Washington and Lee Law Review Online

Volume 73 | Issue 2 Article 7

4-27-2017

Privacy in the Age of Autonomous Vehicles

Ivan L. Sucharski
HERE North America, LLC

Philip Fabinger
HERE Deutschland GmbH

Privacy in the Age of Autonomous Vehicles

Ivan L. Sucharski* & Philip Fabinger**

Abstract

To prepare for the age of the intelligent, highly connected, and autonomous vehicle, a new approach to concepts of granting consent, managing privacy, and dealing with the need to interact quickly and meaningfully is needed. Additionally, in an environment where personal data is rapidly shared with a multitude of independent parties, there exists a need to reduce the information asymmetry that currently exists between the user and data collecting entities. This Article rethinks the traditional notice and consent model in the context of real-time communication between vehicles or vehicles and infrastructure or vehicles and other surroundings and proposes a re-engineering of current privacy concepts to prepare for a rapidly approaching digital future. In this future, multiple independent actors such as vehicles or other machines may seek personal information at a rate that makes the traditional informed consent model untenable.

This Article proposes a two-step approach: As an attempt to meet and balance user needs for a seamless experience while preserving their rights to privacy, the first step is a less static consent paradigm able to better support personal data in systems which use machine based real-time communication and automation. In addition, the article proposes a radical re-thinking of the current privacy protection system by sharing the vision of "Privacy as a Service" as a second step, which is an independently managed method of granular technical privacy control that can better protect individual privacy while at the same time

* Ivan.Sucharski@here.com, Lead Data Strategist, HERE North America LLC.

** Philip.Fabinger@here.com, Global Privacy Counsel, HERE Deutschland GmbH.

facilitating high-frequency communication in a machine-to-machine environment.

Table of Contents

I. Introduction: The Challenges of Modern Privacy Management

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right to be let alone."[1]

What seems to be a statement envisaging the next innovative step in digitization is in fact a flashback. In December 1890, Samuel D. Warren and Louis D. Brandeis came to this conclusion in their groundbreaking article *The Right to Privacy*. Triggered by the publication in newspapers of individuals' "instantaneous photographs" and the corresponding effects on individual privacy, they felt that action must be taken.[2] Now, 127 years later, we are facing machine-to-machine interactions, another type of real-time or "instantaneous" communication that may include a privacy payload. While trying to apply established privacy principles to this type of communication we inevitably conclude: Market disruption must be accompanied by a disruption in the privacy paradigm.

Let us begin by returning to the basic ideas of privacy and its accompanying management and imagine it in a world that will exist tomorrow. Soon we will live in a world where vehicles or, frankly, any type of machine, will talk to each other about us—whether directly or indirectly—and will negotiate with each other on our behalf to make decisions in our best interest for a wide range of purposes, some of which we have not yet imagined. Depending on the scenario, these negotiations are certain to include varying levels of our personal information. While these vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and machine-to-machine (M2M) negotiations will simplify and improve our lives, we must prepare for a future that allows for these eventualities as they challenge our current approaches to managing privacy.

Privacy, at its core, is about choice and control. This includes control of information about the self, particularly one's identity, but also includes connecting that identity with associated

---

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (internal quotation marks omitted).

2. *Id.* at 195.

metadata such as actions, activities, thoughts, desires, affiliations, habits, preferences, and beliefs. The right to privacy, the extent to which that right can be asserted, and the principle of individual control have been well established for decades. But privacy is a constant negotiation between the individual and society about the boundaries of the two worlds of public and private. While the concept of what is specifically private is often in a state of flux, we are currently seeing a seismic shift in consumer habits.[3] The normative values are changing rapidly as technology presses forward, forcing a serious renegotiation of the boundaries of privacy far too regularly.

