https://developer.nvidia.com/blog/drive-labs-how-localization-helps-vehicles-find-their-way/ [https://perma.cc/T8VE-EVQ4].

251. *See* AVENUE21, *supra* note 242, at 260.

252. Sangmin Lee & Jee-Hwan Ryu, *Autonomous Vehicle Localization Without Prior High-Definition Map*, 40 IEEE TRANSACTIONS ON ROBOTICS 2888, 2888 (2024).

Prior active sensor data collections[253] help vehicle safety systems create 3-D maps of the area around roadways.[254] While driving, active sensors "compar[e] the stored geometric features with the data detected in real time, [and] the . . . [vehicle] can locate itself by recognizing these features, known as landmarks."[255] Though not intended to be the sole system of localization,[256] active sensors can establish the geolocation of a vehicle and therefore serve as a redundant mapping feature.

Sensor Recordings. Recordings of the roadway from externally facing sensors serve at least three purposes, potentially simultaneously.[257] First, some object classifications and localization and mapping systems use some data from these recordings to improve themselves through machine learning.[258] Second, externally facing sensor recordings of the roadway can help reconstruct the

253. Amadeo, *supra* note 244.

254. *See* AVENUE21, *supra* note 242, at 89. A growing number of vehicle safety systems have deployed end-to-end artificial intelligence systems to accomplish localization with a less detailed map. The data collected from externally facing sensors remains the same, but these systems process it differently than the localization and mapping systems more commonly in use today. *E.g.*, *Wayve's AV2.0 Approach*, WAYVE, https://wayve.ai/technology/#AV2.0 [https://perma.cc/A6L7-RQA6] ("AV2.0 doesn't rely on HD maps.").

255. AVENUE21, *supra* note 242, at 89.

256. Global positioning systems typically establish a vehicle's location on the 2-D maps that human drivers typically use. Also generating two-dimensional data, inertial measurements track a vehicle's movements from a known starting point to establish its location. AVENUE21, *supra* note 242, at 260.

257. *See* de Bruin, *supra* note 6, at 486, 495; Tianyue Zheng et al., *AutoFed: Heterogeneity-Aware Federated Multimodal Learning for Robust Autonomous Driving*, PROCS. 29TH ANN. INT'L CONF. ON MOBILE COMPUTING AND NETWORKING art. no. 15, at 2 (2023) (citations omitted).

258. *E.g.*, Abhishek Gupta et al., *Deep Learning for Object Detection and Scene Perception in Self-Driving Cars: Survey, Challenges, and Open Issues*, 10 ARRAY art. no. 100057, at 9 (July 2021); *AV2.0 Fleet Learning Loop*, WAYVE, https://wayve.ai/technology/#fleet-learning [https://perma.cc/A9XJ-73CG] (emphasis added) ("AV2.0 introduces a rapid, continuous, and seamless fleet-learning loop: *recording data*, training models, evaluating performance, and deploying updated models.").

circumstances that led to a crash.[259] Third, some vehicles safety system manufacturers share data collected from externally facing sensors among vehicles deploying similar systems.[260]

Though not widely deployed, the long-envisioned Cooperative Intelligent Transport System ("C-ITS") shares "Decentralised Environmental Notification Messages ("DENM"), . . . upon the occurrence of specific events (like accidents) for urgent emergency situations."[261] Describing Brain6, a more advanced integrated vehicle automation system that relies heavily on externally facing sensors, Mobileye CEO Amnon Shashua explained that, "crowdsourced mapping not only teaches Brain6 how to interpret road conditions everywhere, but also provides invaluable driving behavior insights."[262] To give a sense of the potential scale of data recording and sharing, Mobileye systems are currently found in 150 million cars worldwide.[263] By regularly updating the reference maps used by vehicles, the object detection system can reduce processing times and achieve the real-time speed needed for safe driving.[264]

---

259. Harry Surden & Mary-Anne Williams, *Technological Opacity, Predictability, and Self-Driving Cars*, 38 CARDOZO L. REV. 121, 180 (2016).

260. *E.g.*, Nick Gibbs, *Mobileye Says Modular Brain6 Software Opens New Possibilities*, AUTO. NEWS EUR. (Aug. 15, 2024, at 19:14 ET), https://europe.autonews.com/suppliers/mobileyes-modular-brain6-software-boosts-adas-infotainment [https://perma.cc/3UZQ-37LY].

261. *Opinion 03/2017 on Processing Personal Data in the Context of Cooperative Intelligent Transport Systems (C-ITS)—wp252*, EUR. COMM'N NEWSROOM 3 (Feb. 10, 2017), https://ec.europa.eu/newsroom/article29/items/610171 [https://perma.cc/YB46-ZQBT].

262. Gibbs, *supra* note 260.

263. *Id.* Dashcam provider, Nexar, for example, offers access to "130 million miles of crowd-sourced street-level visual data and 3.2 trillion images from roads, highways and cities all over the US." *Sample Imagery for AI Training Application Form*, NEXAR, https://info.getnexar.com/free_data_sample_application [https://perma.cc/7HBS-SGHP] (last visited Mar. 8, 2026).

264. Ambati Pravallika et al., *Deep Learning Frontiers in 3D Object Detection: A Comprehensive Review for Autonomous Driving*, *in* 12 IEEE ACCESS 173936, 1739374 (2024), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10670385&tag=1 [https://perma.cc/L6DJ-PZAL].

4. *Externally Facing Vehicle Sensors and Third-Party Privacy*

In the context of the third-party privacy problem, externally facing vehicle sensors process data from and about people outside of the vehicle (third parties) in service of people in the vehicle (first and second parties). The vehicle manufacturer, as the controller, deploys technologies that, at their core, must collect data from and about third parties to make vehicles function in a safe and legally compliant manner. The next Section explains how these technologies come under the AI Act.

B. From Externally Facing Vehicle Sensors to the AI Act

Object detection systems, localization and mapping functions, and sensor recording systems are key components in vehicle safety systems. The Vehicle General Safety Regulation (EU) 2019/2144 governs the approval requirements for safety systems in vehicles sold in the EU.[265] The implementing legislation issued pursuant to the Vehicle General Safety Regulation cover specific iterations of externally facing vehicle sensor systems as they constitute components of emergency lane-keeping systems, intelligent speed assistance systems, automated driving systems, and event data recorders.[266] The Vehicle Approval Regulation (EU) 2018/858 establishes the process of

265. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166, 2019 O.J. (L 44325) [hereinafter Vehicle General Safety Regulation].

266. General Safety Regulation—Secondary Legislation, (Aug. 28, 2022) https://ec.europa.eu/docsroom/documents/51154 [https://perma.cc/VK5E-VZJU].

third-party conformity assessments used for the safety systems governed under the Vehicle General Safety Regulation.[267]

Both the Vehicle General Safety Regulation and the Vehicle Approval Regulation are listed in Annex I, Part B of the AI Act.[268] Externally facing vehicle sensors, therefore, qualify as high-risk AI safety systems under the AI Act.[269] They are "used as . . . safety component[s] of a product," "covered by the . . . legislation listed in Annex I," and "required to undergo a third-party conformity assessment."[270] Figure 3 offers a sketch of these relationships.

Some of these high-risk AI safety systems are no longer optional for vehicles sold in the EU. As of July 2024, Vehicle General Safety Regulation requires that all new road vehicles must have advanced driver assistance systems that include "intelligent speed assistance" and "reversing detection with cameras or sensors."[271] In short, the AI Act can potentially regulate the effect that vehicle safety systems have on third party privacy. The next Part examines how.

---

267. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (Text with EEA relevance.), 2018 O.J. (L 151/1), Annex II (listing Regulation FILJ V.b.1c (EU) 2019/2144) [hereinafter Vehicle Approval Regulation].

268. EU AI Act, *supra* note 33, Annex I, Section B.

269. Though one might not think of externally facing sensors as artificial intelligence systems, they are key components of vehicle safety systems. For example, a reversing detection system is regulated under the AI Act but qualifies as Level 0 under SAE J3016 standard for driving automation. SAE J3016, *supra* note 3. Accordingly, any increase in the automation level of the vehicle would not change the classification of that vehicle system as a high-risk AI system under the AI Act. The data collection remains the same, its further processing simply changes. *See* Vehicle General Safety Regulation, *supra* note 265, recital 10. From the perspective of the AI Act, the future of driving automation is already here.

270. EU AI Act, *supra* note 33, art. 6(1)(a)–(b).

271. Eur. Comm'n, New Rules on Vehicle Safety and Automated Mobility (July 5, 2024), https://single-market-economy.ec.europa.eu/document/download/cd243af9-c877-401e-9f69-d7d4ab6a90c6_en [https://perma.cc/5ESK-QXT7].

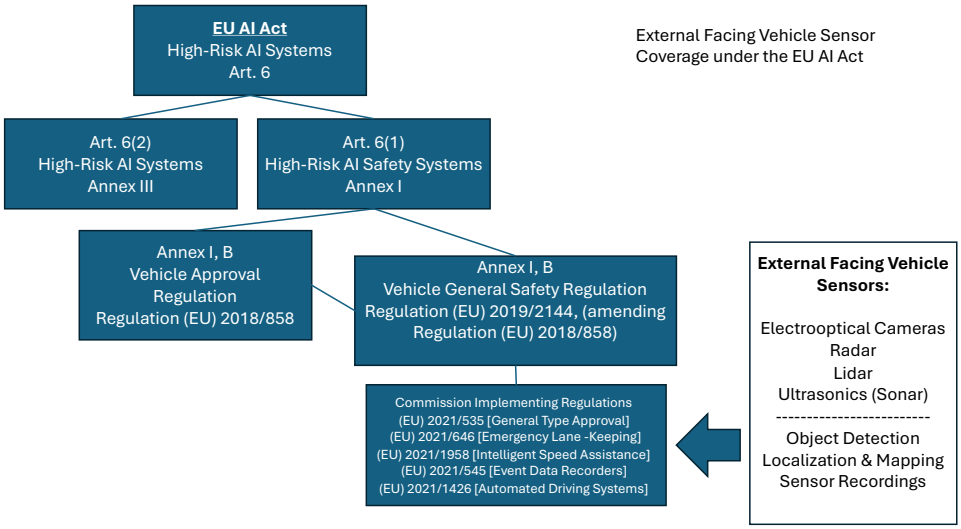

Figure 3

V. THIRD PARTY PRIVACY UNDER THE EU AI ACT

This Part proceeds in three Sections. The first Section frames the analysis of how vehicle safety systems can affect third-party privacy through the AI Act's data governance system. Applying that framework, the second Section explains how different legal regimes require the retention and sharing of data from vehicle safety systems. The privacy implications for third parties are discussed in turn. The third Section concludes, explaining how the AI Act's data governance system falls short of protecting the privacy interests of third parties.

A. Framing a Third-Party Privacy Analysis Under the AI Act

As discussed in Part II.B, the AI Act's risk management system provides opportunities to address the privacy interests of third parties. The provider of a high-risk AI system must "[identify] and analy[ze] . . . the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose."[272] Providers must also "estimate and evaluat[e]. . . the risks that may emerge when the high-risk AI system is used in accordance

272. EU AI Act, *supra* note 33, art. 9(2)(a).

with its intended purpose, and under conditions of reasonably foreseeable misuse."[273] This analysis applies these requirements to the third-party privacy problem in the context of vehicle safety systems. To frame this effort, the concepts of fundamental rights, intended purpose, health and safety, and misuse are discussed in turn.

Fundamental Rights. Fundamental rights represent a broad array of concepts.[274] This analysis will focus primarily on fundamental rights related to privacy and data protection as articulated in Articles 7 & 8 of the EU Charter of Fundamental Rights.[275]

Intended Purpose. "'[I]ntended purpose' means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation."[276] In the context of vehicle safety systems using externally facing sensors, vehicle manufacturers explain that these systems promote safety.[277] That includes the safety of the occupants of the vehicle[278] and others

---

273. *Id.* art. (9)(2)(b).

274. Fundamental rights jurisprudence in EU includes the concepts of ranking of interests and proportionality. Accordingly, a third party's rights to privacy and data protection may be subordinate to, or at least balanced against, other rights and interests such the right to life and intellectual property rights. A complete fundamental rights analysis is beyond the scope of this Article. Hopefully, though, this exploration of the privacy interests of third parties can support a more complete fundamental rights analysis of vehicle safety technologies.

275. Charter of Rights, *supra* note 39, arts. 7, 8.

276. EU AI Act, *supra* note 33, art. 3(12).

277. Each of the top sellers of vehicles in Europe referred to safety as a primary reason for installing increasingly automated systems in their vehicles. *E.g.*, *Iq.Drive*, VOLKSWAGEN, https://www.vw.com/en/iq-drive.html [https://perma.cc/QX45-QA9Z]; *Automated Driving*, TOYOTA, https://www.toyota-europe.com/innovation/zero-accidents/automated-driving [https://perma.cc/K3D7-MSN2]; *The Road to Autonomous Driving*, BMW GROUP, https://www.bmwgroup.com/ en/innovation/automated-driving.html [https://perma.cc/8G4K-MBGU]; *I Would Definitely Let a Machine Drive my Car*, SKODA CAREER BLOG (May 9, 2024), https://www.skoda-career.com/blog/i-would-definitely-let-a-machine-drive-my-car [https://perma.cc/2KT9-SSUF].

278. *E.g.*, *Adaptive Cruise Control*, VOLKSWAGEN, https://www.vw.com/en/iq-drive/adaptive-cruise-control.html [https://perma.cc/8VSX-WSNE].

on the roadway.[279] In short, evidence supports the claim that an intended use of these systems is "safer driving."[280]

Automated enforcement, even if it could promote safer driving, is not an intended purpose of these high-risk AI systems for the purposes of this analysis. "In theory, some of these companies [deploying vehicle safety systems] could already prevent speeding (by implementing intelligent speed control), report speeding (by notifying law enforcement), or penalize speeding (by banning offending users)."[281] Less speeding through automated enforcement could lead to safer driving. But vehicle manufacturers do not describe such automated enforcement as the intended purpose of their high-risk AI systems. Additionally, European privacy authorities have warned of the legal issues posed by sharing vehicle data with law enforcement authorities outside of traditional collection procedures.[282]

Health and Safety. Using externally facing sensors to promote safer driving also helps shape the understanding of the terms "health" and

---

279. *E.g.*, MERCEDES-BENZ, INTRODUCING DRIVE PILOT: AN AUTOMATED DRIVING SYSTEM FOR THE HIGHWAY 5 (Mar. 6, 2023).

280. A broader understanding of the "intended purpose" of these safety systems could also include promoting more driving. *See* Bryant Walker Smith, *Managing Autonomous Transportation Demand*, 52 SANTA CLARA L. REV. 1401 (2012). If vehicles can be driven over longer distances and for longer periods of time without compromising their own safety, or that of others on the roadway, then people are more likely to drive more. *See* Wolfgang Gruel & Joseph M. Stanford, *Assessing the Long-Term Effects of Autonomous Vehicles: A Speculative Approach*, 13 TRANSP. RSCH. PROCEDIA 23–27 (2016), https://www.sciencedirect.com/science/article/pii/S2352146516300035 [https://perma.cc/F9C7-K7NT]. This is part of the promise of increasingly automated vehicles. Benjamin von Bodungen & Hans Steege, *Liability for Automated and Autonomous Driving in Germany*, *in* AUTONOMOUS VEHICLES AND CIVIL LIABILITY IN A GLOBAL PERSPECTIVE: LIABILITY LAW STUDY ACROSS THE WORLD IN RELATION TO SAE J3016 STANDARD FOR DRIVING AUTOMATION 279, 310 (Hans Steege et al. eds., 2024). This benefits the vehicle manufacturers. But vehicle manufacturers deploying these high-risk AI systems do not specifically market them as a means of getting more people to drive their vehicles, well, more. "More driving," therefore, is not an intended purpose of these high-risk AI systems for the purposes of this analysis.

281. Bryant Walker Smith, Jeffrey Michael & Johnathon Ehsani, *Ideal Enforcement: How Do We Achieve Optimal Enforcement of Traffic Law as Ubiquitous Enforcement Becomes Technologically Conceivable?*, 30 MICH. TECH. L. REV. 1, 7 (2024).

282. EDPB CONNECTED VEHICLES, *supra* note 5, at 14; COMM'N NATIONALE INFORMATIQUE & LIBERTÉS, COMPLIANCE PACKAGE: CONNECTED VEHICLES AND PERSONAL DATA (Oct. 2017) [hereinafter CNIL COMPLIANCE PACKAGE].

"safety" in this analysis.[283] Policy discourse attributes several meanings to the terms "health" and "safety."[284] Health may refer to public health,[285] environmental sustainability,[286] or even appropriate levels of competition in the markets.[287] Safety may mean freedom from fear of physical attack,[288] housing security,[289] or even economic well-being.[290] By focusing on the use of externally facing sensors in vehicles "in accordance with . . . [their] intended purpose,"[291] a narrower definition of health and safety emerges.

The definitions of health and safety consistent with the intended purpose of using externally facing sensors to promote safer driving refers to a concept this Article calls *kinetic safety*. "Kinetic safety" means freedom from physical injuries to persons or their property resulting from collision with vehicles in motion under their own power on and around the roadway. Kinetic safety considers the safety of a vehicle's driver and occupants, occupants of other vehicles, as well as the safety of others along the roadway, such as pedestrians and

283. EU AI Act, *supra* note 33, art. 9(2)(a).

284. *See The Future of Self-Driving Cars: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 119th Cong. (2026) (answers to questions for the record of Professor Bryant Walker Smith), https://newlypossible.org/files/2026SenateAnswers.pdf [https://perma.cc/JPJ9-U5YE].

285. *E.g.*, *Guiding Statements*, ARNOLD SCH. PUB. HEALTH, https://www.sc.edu/study/colleges_schools/public_health/about/guiding_statements/index.php [https://perma.cc/6UJ5-NKXT].

286. *See, e.g.*, Marie S. O'Neill et al., *Poverty, Environment, and Health: The Role of Environmental Epidemiology and Environmental Epidemiologists*, 18 EPIDEMIOLOGY 664, 644 (Nov. 2007).

287. *See, e.g.*, Wolfgang Kerber, *Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data*, 9 J. INTELL. PROP., INFO. TECH. & ELEC. COM. L. 310, 311 (2018) (discussing the absence of market health, market failures).

288. COMM'N STUDY, *supra* note 46, at 57 (discussing "perceived safety" as an important factor in women's mobility needs).

289. *See, e.g.*, MARTHA GALVEZ, MAYA BRENNAN, BRADY MEIXELL & ROLF PENDALL, URBAN INST., HOUSING AS A SAFETY NET *passim* (Sep. 2017).

290. *See, e.g.*, STEVEN D. BROWN ET AL., NOTTINGHAM BUS. SCH., PSYCHOLOGICAL WELLBEING AND SAFETY IN A GLOBAL CONTEXT: A RAPID EVIDENCE ASSESSMENT *passim* (2020).

291. EU AI Act, *supra* note 33, art. 9(2)(a).

cyclists. It aims to exclude incidents[292] and crashes that are not part of typical vehicle uses or roadway activities.[293]

Kinetic safety aligns with some of the goals of the EU's vehicle approval and safety regulations, namely avoidance of fatalities and severe injuries[294] and "market surveillance . . . to ensure that vehicles . . . do not endanger [the] health, [and] safety"[295] of roadway users. Kinetic safety, though, expressly excludes other considerations such as "the proper functioning of the internal market,"[296] "environmental performance,"[297] or endangering the "environment or any other aspect of public interest protection."[298] All of these ideas may represent health and safety interests in the public policy discourse,[299] but they are beyond the scope of kinetic safety intended by using externally facing vehicle sensors as part of high-risk AI safety systems. This understanding of kinetic safety also helps define the scope of "reasonably foreseeable misuse."

Misuse. Under the AI Act, "'reasonably foreseeable misuse' means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems, including other AI systems."[300] The most problematic forms of misuse relate to exploiting cybersecurity vulnerabilities in increasingly automated vehicle systems.[301] But providers of high-risk AI systems must already

---

292. *E.g.*, M.O. v. GEICO Gen. Ins. Co., 657 S.W.3d 215 (Mo. 2023) (en banc).