The digital age, with its rapid pace of developing enabling technologies particularly around the collection of personal data and related metadata, long-term storage, and immediate retrieval, has vastly outpaced the ability of both society and policymakers to adequately adapt privacy controls.[4] The idea of individual control over privacy flows into the current "formulaic system of notice and consent,"[5] which may no longer be a suitable mechanism to ensure adequate privacy. The concept has been challenged both in 1:1 (user: service) communication and in big data scenarios and has prevailed so far. It will need to further adapt, however, for scenarios such as when a rapid series of time sensitive 1:1 consents are required or with 1:N (one-to-many) real-time communications between machines. Because of this pace, we are in a constant reactive state rather than meaningfully preparing for the inevitable "next things" regarding commerce, data, and the needs and expectations around privacy when it comes to a merger of the physical and digital world.

---

3. *Consumers' Privacy Concerns Grow*, WARC (Jan. 25, 2017), https://www.warc.com/NewsAndOpinion/News/38101 (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

4. *See* VIKTOR MAYER-SCHOENBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 17 (2013) ("[T]he big-data era also challenges us to become better prepared for the ways in which harnessing the technology will change our institutions and ourselves.").

5. *Id.* at 173.

II. Solutions for Privacy Challenges in the Digital Age

To approach a solution, it is often worthwhile to take a step back to understand how the challenge has emerged. The origins of digital privacy management come from a long-passed, contractual approach to sharing personal information in which a method of notice and informed consent is applied and the affected individual can easily grasp the scope of the ecosystem within which their data will persist.[6] Originally in paper form, the individual would disclose some private information and the form would include simple language about the purpose and intent of the data collection, the sacredness of privacy, and the recognition of the duties of the collecting entity to maintain the data responsibly.[7] In our current privacy paradigm, often focused around digital communication devices and services, the underlying ecosystem is almost wholly obfuscated and is now so complex that few individuals besides industry experts can truly understand the actual breadth to which the provided data is used, shared, and stored.

Along with the vagaries of purposes when consenting to private data collection on digital devices, an additional privacy challenge occurs today because there is a burden placed on the individual to consent while under the pressure of attempting to utilize a service, such as the first time a mobile application is launched, or directly prior to installing it.[8] Furthermore, it is generally unclear what functionality is impacted if the consent is declined and there is often no opportunity to decline consent for specific types of personal data while consenting to other data or

---

6. *See* Jeroen van den Hoven et al., *Privacy and Information Technology*, STAN. ENCYCLOPEDIA OF PHIL. (Nov. 20, 2014), https://plato.stanford.edu/entries/it-privacy/ (last visited Apr. 24, 2017) (describing how informed consent is the principle underlying all data protection laws) (on file with the Washington and Lee Law Review).

7. *See* DEP'T OF HEALTH & HUMAN SERVS., NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION 1–2 (2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/notice.pdf (providing the required contents of the notice).

8. *See* Masooda Bashir et al., *Online Privacy and Informed Consent: The Dilemma of Information Asymmetry*, at 2 (2015), https://www.asist.org/files/meetings/am15/proceedings/submissions/papers/97paper.pdf ("Either the user agrees to give up all their personal information to the service or they choose not to use the service at all.").

consenting to data at a specific chosen level of granularity (such as revealing one's zip code versus a home address).[9] Terms of Service and Privacy Policies are often incredibly long, full of legalese, complex, and overly confusing (some would argue by design). There is no simple way for any user to understand how her data is being used by a single company much less understand the state of her privacy at any given point considering all of the permissions that may have been granted to separate entities over time. The possibility of the individual to adequately assert her "right to be forgotten" is well-nigh impossible as she has no clue what entities have what personal data about her and therefore no way to verify or validate the state of her privacy in any meaningful way.[10] Transparency into privacy may exist at a micro level such as per company, but at the macro level of the individual's shared privacy footprint across the digital landscape, there is no such thing. To add insult to injury, the current response to the individual who wishes to reclaim her privacy (or even some semblance of control) from the multitude of entities she interacts with for basic modern engagement is often "what did you expect, you've given your permission while failing to read the terms of service?"[11] The victim is therefore blamed.