293. *E.g.*, Tammy Eastwick, *Vehicle Falls Off Car Carrier, Causing Wreck on I-55*, 16 ABC WAPT (July 24, 2013, at 18:55 ET), https://www.wapt.com/article/vehicle-falls-off-car-carrier-causing-wreck-on-i-55/2084767 [https://perma.cc/9SR3-HLWX].

294. Vehicle General Safety Regulation, *supra* note 265, recital 3.

295. Vehicle Approval Regulation, *supra* note 267, art. 3(34).

296. Vehicle General Safety Regulation, *supra* note 265, recital 1.

297. *Id.*

298. Vehicle Approval Regulation, *supra* note 267, art. 3(34).

299. Walker Smith et al., *supra* note 281, at 8–9.

300. EU AI Act, *supra* note 33, art. 3(13).

301. Mansi Girdhar, Junho Hong & John Moore, *Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models*, *in* 4 IEEE OPEN J. VEHICULAR TECH. 417 (2023), https://ieeexplore.ieee.org/document/10097455; U.S. DEP'T OF TRANSP.,

footnote continued on next page

account for cybersecurity risks,[302] and vehicle manufacturers, specifically, have a duty to "protect[] against unauthorised use including cyberattacks."[303] Accordingly, within the scope of the AI Act, "reasonably foreseeable misuse" likely means use of high-risk AI systems that do not involve compromising cybersecurity.

Rather, misuse likely means use of vehicle safety systems, or their externally facing sensors, within their operational parameters but towards improper ends. In other words, while still promoting kinetic safety, how could data from externally facing sensor systems cause harm? In the context of the third-party privacy problem, reasonably foreseeable misuse could mean using data from vehicle safety systems to identify third parties while not otherwise violating the law.

B. Two Types of Third-Party Data Production from High-Risk AI Safety Systems

The laws and policies that address the intended purpose of promoting kinetic safety of the roadway extend well beyond vehicle type approval regulations. Tort liability, product liability, and other data sharing requirements all serve the intended purpose of promoting kinetic safety on the roadway. These laws and policies ask vehicle manufacturers to provide data from and about third parties to a wide range of actors. Because sharing outputs from AI systems furthers the intended purpose of promoting kinetic safety, it represents "reasonably foreseeable risks that the high-risk AI system[s] can

---

NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES (Oct. 2016), https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf [https://perma.cc/7CM4-UFWA].

302. EU AI Act, *supra* note 33, art. 15.

303. Vehicle General Safety Regulation, *supra* note 265, art. 4(5)(d); *see also id.* at Annex II(D). Other potentially applicable laws have their own cybersecurity requirements. *See* GDPR art. 32; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L 201) art. 4; Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), 2023 O.J. (L Series), arts. 4(2) & 6(2)(f) [hereinafter Data Act].

pose."[304] Understanding "the entire lifecycle of a high-risk AI system"[305] therefore includes an assessment of how these data will be used by others who receive the AI system's output. Misuse would arise if recipients of these data used them to reidentify third parties.[306] As discussed above, identifiability analysis under GDPR considers the capabilities of the parties receiving the data. Those capabilities include characteristics of the data, legal requirements mandating its sharing, available technologies, and access to additional data.[307]

Taking all these factors together, two distinctive systems emerge that govern the sharing of vehicle data from and about third parties.[308] This Article calls these the *proximate* and *iterative* safety systems. These systems interrelate because the same data flow through both of

304. EU AI Act, *supra* note 33, art. 9(2)(a).

305. *Id.* art. 9(2).

306. In recent years, manufacturers have attracted government attention for their mismanagement of vehicle data at the expense of their customers' privacy. *E.g.*, Dimitrios Papadimoulis, *Collection and Sale of Personal Data by Car Companies*, EUROPEAN PARLIAMENT: PARLIAMENTARY QUESTIONS (Sep. 28, 2023), https://www.europarl.europa.eu/doceo/document/E-9-2023-002847_EN.html [https://perma.cc/87FW-Y54R]; Kosma Złotowski, *Low Levels of Data Protection and Consumer Privacy in the Automotive Sector*, EUROPEAN PARLIAMENT: PARLIAMENTARY QUESTIONS (Sep. 18, 2023), https://www.europarl.europa.eu/doceo/document/E-9-2023-002684_EN.html [https://perma.cc/C76H-FVF7]; Federal Trade Commission Office of Technology and the Division of Privacy and Identity Protection, *Cars & Consumer Data: On Unlawful Collection & Use*, FED. TRADE COMM'N TECH. BLOG (May 14, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use [https://perma.cc/9YED-6ZKB]. If those practices extend to the context of the third-party privacy problem, then vehicle manufacturers themselves would be using external sensor data to identify third parties. *E.g.*, Nina Theobald, Philip Joisten & Bettina Abendroth, *Measuring Pedestrians' Gap Acceptance When Interacting with Vehicles—A Human Gait Oriented Approach*, *in* HCII 2022: COMMUNICATIONS IN COMPUTER AND INFORMATION SCIENCE (Constantine Stephanidis, Margherita Antona & Stavroula Ntoa eds, 2022). If such identification were unnecessary to promote kinetic safety, it would be an incident of misuse by the vehicle manufacturer itself. If that were to occur, third parties would become first parties, and GDPR would apply. *See supra* note 193 and accompanying text.

307. *See supra* Part V.B.

308. *See supra* note 151 and accompanying texts.

them.[309] But the interplay between the parties' lawful means of promoting kinetic safety and their respective capabilities for misuse of the data help form the borders of these different systems.[310]

The *proximate safety* system deploys technologies aimed at preventing direct (real-time) kinetic contact between a vehicle and others on the roadway. These technologies generate data to inform the vehicle's safety systems so that they, or the human driver, can avoid kinetic contact. Connected car technologies, though not widely used, form part of the proximate safety system. The goal of kinetic safety justifies sharing almost any data deemed helpful in preventing kinetic safety issues. The laws in the proximate safety system require sharing as much of these data as possible to adjudicate incidents of kinetic contact. Misuse of the data by any of the parties involved in the adjudication process would allow for the identification of third parties, potentially in real time.

The *iterative safety* system takes these data from the proximate safety system, adds its own storage capabilities, and shares these data via several technologies. The iterative safety system aims to make vehicles safer on the roadway by improving the function of proximate safety technologies. By sharing these data, multiple parties can improve the capabilities of vehicles' safety systems in avoiding kinetic safety incidents. The required recipients in the iterative safety system include parties maintaining vehicles, assessing product liability, serving as market regulators, and others competing in the vehicle and vehicle data markets. These data tend to be shared in an "anonymous" format and may be aggregated. But the participants in the iterative safety system have common technological capabilities and access to similar sets of additional data as well. Misuse of the data would allow

309. And the free movement of that data is possibly enabled by the same software architecture. *See* Balayn & Gürses, *supra* note 55.

310. These two systems track closely with the privacy norms around automated vehicles identified by Cara Bloom and Josiah Emery. *See* Bloom & Emery, *supra* note 2. Norms around fault correspond to the proximate safety system. The iterative safety system focuses on the safety of automated vehicles. *Id.* at 1652. The MIT Moral Machine experiment, famously, also tried to identify social norms around automated driving. But those norms focused on life-and-death situations, and not the broader questions in Bloom & Emery's work. Edmond Awad et al., *The Moral Machine Experiment*, 563 NATURE 59, 59 (2018).

for identification of third parties within otherwise-anonymous data sets.

In the future, data may move freely among these systems in real time,[311] limiting the value of these distinctions. But these categories help explain data flows within today's vehicle data environment.[312] Accordingly, this analysis hews closely to the requirements established by the data governance systems in the AI Act. The next Section explores each of these systems and their potential impact on third party privacy.

1. *Proximate Safety*

a. *Applicable Laws & Technologies*

Traffic laws across Europe require a series of driving behaviors that reduce the risk of kinetic contact.[313] Congruent with these laws, AI technologies deployed in vehicle safety systems also aim to reduce the likelihood that vehicles collide with objects in the roadway, either by warning the driver or by controlling the vehicle to avoid a collision.[314] In short, if all drivers and vehicles do what they are supposed to do, the chances of kinetic contact on the roadway are very small.

---

311. *See* Determann & Perens, *supra* note 5; Gruel & Stanford, *supra* note 280; Guy Seidman & Aviv Gaon, *A Future Without Human Driving*, 18 GEO. J.L. & PUB. POL'Y 503, 508–10 (2020); Zheng et al., *supra* note 257, at 2.

312. An argument could be made for a third system: The ambient safety system. In that system, data from externally facing vehicle sensors helps inform decisions that make the roadway safer for vehicles. There are some instances where vehicle manufacturers may have to share vehicle data with government authorities to those ends. *See* Straßenverkehrsgesetz (StVG) [Road Traffic Act], § 1g Datenverarbeitung [Data Processing] (2019) https://www.gesetze-im-internet.de/stvg/__1g.html [https://perma.cc/U4X4-QD4F] (Ger.). These requirements fall within the scope of legal incentives for further processing described by the third-party privacy problem. But these laws are not pervasive enough to fall under the "intended purpose" or "reasonably foreseeable misuse" frames established by the AI Act. Accordingly, the analysis of the ambient safety system and its data flow are reserved for a future work, Sella-Villa, *Towards a Political Economy of Third Party Privacy*, *supra* note 88.

313. *E.g.*, D.L. 30 April 1992, n.285, G.U. May 18, 1992, n.114 (It.).

314. *See supra* Part IV.A.3.

To help ensure that vehicle safety systems operate as intended,[315] vehicle type regulations set minimum standards for vehicle safety.[316] With regards to the AI systems in question, the Vehicle General Safety Regulation broadly requires that covered manufacturers "ensure that vehicles are designed, constructed and assembled so as to minimize the risk of injury to vehicle occupants and vulnerable road users."[317] These rules and practices affect which vehicle safety systems may deploy in the moments before and after a collision. Some countries set additional standards for type approval of vehicles with higher levels of automation.[318] In Germany, for example, various provisions suggest that the vehicle record specific information about when, where, and under what conditions the disengagement of the automated system takes place, independent of whether the vehicle is involved in a collision.[319]

This data retention requirement builds on the provisions regarding event data recorders in the Vehicle General Safety Regulation. Event data recorders are required to store information for the "period [of time] shortly before, during, and immediately after a collision."[320] They are required to record whether automated vehicle systems are operating in the event of a collision.[321] Because a collision can happen at any time, event data recorders must operate continuously, cannot be disabled, and must ensure a "high level of accuracy and ensured

315. And that drivers operate the vehicles within the safe operating parameters of those safety systems. von Bodungen & Steege, *supra* note 280, at 311 ("It is reasonable to assume that product user's legitimate safety expectations will also be shaped by these legal design specifications.").