This is the current landscape, and the future of digital privacy appears hopeless without some radical rethinking. The evolution from personal (i.e. in-person) privacy data interactions

---

9. *See id.* at 9 ("Our survey results illustrate this perception of coercion, as the vast majority of respondents (81%) indicated that in at least one incident, they had submitted information online when they wished they were not required to do so."); EURO. DATA PROTECTION SUPERVISOR, GUIDELINES ON THE PROTECTION OF PERSONAL DATA PROCESSED BY MOBILE APPLICATIONS (2016), https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_mobile_apps_en.pdf (providing that consent should be specific, expressed through an active choice, and freely given).

10. *See generally* JOSEPH TUROW, MICHAEL HENNESSY & NORA DRAPER, THE TRADEOFF FALLACY, ANNENBERG SCH. FOR COMM., U. PENN (Aug. 10, 2016), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf (arguing against the notion that Americans willingly give up privacy for benefits).

11. Robert Glancy, *Will You Read This Article About Terms and Conditions? You Really Should Do*, GUARDIAN (Apr. 24, 2014), https://www.theguardian.com/commentisfree/2014/apr/24/terms-and-conditions-online-small-print-information (last visited Apr. 24, 2017) ("We live in a time of terms and conditions. Never before have we signed or agreed [to] so many. But one thing hasn't changed: we still rarely read them.") (on file with the Washington and Lee Law Review).

occurring between an individual and a known physical entity, to the digital equivalent of that physical entity, and now further on to a multitude of tangentially-known digital entities regularly requesting access to a myriad of personal data points, has led to a system of consent and consumer protection that no longer makes sense. Additionally, applying this current system to near-future concepts of maintaining control and managing digital privacy in cases where time sensitive M2M communications containing "privacy payloads" (sets of personal or private data) occurs is fundamentally broken, meaning that the modern methods of notice and consent will soon become unsustainable. We need a new approach to concepts of granting consent, managing privacy, and dealing with the need to interact quickly and meaningfully while reducing the information asymmetry between the user and collecting entities that is commonplace in modern privacy negotiations.

This Article rethinks the traditional notice and consent model in the context of real-time M2M communication and proposes a re-engineering of privacy concepts to prepare for a rapidly approaching digital future. In this future, multiple independent actors—in the form of vehicles or other machines—may seek personal or private information at a rate that makes the traditional informed consent model untenable. While this article focuses on V2V or V2I communication, the principles outlined can also apply to various M2M cases in which a privacy payload is involved (e.g. drones identifying who they belong to when negotiating priority in airspace, or after being involved in an accident).

A two-step approach is proposed. The first step is an attempt to meet and balance user needs for a seamless experience while preserving their rights to privacy. It is believed that by shifting our approach to consent away from the traditional 1:1 model, and towards a more general management method similar to how we handle the current configuration options for cookie acceptance in a web browser, we will maintain privacy while allowing for a number of high-value use cases to develop. Examples of such cases include improving infrastructure in smart city initiatives, monitoring the performance of a vehicle, or increasing traffic safety.

The second step proposes the concept of Privacy-as-a-Service in which a configured service negotiates privacy on behalf of the individual and collects an audit trail of entities requesting and granted data from the vehicle, or machine, on behalf of the user. In this sense, there is a huge opportunity for the individual to reclaim control of her privacy by consenting to the level of granularity that she prefers while radically increasing general transparency around what is collected and by what entity, thus reducing current information asymmetry. This approach allows for commercial and technological progress to take on many forms, at whatever pace is fitting, without the need for defining completely new methods of privacy control. Lastly, such a system can be accomplished without regulation, thereby removing reactive restrictions that limit commercial opportunities due to consumer's appropriate feelings of exploitation, victimization, and helplessness.