316. *Id.*

317. Vehicle General Safety Regulation, *supra* note 265, art. 4(4).

318. von Bodungen & Steege, *supra* note 280, at 285–86.

319. Straßenverkehrsgesetz (StVG) [Road Traffic Act], § 1g Datenverarbeitung [Data Processing] (1)(8) (2019), https://www.gesetze-im-internet.de/stvg/__1g.html [https://perma.cc/U4X4-QD4F] (Ger.); *id.* § 63a [Data Processing for Motor Vehicles with Highly or Fully Automated Driving Functions], https://www.gesetze-im-internet.de/stvg/__1g.html [https://perma.cc/4G6C-Y5AS] (Ger.).

320. Vehicle General Safety Regulation, *supra* note 265, art. 6(4)(a).

321. UN Regulation No 160—Uniform Provisions Concerning the Approval of Motor Vehicles with Regard to the Event Data Recorder [2021/1215], 2021 O.J. (L 265), Annex 4.

survivability of the data."[322] Guidance from the United Kingdom suggests that event data recorders should store information for at least "30 seconds before the . . . [collision], and 15 seconds after [it.]"[323] In the narrower context of "accidentology studies," the French data protection authority recommends storing "recordings of the 45 seconds before the reference event or sequence, and of the 15 seconds after the reference event or sequence."[324] In short, though constantly recording, only a short period of time should be captured by the vehicle's event data recorders.

Separate systems record, potentially indefinitely,[325] the data collected and processed by externally facing sensors.[326] The German Autonomous Driving Act also requires the recording of "data on . . . the instance that triggered the safety system."[327] To use the object detection system as an example, information generated by externally facing sensors about features of the roadway would be recorded as the "data . . . that triggered the safety system."[328] The German Autonomous Driving Act, however, offers no guidance on when such information may be deleted.[329]

These data recordings serve an important role in the proximate safety system. Criminal enforcement is typically reserved for egregious violations, like reckless driving or driving while impaired by drugs or alcohol. Tort law functions as the primary legal enforcement mechanism for collision avoidance.[330] The mandatory insurance system

322. Vehicle General Safety Regulation, *supra* note 265, art. 6(4)(a).

323. *Code of Practice: Automated Vehicle Trialling*, GOV.UK (Nov. 30, 2023), https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public/code-of-practice-automated-vehicle-trialling [https://perma.cc/N4X8-UDYR].

324. CNIL COMPLIANCE PACKAGE, *supra* note 282, at 25.

325. *See supra* Part IV.A.3.

326. MERCEDES-BENZ, *supra* note 279, at 48.

327. *See* Straßenverkehrsgesetz (StVG) [Road Traffic Act], § 1g Datenverarbeitung [Data Processing] (1)(8) (2019), https://www.gesetze-im-internet.de/stvg/__1g.html [https://perma.cc/U4X4-QD4F] (Ger.).

328. *Id.*

329. *See id.* art. 1g.

330. *See* de Bruin, *supra* note 6, at 494.

and the courts sort out liability after most collisions.[331] "The data recorded in [the vehicle] might be critical to clarify the conditions of an accident to allocate responsibility."[332] Keeping the driver potentially liable has direct consequences on the design and operation of the proximate safety system.[333] If the vehicle operates as intended, then, relative to the AI system, the driver likely bears full responsibility.[334] If the vehicle does not operate as intended, then the vehicle manufacturer may be liable under a theory of product liability.[335] Data recordings from a vehicle's external sensors can help in the resolution of these questions. The data recorded in vehicles, therefore, play an important role in the design and function of both the legal and technical components of the proximate safety system.

b. Third Party Privacy Assessment

To help avoid collisions, externally facing sensor systems observe the world around the vehicle. Electrooptical camera systems identify the presence of people and their property on, and visible from, the roadway. Active sensors take measurements of the same. These data streams inform the actions of vehicle AI safety systems. Additionally, because of their ability to enable perception beyond barriers that prevent visual observation, like the corner of a building, a fence, or a hedgerow, some externally facing sensors can collect information about an individual's "private . . . life [or] home."[336]

This information about others on the roadway likely meets the definition of personal data under the GDPR. Under the GDPR,

---

331. *See* Belinda Bennett, Jane Evelyn & Bridget Weir, *Driving into New Frontiers: Data and Driverless Cars*, U. NEW S. WALES L.J.F. art. no. 8, at 12 (2019) https://eprints.qut.edu.au/133478/ [https://perma.cc/B4A4-44GG].

332. Antonios E. Kouroutakis, *Autonomous Vehicles: Regulatory Challenges and the Response from Germany and UK*, 46 MITCHELL HAMLINE L. REV. 1103, 1117 (2020).

333. Crootof et al. *supra* note 58, at 437 ("Tort rules, though not intended to affect the design or operation of the hybrid system, profoundly shape its dynamics.").

334. *Id.*

335. von Bodungen & Steege, *supra* note 280, at 300–01.

336. Charter of Rights, *supra* note 39, art. 7. These observations of private life made incidentally while "protect[ing] the rights and freedoms of others" by avoiding collisions, are likely consistent with the Charter of Rights' principle of proportionality. *Id.* art. 52(1).

"'personal data' means any information relating to an identified or identifiable natural person."[337] The images and measures of pedestrians, cyclists, other vehicles, their drivers and occupants, and property adjacent to the roadway constitute "any information."[338] The European Court of Justice has found that information "relates" to a data subject "where the information, by reason of its content, purpose or effect, is linked to a particular person."[339] Alone, data from externally facing sensors have the effect of linking the presence of a person or their property to a vehicle in their proximity. In combination with other information—GPS coordinates, proximity to a known landmark, or even a road sign—externally facing sensor data can link a data subject to a location at a particular time. In the context of an incident involving the person and the vehicle, the effect is to help identify the person for purpose of dispute resolution.

Data protection authorities in Europe support this interpretation. The Swedish Privacy Authority has found that lidar data can be personal data under the GDPR.[340] As a core function, certain vehicle safety systems, like object detection, classify information about the world around the vehicle. In its recommendations on the ethics of connected vehicles, the European Commission found that such ad hoc groupings of information about third parties may still qualify as personal data.[341] In its review of the Mercedes Drive Pilot system, the Data Protection Authority of Baden-Württemberg noted that the

337. GDPR, supra note 11, art. 4(1).

338. *See* Nowak v. Data Prot. Comm'r, Case C-434/16, 2017, ¶ 34, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CN0434&qid=1775429466487 [https://perma.cc/GN4X-9VK9].

339. *Id.* paras. 34–35.

340. Integritetsskydds myndigheten, IMY-2024-1650, English Summary: The Swedish Authority for Privacy Protection, IMY, Finishes its Second Regulatory Sandbox Pilot (2024), https://www.imy.se/globalassets/dokument/rapporter/english-summary---the-swedish-authority-for-privacy-protection-imy-finishes-its-second-regulatory-sandbox-pilot.pdf [https://perma.cc/LU9C-NPNF].

341. *See European Commission Independent Expert Report*, Ethics of Connected and Automated Vehicles: Recommendations on Road Safety, Privacy, Fairness, Explainability, and Responsibility 40 (2020), https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en [https://perma.cc/9TXK-Q56Y].

vehicle's externally facing sensors initially capture personal data.[342] In short, data from vehicles' externally facing sensors are fundamentally data about people or their property. As such, data from externally facing sensors implicate third parties' rights "to the protection of personal data."[343] In the context of dispute resolution regarding incidents involving these people and the vehicle, identifiability of a third party is all but assured.

But this is not necessarily a problem for a driver operating a vehicle in a personal capacity.[344] If the data are processed, and no recordings are maintained[345]—as in the case of some event data recorders—then the driver probably qualifies for the "personal processing" exemption under the GDPR.[346] Even if the data are recorded, but the driver never accesses them, then the personal processing exception would probably still apply.[347] Though personal data about third parties would exist, they would be inaccessible, and

---

342. DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT, DATENSCHUTZ + DIGITALISIERUNG = NACHHALTIGE ENTWICKLUNG: UNSERE FREIHEITEN: DATEN NÜTZEN – DATEN SCHÜTZEN: TÄTIGKEITSBERICHT DATENSCHUTZ 105 2022 [THE STATE COMM'R FOR DATA PROT. & FREEDOM OF INFO., DATA PROTECTION + DIGITALISATION = SUSTAINABLE DEVELOPMENT: OUR FREEDOMS: USE DATA–PROTECT DATA: ANNUAL REPORT DATA PROTECTION 105 (2022)], https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2023/02/TB_38_Datenschutz-2022_V1-.pdf [[hereinafter BADEN-WÜRTTEMBERG 2022 DPA REPORT].

343. Charter of Rights, *supra* note 39, art. 8.1.

344. The analysis would be different for someone operating a vehicle in a commercial capacity. *See* EDPB CONNECTED VEHICLES, *supra* note 5; CNIL COMPLIANCE PACKAGE, *supra* note 282.

345. *See* George et al., *supra* note 103.

346. GDPR, supra note 11, art. 2(2)(c); *see also* EDPB CONNECTED VEHICLES, *supra* note 5, at 19; CNIL COMPLIANCE PACKAGE, *supra* note 282, at 20.