III. Consent Reimagined

A. Preparing for a Future of On-the-Fly Privacy Management

Tomorrow's smart city initiatives will collect data about vehicles interacting within municipal systems to provide information regarding such actions as road usage and parking dwell time behaviors, thereby improving traffic efficiency by utilizing an invisible data layer, created by vehicles, on top of the existing infrastructure.[12] Systems are being developed to broadcast information between vehicles such as slowing traffic ahead, an accident, or a dangerous patch of road. This information enables drivers or vehicles to make navigation decisions that increase safety and maximize traffic flow.[13] Collaboration between connected vehicles or vehicles and infrastructure will improve traffic safety beyond all current recognition[14] and is critical to master the next levels of

12. A European Strategy on Cooperative Intelligent Transport Systems, A Milestone Towards Cooperative, Connected and Automated Mobility, EUR. PARL. DOC. (COM 766) 2, 3 (2016) [hereinafter A European Strategy]

13. *Id.*; Federal Motor Vehicle Safety Standards, 49 C.F.R. § 571 (2016).

14. 49 C.F.R. §§ 571.101–500 (providing instructive research for the

automation and highly autonomous driving. Connectivity can enable multimodal transport systems connecting all different actors, from vehicles to pedestrians, cyclists, drones, infrastructure, traffic managers and mobility providers, structuring their behavior and matching supply and demand in real time. While there are plenty of examples of data sharing opportunities related to the functioning of road networks, municipal information, traffic safety, or the functioning of a truly integrated transportation system, there are also untold commercial applications of personal data imported or derived from a vehicle, a user, or the interactions of a user in a vehicle.[15] Vehicles will collect more data via built-in sensors and also become more connected to cloud services, the internet, the infrastructure, digital platforms, and each other.

These next steps of innovation in mobility leading to a market disruption entailing fundamental and game-changing autonomous systems will be enabled through digitized communication. Cooperation and communication between intelligent and connected vehicles is a prerequisite to enable higher levels of automation and to significantly improve traffic safety.[16] Thus, solving privacy issues with V2V and V2I communication is necessary to prepare for the future of mobility. While some of the manifold information generated through vehicle sensors and transmitted from the vehicle can be provided in anonymized form without carrying a privacy payload, other information may be reasonably linkable to an individual or may sometimes be considered personal data due to different regulatory approaches in different jurisdictions.[17]

United States Department of Transportation, National Highway Traffic Safety Administration).

15. *See* MCKINSEY & CO., AUTOMOTIVE REVOLUTION—PERSPECTIVE TOWARDS 2030, at 6 (2016), http://www.mckinsey.com/~/media/mckinsey/industries/high%20tech/our%20insights/disruptive%20trends%20that%20will%20transform%20the%20auto%20industry/auto%202030%20report%20jan%202016.ashx ("Connectivity, and later autonomous technology, will increasingly allow the car to become a platform for drivers and passengers to use their transit time for personal activities, which could include the use of novel forms of media and services.").

16. A European Strategy, *supra* note 12, at 2; 49 C.F.R. § 571.

17. *See* A European Strategy, *supra* note 12, at 8. For a highly different approach, however excluding collection or use of V2V data by commercial entities or other third parties, see 49 C.F.R. § 571.

In an environment in which vehicles are broadcasting and sharing personal data, the appropriate consents of the affected individuals must be obtained. A consent is the manifestation of the individual´s "say" regarding control over her right to privacy.[18] In the case of multiple parties near-simultaneously requesting time sensitive consent, the current 1:1 consent based models employed in the physical world or by software applications between actors with clear role allocations do not scale. Mobility's future dynamic information ecosystem with multiple stakeholders includes data collectors with whom the individual has not had a relationship before and leads to difficult questions as to who is the data controller and who is the data subject to be protected by the privacy laws in a given data interaction.[19] Even in the case of a single entity requesting consent, its Terms of Service and Privacy Policy could rarely be meaningfully reviewed by the motivated person on the move. This problem is compounded by the behavior of potentially dozens of vehicles or entities asking for variable permissions of a given driver at a point in time. Aside from the driver behaving in one of three subpar manners (grant all, grant none, grant randomly) the cognitive burden on them is unduly intense considering the distractive and annoying aspects that something akin to pop-up consent requests would create.[20]

Given the above scenarios, the future of V2V or V2I communication includes the potential for a multitude of separate actors vying for general and specific personal data controlled by drivers, in real time or near-real time. These actors could include other vehicles, municipal signal towers, infrastructure objects like traffic signs and stoplights, buildings and billboards, and a variety of actors that have yet to manifest. Each actor will have

---

18. *See generally* ICO, CONSULTATION: GDPR CONSENT GUIDANCE (2017), https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf (providing guidance on how to conform with the GDPR in the UK).

19. *See* FUTURE OF PRIVACY FORUM, COMMENT LETTER ON THE DEP'T OF TRANSPORTATION AND NAT'L HIGHWAY TRAFFIC SAFETY ADMIN.'S FEDERAL AUTOMATED VEHICLES POLICY GUIDANCE 9 (Nov. 22, 2016) [hereinafter FUTURE OF PRIVACY FORUM NHTSA COMMENTS], https://fpf.org/wp-content/uploads/2016/11/FPF-Comments-on-DOT-Guidance_112216_Final.pdf.

20. *Id.* at 7.

its own potentially complex purpose, request specific types of information, and will often need consent for collecting such information nearly instantaneously.

Transferring the legal requirements for a valid consent under the European Union's upcoming General Data Protection Regulation (GDPR)[21] or in the U.S. requiring a comparable type of notice and choice to the above use-cases leads to a basic conclusion: The current consent schemes are too static and cumbersome for scenarios with multiple unknown actors in shared spaces and split-second communication and decision making, and the schemes do not support the kinds of high frequency and highly agile communication required for safe and seamless future transportation experiences. Consequently, we need to rethink the current approach, modify the requirements for a valid consent, and prepare for a future of on-the-fly privacy management.

B. Consent Under the GDPR

The European strategy on Cooperative Intelligent Transport Systems (C-ITS) concludes that "data broadcast by C-ITS from vehicles will, in principle, qualify as personal data as it will relate to an identified or identifiable natural person."[22] Under the upcoming GDPR in the European Union, "consent" of the respective individual, the data subject, means "any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[23] Based on these requirements, consent must relate to specific processing operations.[24] Consequently, a general broad consent to unspecified processing operations as they might arise would be

21. *See generally* Council Regulation 2016/679, 2016 O.J. (L 119). The GDPR enters into force on May 25, 2018.

22. A European Strategy, *supra* note 12, at 8. We use the term "personal data" in the sense of Article 4 (1) of the GDPR. *See* Council Regulation 2016/679, *supra* note 21, at L 119/33.

23. Council Regulation 2016/679, *supra* note 21, at L 119/34.

24. *Id.*

invalid. For consent to be informed, "the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended."[25] A clear affirmative action

> could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject´s acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject´s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.[26]

This means people shall positively and demonstrably indicate that they agree with the proposed data collection and use before it happens. It also means that the individual needs to know the requesting entity, the type of data to be collected, and the envisaged purposes of data processing. In addition, the individual must have the "genuine choice" to agree or disagree to the collection and further processing of her personal data and that these requirements function as a minimum standard to provide her with a solid information basis for her choice.[27]

Applying these strict requirements for a valid consent to the previously mentioned use-cases presents several difficult challenges. First, in such a dynamic, multi-actor environment, it would be extremely difficult, if at all possible, to obtain consent that is specific enough to satisfy current and proposed regulatory requirements. When a vehicle is broadcasting information via a wireless network, other nearby vehicles and infrastructure units can receive the messages and respond to them. Each vehicle may be both broadcasting and receiving multiple communications simultaneously. To have a meaningful impact on traffic safety necessitates communication between vehicles with very low

25. *Id.* at L 119/8.
26. *Id.* at L 119/6.
27. *Id.* at L 119/8.

latency,[28] and services for the management of traffic flows or efficiency improvements that utilize swarm intelligence will require near real time communications to generate valuable information. In both contexts, it is difficult to determine the data controller as the party defining the purposes and means of the processing of personal data,[29] especially since the controllers are likely not to have an established relationship with the broadcasting data subject. If it is unclear with whom context-specific information is going to be shared, transparency can only be provided ad hoc or in a more generic way. Current solutions, such as just-in-time notices,[30] that have been established as best practices in smartphone applications could distract the driver of a vehicle and are therefore detrimental from a safety perspective and would likely overload the driver with multiple simultaneous requests to provide consent.[31]