347. *See* Joint Statement, Conference of the Independent Data Protection Authorities of the Federal and State Governments of Germany and the German Association of the Automotive Industry (VDA), Data Protection Aspects of Using Connected and Non-connected Vehicles 2 (Jan. 26, 2016), https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf [https://perma.cc/Q6JC-L3Z5] [hereinafter Joint Statement]; Tanja Kammersgaard Christensen, *Pre-installed Cameras in Vehicles—New Technology from a Data Protection Law Perspective*, 53 COMPUT. L. & SEC. REV., THE INT'L J. TECH. L. & PRACT. art. no. 105980, at 8 (July 2024). *But see id.* at 3 (discussing the potential limits of the personal processing exception).

therefore of minimal concern relative to the privacy interests of third parties.[348]

The Vehicle General Safety Regulation supports the idea that certain data collected by externally facing vehicle sensors fall outside the scope of GDPR. Under GDPR, "[t]he principles of data protection . . . [do] not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[349] The Vehicle General Safety Regulation requires that the information in event data recorders be "anonymised and protected against manipulation and misuse."[350] Accordingly, by avoiding the creation of or limiting access to personal data, these features of the proximate safety system protect a third party's fundamental right "to the protection of personal data."[351]

Multiple parties, though, can access data recorded by vehicles' externally facing sensors after a collision.[352] When determining liability, the parties involved in the collision have already been identified. Accordingly, the information accessed from an event data recorder clearly "relat[es] to . . . identified natural . . . person[s]."[353] The use of personal data in this context, though, does not necessarily impinge on data privacy rights. Article 8.2 of the EU Charter allows for the processing of personal data if it is done "fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[354] Assuming the specified purpose of adjudicating liability after a collision, the processing of personal data from an event recorder can proceed based on consent. Alternatively, the "legitimate basis laid down by law" to justify processing may be the evidentiary rules of the court. [355]

---

348. Aulino et al., *supra* note 5, at 257.
349. GDPR, *supra* note 11, recital 26.
350. Vehicle General Safety Regulation, *supra* note 265, art. 6(4)(c)(ii).
351. Charter of Rights, *supra* note 39, art. 8.1.
352. *See* Kouroutakis, *supra* note 332 and accompanying text; *see infra* Part V.B.1.a.
353. GDPR, *supra* note 11, art. 4(1).
354. Charter of Rights, *supra* note 39, art. 8.1.
355. *Id.*

In the context of the proximate safety system, parties affected by the kinetic contact will always be able to identify themselves in the data. Data from externally facing sensors, accordingly, probably come closest to meeting the GDPR definition of pseudonymous data.[356] "'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information."[357] Pseudonymous data are still personal data.

But unlike the GDPR definition that requires the party processing the data to use "technical and organisational measures" to keep "such additional information . . . separate[],"[358] the third party being observed has the additional information. Under the GDPR, data subjects have a right to access data about themselves.[359] Accordingly, there is no "technical [or] . . . organizational measure . . ."[360] that can prevent the possible reidentification of these data.[361] To borrow a concept from chemistry, a third party's access request acts as a free radical,[362] transforming otherwise unidentifiable data in a vehicle into personal data about the third party and, potentially, anyone else observed at that time.[363]

A Danish case illustrates the issue. "[A] young police officer was hit by a car while on duty, and the prosecution presented a video from

---

356. GDPR, *supra* note 11, art. 4(5).

357. *Id.*

358. *Id.*

359. GDPR, *supra* note 11, art. 15.

360. *Id.* art. 4(5); *see also* CNIL COMPLIANCE PACKAGE, *supra* note 274, at 29.

361. *Cf.* Gürses & van Hoboken, *supra* note 51, at 597 ("The conflation of user intentions with observations of their actions raises a fundamental question of what it means to consider users as stakeholders in the governance of services.").

362. *See, e.g.*, *Free Radicals*, LIBRETEXTS CHEMISTRY, https://chem.libretexts.org/Bookshelves/Organic_Chemistry/Supplemental_Modules_(Organic_Chemistry)/Fundamentals/Reactive_Intermediates/Free_Radicals [https://perma.cc/2CZT-HJVK] (last visited Dec. 6, 2024).

363. *See* Joint Statement, *supra* note 347, at 1 ("And, especially when further information is added, the data generated may be linked . . . and may contain information about the personal or material circumstances of an identifiable person."); *see also* Veale, *supra* note 9, at 10–11; *supra* Part II.A (discussing the concept of second parties).

a Tesla that filmed the collision as part of the evidence."[364] Because the data were recorded, they were linked to the police officer, and anyone else involved with the incident. Without other rules limiting its collection, storage, access, and use, access rights under the GDPR apply to externally facing sensor data stored in a vehicle.

Other elements of the proximate safety system facilitate misuse. Some recordings of externally facing sensor data do not have anonymization requirements and may be stored indefinitely.[365] Some of these data may be shared continuously through connected vehicle systems.[366] The longer the data are available in a vehicle, the more parties that have access to them, [367] and the more likely it is that the data can be used to "relat[e] to an identified or identifiable natural person."[368] This means that any party receiving data via a proximate safety system only needs to identify one third party to enable a chain reaction of identifiability.

For a third party's personal data to be processed in a manner consistent with Article 8.2 of the EU Charter, it "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[369] Because externally facing sensors observe the world around the vehicle, it is not possible to obtain consent from every person whose data are

364. Christensen, *supra* note 347, at 9.

365. Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 Laying Down Rules for the Application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as Regards Uniform Procedures and Technical Specifications for the Type-Approval of the Automated Driving System (ADS) of Fully Automated Vehicles, O.J. (L 221/15) Annex II, secs. 9.6.1 note 4, 9.1.8 & 9.7; *EQS Drive Pilot Supplement* +, MERCEDES-BENZ [13], https://www.mbusa.com/content/dam/mb-nafta/us/owners/drive-pilot/EQS%20DRIVE%20PILOT%20Supplement.pdf [https://perma.cc/KM5D-3R3U] (staff-uploaded); *see* Gibbs, *supra* note 260; Glancy, *supra* note 9, at 1197 ("Personal data retained indefinitely beyond the awareness of the person who is the subject of the information is a nightmare scenario.").

366. *E.g.*, Livia Aulino, *Human Machine Interaction and Legal Information in the Autonomous Vehicles: The Opportunity of the Legal Design*, 2 EUR. J. PRIVACY L. & TECH. 275, 275 (2020).

367. Bennett et al., *supra* note 331, at 6.

368. GDPR, *supra* note 11, art. 4(1).

369. Charter of Rights, *supra* note 39, art. 8.2.

being processed.[370] Even if this were possible, some have argued that fellow motorists, pedestrians, and other users of the roadway would not consent to such collections of personal data.[371] In the context of the proximate safety system, the legitimate basis of promoting fundamental rights impacted by kinetic contact on the roadway (and adjudicating fault after such collisions) supports the kind of data processing that takes place with event data recorders that only retain short recordings for a brief period of time. In terms of GDPR compliance, these unconsented recordings may be lawful under Article 6(1)(c), where processing "is necessary for compliance with a legal obligation to which the controller is subject."[372]

The need to adjudicate kinetic contact on the roadway does not support the kind of processing of third-party personal data that occurs when sensor data can be stored indefinitely and potentially used beyond the context of the proximate safety system. The German Autonomous Driving Act could serve as a basis for the collection and storage of third-party personal data beyond the storage limits set for certain data in event data recorders.[373] Mercedes vehicles with the Drive Pilot system, for example, used a separate event data recorder just for sensor data.[374] In the context of the fundamental privacy rights impacted by proximate safety systems, that may be enough of a legal obligation to justify processing under GDPR Article 6(1)(c). As discussed below,[375] such laws, however, may not be enough to address

370. Aulino, *supra* note 366, at 282; EDPB CONNECTED VEHICLES, *supra* note 5, at 14.

371. Maria Cristina Gaeta, *Data Protection and Self-Driving Cars: The Consent to the Processing of Personal Data in Compliance with GDPR*, 24 COMM. L., 2019, at 15, 17–19; Kouroutakis, *supra* note 332, at 1113.

372. GDPR, *supra* note 11, art. 6(1)(c).

373. Straßenverkehrsgesetz (StVG) [Road Traffic Act], § 1g Datenverarbeitung [Data Processing] (1)(8) (2019), https://www.gesetze-im-internet.de/stvg/__1g.html [https://perma.cc/U4X4-QD4F] (Ger.); Datenverarbeitung [Data Processing for Motor Vehicles with Highly or Fully Automated Driving Functions] 63a (2019), https://www.gesetze-im-internet.de/stvg/__1g.html [https://perma.cc/4G6C-Y5AS] (Ger.); *see supra* note 365 and accompanying text.

374. MERCEDES-BENZ, *supra* note 365.

375. *See infra* Part V.B.2.

all of the privacy interests impacted by externally facing sensor data stored for longer periods of time.

In jurisdictions that do not have a law requiring vehicle AI safety systems to store data beyond the limits set for event data recorders,[376] the lawful basis for processing personal data could be met under GDPR Article 6(1)(f).[377] In relevant part, it states that "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data."[378] This provision starts with a balancing test similar to the one implied by Article 8.2 of the EU Charter,[379] but the GDPR provisions place a proverbial thumb on the scale in favor of the "interest or fundamental rights and freedoms of the data subject."[380] The processing of third parties' personal data beyond the limits set for event data recorders does little to advance an individuals' rights that are impacted by roadway collisions.[381] Such processing, though, impacts an individual's "right to respect for his or her private . . . life, [and] home."[382] Therefore, processing third parties' personal data beyond the short time limits needed for event data recorders likely does not meet GDPR Article 6(1)(f) standard for lawful data processing. In the context of the proximate safety system, such processing likely does not comply with GDPR.

In absence of GDPR compliance, processing externally facing sensor data beyond the limits set for event data recorders likely does not have a "legitimate basis laid down by law."[383] Such processing, therefore, potentially violates an individual's fundamental privacy

376. Which would satisfy lawful bases for data processing under GDPR Article 6(1)(c)–(e).

377. Funta, *supra* note 9, at 114.

378. GDPR, *supra* note 11, art. 6(1)(f).

379. Charter of Rights, *supra* note 39, art. 8.2.

380. GDPR, *supra* note 11, art. 6(1)(f).

381. Charter of Rights, *supra* note 39, art. 2.1 ("right to life"); *id.* art. 3.1 ("right to respect for his or her physical and mental integrity").

382. *Id.* art. 7

383. *Id.* art. 8.2.

rights per EU Charter Article 8.2. The iterative safety system, though, may offer just such a legal basis.