Another challenge is the limitation of "real" choices, required in principle for a "freely given" consent. It is impossible to provide individuals with actual choice in scenarios where the reliability of safety functions, or even the operations of highly autonomous vehicles, require a continuous data communication. Any requirement to interrupt or disrupt connectivity to obtain considered choice would impair functionalities, leading to reduced safety and opening the door for even more complex liability questions in case something goes wrong.[32]

It is therefore apparent that a strict interpretation of the GDPR's transparency requirements would render it impossible to obtain a valid consent for collecting and processing personal data in connected vehicle scenarios with high-frequency communication between multiple actors. At this stage, the data

---

28. V2V messages are broadcast in a limited range ten times per second. *See* Federal Motor Vehicle Safety Standards, 49 C.F.R. § 571 (2016).

29. Council Regulation 2016/679, *supra* note 21, at L 119/33.

30. NAT'L SCI. AND TECH. COUNCIL, NATIONAL PRIVACY RESEARCH STRATEGY 15–16 (2016), https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf.

31. *See* FUTURE OF PRIVACY FORUM NHTSA COMMENTS, *supra* note 19, at 7 (discussing how just-in-time notices that appear on a phone's screen when opening apps could distract drivers).

32. *See id.* at 8 ("These are challenging considerations given the rapidly changing pace of these technologies, and definitional lines may prove difficult to draw at this time.").

protection law presents a bottleneck for the next level of advanced vehicle connectivity and thus threatens to be a burden to realizing the overwhelmingly positive impact of such technologies on society.

C. A Loophole: The Future of Mobility Is Communication

One of the key questions the U.S. National Privacy Research Strategy asks is "how can notice and choice be standardized and conveyed in ways that facilitate automation and reduce transaction costs for users and stakeholders?"[33] A feasible approach to answer this question for the connected vehicle context can be deduced from upcoming regulation in the European Union.

In early January 2017, the European Commission published the draft Regulation on Privacy and Electronic Communications (Regulation),[34] the replacement of the ePrivacy Directive (also known as the "Cookie Directive").[35] Although only a draft for the time being, once in effect, the Regulation will enter the next level of the "Internet of Everything" and go far beyond cookie rules, as set forth in its Recital 12:

> Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications.[36]

---

33. NATIONAL PRIVACY RESEARCH STRATEGY, *supra* note 30, at 16.

34. Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC, EUR. PARL. DOC. (COM 10) (2017) [hereinafter The Regulation].

35. Council Directive 2002/58, 2002 O.J. (L 201) (EC).

36. The Regulation, *supra* note 34, at 13–14.

With this important clarification, the proposed regulatory content would apply to V2V and V2I communication.

With respect to cookies, the Regulation considers the need for an undisturbed user experience:

> The methods used for providing information and obtaining end-user´s consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment.[37] As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application.[38]

The European Commission considers web browsers as gatekeepers and sees them "in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment."[39] Therefore, the draft Regulation would ideally like consent to be obtained at the device configuration stage. Instead of having to give consent every time a website wants to track a user, users should be able to configure their browsers to either accept tracking or not, or to grant this right only to selected parties, be it truly trusted partners or providers simply offering an indispensable service. The implication is that a device would need to present a clear option to the user, who would then be forced to make a positive decision to allow the data collection. This approach, adopted from today's web browser or smart device configuration methods, presents a

---

37. "Terminal equipment" pursuant to Article 1 of Commission Directive 2008/63, 2008 O.J. (L 162) 21 (EC), means:

> Equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case . . . the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network.

Although the draft Regulation only mentions smart phones, tablets, and computers as examples for terminal equipment, connected vehicles clearly fall into this category as well.