2. Iterative Safety

a. Applicable Laws & Technologies

In their fundamental function, all parts of the iterative safety system gather data from similar circumstances over time. In the interest of avoiding kinetic contact, AI safety features in vehicles may exceed human performance standards for repetitive tasks, like lane-keeping.[384] Onboard analytics aim to make these repetitive tasks even better over time.[385]

Most self-learning features process data about third parties over extended periods of time. Waymo, which develops and deploys highly automated vehicles, has indicated that its most advanced automated systems use data from multiple vehicles to "learn[] from the collective experiences gathered across our fleet."[386] Mapping and localization features also benefit from externally facing sensor data shared among vehicles. They update the maps in the vehicle software, potentially in real-time. More accurate maps lead to faster computations and faster reaction times from the safety systems, thereby improving kinetic safety.[387]

Externally facing sensor data, in combination with other vehicle data, also allow vehicle safety systems to learn from "near-misses." Near-misses represent scenarios that narrowly avoid kinetic contact, like hard braking and swerving.[388] By learning from near-misses, AI-safety systems can be improved (through self-learning,[389] periodic

384. Crootof et al., *supra* note 58, at 438.

385. Ellen Kim et al., *Vision Zero: A Toolkit for Road Safety in the Modern Era*, 4 INJURY EPIDEMIOLOGY 1, 7 (2017).

386. Jay Ramey, *Waymo's Next-Gen Robotaxi Could Face a Big Barrier*, AUTOWEEK (Aug. 22, 2024, at 11:47 ET), https://www.autoweek.com/news/a61946456/waymo-sixth-generation-robotaxi-geely/ [https://perma.cc/N59D-JWRE].

387. *See supra* notes 252–259 and accompanying text.

388. Christopher Carey, *European Cities Leverage Data for Safer and Smarter Roads*, ITU: THE UN AGENCY FOR DIGIT. TECHS. (Mar. 31, 2022), https://www.itu.int/hub/2022/03/road-safety-data-europe-cities-today/ [https://perma.cc/D6X5-TXPL].

389. von Bodungen & Steege, *supra* note 280, at 309.

updating,[390] or even real-time information sharing[391]) to further avoid kinetic contact. In short, vehicle manufacturers process data from and about third parties as part of the iterative safety system.

Beyond the technologies themselves, the vehicle type approval rules require manufacturers to employ a process of using new information to improve the performance of vehicle safety systems. That data collection cycle begins well before a vehicle comes to market. Each new application for vehicle type approval requires multiple rounds of testing,[392] iterates periodically when the vehicle manufacturer conducts regular safety inquiries and analysis,[393] and incorporates new information at irregular intervals when market surveillance authorities conduct their own tests, for example, because of "sustained complaints."[394] All this information informs improvements to the design and operation of vehicle safety systems.

To facilitate the work of market surveillance authorities, the vehicle type regulations anticipate the processing of data held in event data recorders. The data recorded should be made available to these authorities "only for the purpose of accident research and analysis, including for the purposes of type approval of systems and components."[395] Specific to externally facing vehicle sensor systems, at a minimum, the event data recorder must allow authorities to identify "the active safety and accident avoidance systems fitted to the vehicle."[396]

---

390. *Id.* at 297.

391. Carey, *supra* note 388 (describing how "[p]otential collision spots are automatically identified by individual alerts").

392. *E.g.*, Commission Delegated Regulation (EU) 2021/1958 of 23 June 2021 supplementing Regulation (EU) 2019/2144 of the European Parliament and of the Council by laying down detailed rules concerning the specific test procedures and technical requirements for the type-approval of motor vehicles with regard to their intelligent speed assistance systems and for the type-approval of those systems as separate technical units and amending Annex II to that Regulation, 2021 O.J. (L 409/1) art. 4 (describing the evidence of testing that must be submitted to receive type approval for intelligent speed assistance systems).

393. *E.g.*, *id.* art. 3.3.

394. Vehicle Approval Regulation, *supra* note 267, art. 8(1)(b).

395. Vehicle General Safety Regulation, *supra* note 265, art. 6(4)(d).

396. *Id.* art. 6(4)(c)(iii).

Additionally, the market surveillance authorities in Europe already employ a robust information-sharing system.[397] Because these are the minimum standards, national laws on autonomous systems in vehicles may require additional data processing by the relevant authorities.[398] Considering that the goal of these iterative safety systems is to improve the technologies that aim to avoid kinetic contact, such information processing may become even more important as a means of improving the functionality of high-risk AI safety systems in vehicles.[399] Vehicle type regulators, therefore, also potentially process data about third parties captured by externally facing vehicle sensors.

The vehicle type regulations also require that vehicle repair and maintenance facilities, whether operated by the vehicle manufacturer or independent providers, "have . . . access rights to essential technical information and diagnostic data via the on-board diagnostic [("OBD")] adapter."[400] The adapter allows an OBD device to display fault codes from the vehicle. Vehicle repair and maintenance facilities may also process data about third parties captured by externally facing vehicle sensors. To interpret the fault codes, the vehicle manufacturer must provide adequate documentation for anyone using the OBD to determine what system(s) within the vehicle generated the fault code, the "[m]onitoring strategy; [f]ault detection criteria; . . . activation criteria; [s]econdary parameters; [and the] Preconditioning Demonstration test" to support the determination of that particular fault.[401] Depending on the specific safety system, each of these could reveal information from and about third parties observed by externally facing sensors. Information collected from specific vehicles

397. *See* Vehicle Approval Regulation, *supra* note 267, art. 11.

398. *See, e.g.*, Straßenverkehrsgesetz (StVG) [Road Traffic Act], § 1g Datenverarbeitung [Data Processing], https://www.gesetze-im-internet.de/stvg/__1g.html [https://perma.cc/U4X4-QD4F] (Ger.); Datenverarbeitung [Data Processing for Motor Vehicles with Highly or Fully Automated Driving Functions] 63a (2019), https://www.gesetze-im-internet.de/stvg/__1g.html [https://perma.cc/4G6C-Y5AS] (Ger.).

399. Bennett et al., *supra* note 331, at 12.

400. Kerber, *supra* note 287, at 315.

401. Vehicle Approval Regulation, *supra* note 267, Annex C, app. 2, sec. 2.3.

can inform additional improvements to vehicle safety systems, even before incidents occur.

The product liability regime advances iterative safety by incentivizing product improvements before contact occurs, thereby potentially avoiding the proximate safety system altogether. If a party suffered a direct loss because of the failure of a specific vehicle's safety system, that would be addressed by the proximate safety system discussed above. The product liability regime contributes to iterative safety by compensating people affected by defects in vehicle safety systems, independent of whether the defects in those systems present kinetic safety issues for all users of the vehicle safety systems.[402]

Product liability arises when a "claimant . . . prove[s] the defectiveness of the product, the damage suffered and the causal link between that defectiveness and that damage"[403] In relevant part, Article 7 of the new EU Product Liability Directive explains that:

> A product shall be considered defective where it does not provide the safety that a person is entitled to expect or that is required under Union or national law . . . tak[ing] . . . into account, . . . (b) reasonably foreseeable use of the product; (c) the effect on the product of any ability to continue to learn or acquire new features after it is placed on the market or put into service; (d) the reasonably foreseeable effect on the product of other products that can be expected to be used together with the product, including by means of inter-connection; . . . (f) relevant product safety requirements, including safety-relevant cybersecurity requirements; . . . [and] (i) in the case of a product whose very purpose is to prevent damage, any failure of the product to fulfil that purpose.[404]

---

402. *See* de Bruin, *supra* note 6, at 494.

403. Directive of the European Parliament and of the Council on Liability for Defective Products and Repealing Council Directive 85/374/EE art. 10(1) (2022/0302(COD)) (Sep. 25, 2024) [hereinafter Updated Product Liability Directive].

404. *Id.* art. 7(1)–(2).

This sweeping definition of "defective" can capture multiple ways in which vehicle safety systems can contribute to kinetic contact.

Adjudication of product liability claims, accordingly, necessitates that vehicle manufacturers share extensive information about the design and performance record of vehicle safety systems with the affected party.[405] That can include data collected from and about third parties via externally facing vehicle sensors. Failure of a vehicle manufacturer to share such "relevant evidence" creates a presumption that the product is defective, effectively shifting the burden of proof.[406] Accordingly, unless vehicle manufacturers want to assume the burden of proof when defending product liability claims, the new EU Product Liability Directive creates strong incentives to record data from externally facing sensors in multiple vehicles and share it with claimants.[407]

In addition to examining their own data, vehicle manufacturers may need to show they "exhaust[ed] all available possibilities" to learn about potential safety issues, including "analysing trade journals and conference reports as well as competitors' products for improved safety standards" at the design phase.[408] This information must inform safer design choices.[409] After a vehicle is in circulation, the manufacturer must then show that it continued to gather similar information, monitored vehicle performance, and applied the learnings to improve the operation of its safety systems.[410] Data collected from event data recorders, OBD devices, and vehicle connectivity services can play an important role in this monitoring. All of these sources potentially contain information about third parties observed by externally facing vehicle sensors.

The product liability regime allows for "[t]he liability of an economic operator . . . [to] be reduced or disallowed where the damage is caused both by the defectiveness of the product and by the fault of

405. von Bodungen & Steege, *supra* note 280, at 295.

406. Updated Product Liability Directive, *supra* note 403, art. 10(2)(a).

407. *See* Orian Dheu & Jan De Bruyne, *Artificial Intelligence and Tort Law: A 'Multi-faceted' Reality*, 31 EUR. REV. PRIV. L. 261, 265–66 (2023).

408. von Bodungen & Steege, *supra* note 280, at 291.

409. *Id.* at 291–92.

410. *Id.* at 295, 313.

the injured person or any person for whom the injured person is responsible"[411] As automated safety features become a larger part of the driving experience, the opportunities for human fault will hopefully diminish.[412] To help avoid product liability, vehicle manufacturers will need to monitor vehicle performance even more closely.[413] This necessary oversight increases the probability that data generated by externally facing sensors will be collected and retained by vehicle manufacturers to further improve the AI-safety systems.

The iterative safety system has other requirements which may necessitate sharing data collected from and about third parties.[414] The EU's Data Act mandates data sharing for "connected products" and "related services."[415] Because externally facing sensors process data about the environment around the vehicle to conduct safe vehicle operations, vehicles with externally facing sensor systems would meet the Data Act's definition of a "connected product."[416] This processing also meets the Data Act's definition of a "related service," because these systems are integrated into vehicles at the time of purchase and the absence of externally facing sensor data "would prevent . . . [a vehicle] from performing one or more of its functions."[417] Data from connected products and related services includes information about third parties captured by externally facing vehicle sensors.

---

411. Updated Product Liability Directive, *supra* note 403, art. 13(2).

412. *But see*, Meg L. Jones, *The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles*, 18 VAND. J. ENT. & TECH. L. 77, 88–92 (2020) (discussing how increased automation might increase the chance of human error).

413. *See* Kouroutakis, *supra* note 332, at 1109.

414. If the sharing is done via public communications networks, the ePrivacy Directive may apply. EDPB CONNECTED VEHICLES, *supra* note 5, at 7–9. *But see* EUR. AUTO. MFRS. ASS'N, EDPB GUIDELINES 1/2020 ON PROCESSING PERSONAL DATA IN THE CONTEXT OF CONNECTED VEHICLES AND MOBILITY RELATED APPLICATION 7–9 (Apr. 2020) [ACEA CONNECTED VEHICLE COMMENTS], https://www.acea.auto/files/ACEA_comments_EDPB_guidelines_1-2020.pdf [https://perma.cc/Y7H5-4ABA] (disputing the applicability of the ePrivacy Directive in vehicles that transmit data).

415. Data Act, *supra* note 303, art. 2(5)–(6).

416. *Id.* art. 2(5).

417. *Id.* art. 2(6).

The EU's Data Act requires that "[c]onnected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, . . . directly accessible to the user."[418] In short, a vehicle manufacturer will likely have to share externally facing sensor data with the owner or driver of a vehicle.

The Data Act, however, places some limitations on the further sharing and use of such data.[419] But the Data Act contemplates that "users of connected products should be able to share [non-personal] data with others, including for commercial purposes, with minimal legal and technical effort."[420] Though third-party recipients may not use non-personal data in certain ways,[421] these data sharing can contribute to independent research into the efficacy of externally facing sensor systems in vehicles. That research, accordingly, feeds into other operations of iterative safety systems that aim to improve high-risk AI safety systems in vehicles.

b. Third-Party Privacy Assessment

In the iterative safety system, regulators can process data recorded from externally facing vehicle sensors to ensure vehicle safety systems to comply via the vehicle type regulations[422] and to facilitate crash investigations.[423] Similarly, vehicle type regulations and product liability laws require vehicle manufacturers to continuously process data to improve the operations of vehicle safety systems.[424] Maintenance facilities can process data to similar ends as well.[425] The product liability regime and the Data Act require a vehicle manufacturer to share versions of these data with other market

418. *Id.* art. 3(1).
419. *Id.* arts. 5–9, 11–13, 32.
420. *Id.* recital 26.
421. *Id.* art. 6(2).
422. Vehicle Approval Regulation, *supra* note 267, art. 2(34).
423. Bennett et al., *supra* note 331, at 6.
424. ACEA Connected Vehicle Comments, *supra* note 414, at 7; *supra* notes 392–399, 402–413 and accompanying text.
425. *See* Determann & Perens, *supra* note 5, at 957.

participants so they can also make improvements to vehicle safety systems.

All of these are a "legitimate basis laid down by law" that would support the processing of personal data from and about third parties in the context of the iterative safety system.[426] Under GDPR, these legal requirements likely constitute "processing . . . necessary for compliance with a legal obligation to which the controller is subject."[427] This means that multiple parties have a legal basis for processing personal data about third parties. But it is not clear that the iterative safety system necessarily processes *personal* data from and about third parties within the scope of its intended purpose.

In contrast with the proximate safety system, data shared within the iterative safety system for the intended purpose of promoting kinetic safety would not qualify as personal data under GDPR. The Vehicle Type Regulations and the Data Act both require that data from vehicle safety systems be shared anonymously or as non-personal data.[428] The vehicle maintenance and product liability systems need to aggregate data to identify potential kinetic safety issues with particular vehicle models.[429] Data scientists regularly deploy anonymization and aggregation techniques to limit a data set's ability to reveal personal data.[430]

But the potential for data misuse is significant. One reason data can move freely through the iterative safety system is because they

426. Charter of Rights, *supra* note 39, art. 8.2.

427. GDPR, *supra* note 11, art. 6(1)(c); *see* Gesamtverband Autoteile-Handel e.V. v Scania CV AB, Case C-319/22, 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:62022CJ0319 [https://perma.cc/WQ7L-4KSS].

428. Vehicle General Safety Regulation, *supra* note 265, art. 6(4)(c)(ii); Data Act, *supra* note 303, art. 6(2).

429. *See* Lev-Aretz, *supra* note 68, at 6.

430. *See* Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1117 (2013); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1 *passim* (2021); Batistič, *supra* note 100, at 5–6. It is difficult to imagine how adding statistical noise would benefit the iterative safety system, as it is attempting to gain an accurate picture of how vehicle safety systems actually perform. *Cf.* Cai et al., *supra* note 72 (discussing differential privacy).

start as non-personal data.[431] The pursuit of kinetic safety offers no limit on how much data any organization can accumulate.[432] If the data remain non-personal, the GDPR offers no limit on its sale or further use.[433]

A vehicle's external sensors can capture data from and about otherwise anonymous third parties at a high spatial and temporal density.[434] In other words, a vehicle's external sensors collect a lot of data about people in a limited geographic space during a short period of time. In 2013, a team led by Professor Yves-Alexandre De Montjoye demonstrated that even in an anonymized dataset with low spatial and temporal density, it was possible to track the unique movements of people with no more than eleven locations and, for most people, as few as four.[435] This means that aggregating external sensor data could provide myriad data points about third parties on and along the roadway. "For the purpose of re-identification, more sophisticated approaches could collect points that are more likely to reduce the uncertainty, exploit irregularities in an individual's behaviour, or implicitly take into account information such as home and workplace or travels."[436]

---

431. *Cf.* Balayn & Gürses, *supra* note 55 ("[P]roviders[, as recipients of data,] can weave their own business interests seamlessly into the everyday functionality integral to the deployers[, the vehicle manufacturers that share the data].").

432. In fact, the new Product Liability Directive seems to encourage vehicle manufacturers to collect and share data extensively. *See supra* notes 405–413 as accompanying text; *cf.* Damien Geradin et al., *GDPR Myopia: How a Well-Intended Regulation Ended up Favouring Large Online Platforms—The Case of Ad Tech*, 17 EUR. COMPETITION J. 47, 74 (2020) (discussing how purpose limitation offers little resistance to an organization's accumulation, use, or sharing of data). This concept is explored further in a subsequent piece, Sella-Villa, *Towards a Political Economy of Third Party Privacy*, *supra* note 88.

433. *See* Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018 O.J. (L 303/59); *cf.* Salami, *supra* note 165, at 368 (discussing the regulatory guidance that forms the legal basis for a market in personal data in the EU).

434. *E.g.*, Franchi et al., *supra* note 4, at 2890.

435. Yves-Alexandre De Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REPS. 1376 (2013).

436. *Id.* at 1380.

Since Prof. De Montjoye published his study, the available technologies for performing these analyses have both improved and become more ubiquitous.[437] With just one other piece of information, like an image from Google's StreetView,[438] those unique patterns can be associated with known people.[439] In short, as the data set from the iterative safety system grows, the probability of identifying third parties also increases.[440]

Identifying third parties does not advance the goal of promoting kinetic safety on the roadway. But for non-government actors, there are few legal limitations on their use of these data and their ability to combine them with other data.[441] Consistent with the *Breyer* and *SRB* cases, this combination of data access, technological capabilities, and legal permission indicates that non-governmental actors in the iterative safety system can identify third parties.[442] So whether it is the parties in the iterative safety system or someone else that they provide the data to, only the threat of GDPR compliance can stop third party identification using external sensor data.

C. Third-Party Privacy and the Limits of Artificial Intelligence Regulation

The privacy analyses of high-risk AI systems under the AI Act identified two scenarios that give rise to third party personal data from externally facing sensors. First, data from external sensors stored in vehicles are likely pseudonymous data because third parties can identify themselves. Although circumstances surrounding the adjudication of roadway incidents present the most likely scenario in which a third party would request access to such data, it does not change the nature of the data. A provider of high-risk AI safety systems would need to evaluate its specific circumstances, but the

437. *See* Salami, *supra* note 165, at 363, 371; Chowdhury et al., *supra* note 14, at 353–55; Veale, *supra* note 9, at 3 (arguing that even without "amassment of data," platforms can render populations legible).

438. Fiodar Kazhamiaka et al., *Challenges and Opportunities for Autonomous Vehicle Query Systems*, *in* CONFERENCE ON INNOVATIVE DATA SYSTEMS RESEARCH 6 (2021).

439. *See* Salami, *supra* note 165, at 370; Krontiris et al., *supra* note 9, at 2.

440. Bennett et al., *supra* note 331, at 6.

441. *See* Vigorito, *supra* note 201, at 240.

442. *See supra* notes 170–177 and accompanying text.

iterative safety system presents all factors that enable someone to identify third parties under the GDPR's identifiability jurisprudence.[443] This gives rise to the second scenario—multiple parties can readily use the data required to be shared via iterative safety systems to identify third parties. This means that data collected by the externally facing sensors of vehicle safety systems are likely third-party personal data under the GDPR.

Just because a controller can process personal data does not mean it has a lawful basis for doing so.[444] As argued above, both the proximate and iterative safety systems create legal obligations that justify the processing of personal data from and about third parties.[445] But this analysis has only focused on third party identification from the perspective of that party. The core data processing relationship at the heart of the third-party privacy problem—between the first party and the controller—provides other means of justifying the processing of data which identifies third parties.

If the features of vehicle safety systems can be understood as a contract,[446] it provides another lawful basis that could result in processing third-party personal data.[447] Depending on the specific vehicle safety system, processing personal data might be understood "to protect the vital interests of the data subject or of another natural person," like a second or a third party.[448] Even when applying a balancing test to justify data processing, the "interests of the controller to improve fleet learning and algorithmic precision"[449] may outweigh

443. For an example of analyses that examined related questions about third party privacy, see BADEN-WÜRTTEMBERG 2022 DPA REPORT, *supra* note 342, at 105. *See also id.* at 89–90 (providing a similar discussion on same).

444. Salami, *supra* note 165, at 371.

445. de Bruin, *supra* note 6, at 498.

446. In fact, vehicle manufacturers are increasingly selling certain features as a subscription, or a service, rather than a productized feature of the vehicle itself. Daniel Davenport, *The Rise of Subscription Services for Cars: From One-Time Purchase to Connected Mobility Platforms*, MEDIUM (May 13, 2023), https://danieldavenport.medium.com/the-rise-of-subscription-services-for-cars-from-one-time-purchase-to-connected-mobility-platforms-8981208fb23b [https://perma.cc/4MXV-A9T8].

447. GDPR, *supra* note 11, art. 6(1)(b).

448. *Id.* art. 6(1)(d).

449. Hacker, *supra* note 6, at 275.

the interests of third parties who are on a public roadway.[450] The controller only needs to justify identifying third parties incident to these ends. In short, what may count as a foreseeable misuse of data from third parties could fall within the intended purpose of the AI system for first parties.

These legal bases for personal data processing, supported by the AI Act's data management requirements, create a privacy rights cliff for third parties under the GDPR.[451] Typically, the GDPR affords a data subject the following rights in their data: notice of processing, access to her data, rectification, erasure of her data, restriction of processing, data portability, objection of processing,[452] and "the right not to be subject to a decision based solely on automated processing, including profiling."[453] Third parties, however, only enjoy the rights to notice and access.

As long as the processing is justified by contract performance, compliance with legal obligations, or protecting the physical safety of people outside the vehicle,[454] the GDPR does not afford people outside a vehicle observed by externally facing sensors the right to object to such data processing.[455] Additionally, processing third party personal data enables vehicle features that promote kinetic safety, and therefore "safeguard the data subject's rights and freedoms and legitimate

---

450. *But see supra* Part IV.A.2 (discussing the capabilities of sensor systems that push past visual barriers and may therefore capture information from non-public spaces). The scope of "panorama rights" may provide an analogous framework for balancing controller interests and third-party privacy interests. *See generally* Mary LaFrance, *Public Art, Public Space, and the Panorama Right*, 55 WAKE FOREST L. REV. 597 (2020).

451. This phrasing borrows from the concept of the "precedential cliff," articulated by Professor Madalyn Wasilczuk, in her excellent piece, *Killing Stays*. WIS. L. REV. 859, 906–12 (2024). Though derived from a very different legal context, it captures the impossibility of a party exercising her rights under a given set of legal circumstances.

452. GDPR, *supra* note 11, arts. 12–21.

453. *Id.* art. 22(1).

454. GDPR, *supra* note 10, art. 21(1) (referring, by omission, to GDPR art 6(1)(b)-(d)); *see supra* notes 336–338 and accompanying text; *see also supra* notes 370–371 and accompanying text (explaining why consent is not an option for processing personal data from and about third parties).

455. GDPR, *supra* note 11, art. 21(1).

interests."[456] Accordingly, the GDPR does not protect the right of third parties to be free from "decision[s] based solely on automated processing."[457] In other words, the GDPR offers third parties no opportunity to prevent externally facing sensors from collecting personal data about them.

Processing personal data collected by externally facing sensors for the purpose of advancing kinetic safety also likely falls under GDPR Article 11.[458] "[T]he controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with [the GDPR]."[459] This may help make data processed by externally facing sensors harder to associate with a person, but it does not prevent its collection or storage.

When it comes to data from externally facing sensors in vehicles, the right of rectification for people observed by such sensors is inapposite.[460] The right to erasure also does not apply because data from externally facing sensors helps vehicle manufacturers either meet legal obligations pursuant to the Vehicle Approval Regulation[461] or defend claims under various legal regimes,[462] including product liability.[463] Because processing third-party personal data is based neither on the consent of a third party nor a contract between the third party and the vehicle manufacturer, the GDPR does not afford third parties the vehicle the right to data portability.[464]

---

456. *Id.* art. 22(2)(b).

457. *Id.* art. 22(1).

458. GDPR *supra* note 11, art. 11. But, if the purpose of processing of externally facing sensor data is to enable more driving, to automate law enforcement, or to conduct direct marketing to people outside a vehicle, then GDPR Article 11 would likely not apply.

459. *Id.* art. 11(1); *see also* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1836–48 (2011).

460. GDPR, *supra* note 11, art. 16. It is difficult to image both what a person observed by externally facing sensors would argue should be corrected in the data and how to technically achieve such correction.

461. GDPR, *supra* note 11, art. 17(3)(b).

462. *Id.* art. 17(3)(e).

463. *See* ACEA CONNECTED VEHICLE COMMENTS, *supra* note 414, at 7; *supra* Part V.B.2.a.

464. GDPR, *supra* note 11, art. 20(a).

GDPR also falls short of limiting the sharing of third-party data.[465] Article 8.1 of the EU Charter ensures that "[e]veryone has the right to the protection of personal data concerning him or her."[466] Accordingly, externally facing sensor data from vehicle safety systems must be shared in such a way that prevents or limits the sharing of personal data. The vehicle type regulations attempt to do this by requiring government authorities to use data from event data recorders solely for compliance with the GDPR.[467] But the construction here is circular. GDPR Article 6(1)(e) authorizes processing of personal data "for the performance of a task carried out in the public interest."[468] And the task carried out in the public interest is the processing of personal data from event data recorders, as spelled out in the vehicle type regulations.

If a person outside of a vehicle can demonstrate that data collected by externally facing sensors are data from or about themselves,[469] they enjoy limited rights under GDPR. A notice including specific information about the data processing and the exercise of their rights must be made available to them.[470] But the only right left for them to exercise would be the right of access.[471] The combination of notice requirements and the right of access, ironically, facilitates the association of data collected from externally facing sensors with "identified and identifiable natural persons."[472]

In sum, though the analyses required by the AI Act can help identify the privacy interests of third parties, the only privacy rights

465. *Cf.* Franchi et al., *supra* note 4, at 2881 (describing a fuller set of third party privacy rights, "where the subjects are not required to give consent and have no right to revoke the transmission unless they preempt the information flow via requesting an obfuscation of their appearance in the dataset").

466. Charter of Rights, *supra* note 39, art. 8.1.

467. Vehicle General Safety Regulation, *supra* note 265, art. 6(4)(d).

468. GDPR, *supra* note 11, art. 6(1)(e).

469. *Cf. id.* art. 11(2) (explaining the inapplicability of certain data protection rights when "the controller is able to demonstrate that it is not in a position to identify the data subject").

470. *Id.* arts 12 & 14; *see* BADEN-WÜRTTEMBERG 2018 DPA REPORT, *supra* note 443, at 89–90.

471. GDPR, *supra* note 11, art. 15; *see also* Salami, *supra* note 165, at 376.

472. *Id.* art. 4(1); *see* Solve & Schwartz, *supra* note 459, at 1876–77; Veale, *supra* note 9, at 4.

available to third parties are those of notice and access. This grants third parties the opportunity to learn just how much externally facing sensors might affect their privacy but offers them no tools to advocate for themselves.[473] The data governance mechanisms of the AI Act effectively legitimate the production of third-party personal data with no limitation.[474] Despite the broader data governance scope provided by the AI Act the third-party privacy problem persists.

The EU AU Act's application to externally facing sensors relies on the individualist approach of the GDPR, which leaves third-party privacy interests inadequately protected. The AI Act's delegated acts may to address the third-party privacy problem presented by high-risk AI safety systems by changing the circumstances of the production of third-party data to account for the ways such data must be used and could be misused. They could influence technical designs that allow for the collection of data from and about third parties. These legislative efforts could also change the legal requirements regarding data storage and sharing within their purview. Accordingly, hope remains that the AI Act can address the third-party privacy problem.[475]

VI. Conclusion

Vehicles' externally facing sensors impact the privacy of individuals observed by these systems, yet the theoretical and legal implications of this phenomenon have been largely underexplored. This Article offered an account of the "third-party privacy problem." An issue in multiple fields, the phenomenon arises where technologies collect personal data from individuals who are neither users nor direct participants in a service, but additional rules incentivize the further processing of their data. Using the EU as a test case, this Article examined whether the world's most comprehensive privacy and AI

473. *See* Julie E. Cohen, *From Lex Informatica to the Control Revolution*, 36 Berkeley Tech. L.J. 1017, 1044 (2021).

474. Niklas Eder, *Beyond Automation: Machine Learning-Based Systems and Human Behavior in the Personalization Economy*, 25 Stan. Tech. L. Rev. 1, 5 (2021).

475. A subsequent piece, Sella-Villa, *Towards Political Economy of Third Party Privacy*, *supra* note 88, assesses the ability of the AI Act's delegated acts to address the third-party privacy problem. Where shortcomings remain, that piece also offers potential solutions.

regulatory framework can recognize and protect third-party privacy interests. The analysis established that the EU AI Act's data governance provisions have the potential to protect third-party privacy interests. But applied to the case study of data collected by vehicles' externally facing sensor, protections for third-party privacy prove anemic.

Defining the third-party privacy problem aids in understanding why even the EU's comprehensive privacy regime falls short. The GDPR's one-to-one relational model inadequately captures third-party privacy interests when processing data from and about other individuals. This Article's analysis revealed that even when applying the AI Act's data governance provisions, third parties can only realize their privacy interests through rights of notice and access. They lack rights to limit processing, rectification, or erasure. Under the broad purpose of safety, data from third parties follows freely with promise of improving future AI systems. These limited protections demonstrate that existing frameworks, even in the world's most stringent regulatory environment, fail to adequately safeguard third parties' privacy interests.

However, hope for third-party privacy remains. The EU AI Act offers an opportunity to protect third parties by incorporating robust data governance practices into the conformity assessment process for certain AI systems. Rather than relying solely on privacy law's individual rights framework, this regulatory approach could mandate organizational and technical safeguards before AI systems enter the market. Whether this mechanism proves effective in practice requires careful examination of the AI Act's implementation and enforcement.

This Article raises questions that merit continued exploration. Future work will examine the third-party problem in other AI and legal contexts, beyond vehicle sensors in the EU. Additionally, analysis of potential interventions across contexts can reveal the relative advantages and disadvantages of arming third parties with additional legal tools, restricting technologies' capabilities, or mandating particular data processing. The third-party privacy problem, accordingly, offers a new perspective on privacy law and theory.