38. The Regulation, *supra* note 34, at 17 (emphasis added).

39. *Id.*

solution for the challenge described above of adopting specific consent requirements to fast-paced multi-stakeholder communication in the connected vehicle. Additionally, the device configuration model is also a suitable means to provide the appropriate level of transparency and choice to enable next levels of vehicle connectivity as the requesting entities will be nothing more than providers of "information society services,"[40] similar to those in use today.

The draft Regulation emphasizes that consent of an end-user shall have the same meaning and be subject to the same conditions as the data subject´s consent under the GDPR.[41] This might be surprising, as transparency regarding the identity of the data controller, specific purposes, or requested data elements can only be provided on a more generic level through configurations such as "accept all 3rd party cookies." This is not a contradiction, however, given that the GDPR explicitly provides that "choosing technical settings for information society services" is an appropriate means to obtain consent.[42] Because future mobility will, to a large extent, be enabled through communication services, vehicle connectivity can be treated the same way as classical information society services that enable communication between humans. Additionally, device configurations regarding connectivity functions embedded in the vehicle present the most reliable solution to reach the driver as the privacy protected individual, respectively the driver as the individual with the highest privacy related risk profile in a vehicle with a steering wheel. For example, individual drivers could pre-select their privacy settings or profiles such as "accept all 3rd party requests" through an online or app-based dashboard. Each individual's privacy profile would be recognized by the vehicle, either through active driver input or connectivity-based recognition of the settings in a driver's smartphone or other personal digital device. The vehicle would then automatically adjust its communications and sensor technologies to accommodate the privacy choices of

40. Pursuant to Article 1(1)(b) of Directive 2015/1535, 2015 O.J. (L 241) 3 (EC), an information society service is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

41. The Regulation, *supra* note 34, at 15.

42. Council Regulation 2016/679, *supra* note 21, at L 119/6.

individual drivers. Such a system would allow a single vehicle to accommodate the privacy preferences of multiple individual drivers in situations where vehicles may include pooled use, such as with families or through vehicle sharing services. Compare the privacy related driver settings to seating or mirror adjustments covering the specific needs of the respective driver. Ultimately, the device configuration model comes along with less transaction specific transparency. However, it provides a viable solution for declaring consent in high-frequency communications and it respects individual choice by targeting the decision making directly to the individual driver. Additionally, this model is derived from established and socially accepted norms for classical web browsing, which is nothing else than mobility in the digital space.

The EU's C-ITS initiative names as one action item for its next steps "ensuring the practical implementation of the GDPR in the area of C-ITS."[43] At the same time, the National Highway Traffic Safety Administration (NHTSA) seeks comment on ways to provide consumers with more of a choice to "opt in" to V2V technology.[44] The draft Regulation on Privacy and Electronic Communications presents a transferable solution as a way out, preventing data privacy laws from being bottlenecks for the connectivity-enabled disruption of the mobility market.

The proposed near-term solution suggests a practical and expedient way to solve an upcoming issue where privacy and technology may collide, with a net benefit of seamless interaction for the user and the requesting services. The solution, however, fails to improve the privacy and control of the individual, merely extending a current interaction method that is functional but prone to legal challenge. As technologies advance, we should strive to improve the quality of all aspects of interaction models, not just provide additional functionality. As such, the systems of tomorrow should include both technological improvements as well as better and more complete solutions to human comfort and ethical issues such as privacy and trust.

---

43. A European Strategy, *supra* note 12, at 11.

44. *See* Federal Motor Vehicle Safety Standards, 49 C.F.R. § 571 (2016).

IV. Abstracting Privacy Control: The Virtues of Privacy-as-a-Service

As mentioned previously, in the future of V2V and V2I communications it is expected that a travelling vehicle will encounter requests and receive information from many separate agents such as other vehicles and infrastructure components, potentially in very short periods of time if not in a constant stream. The potential for a barrage of data sharing requests to a driver who, despite the autonomous nature of the vehicle, is expected to be prepared to take control at any point, creates a situation in which deciphering the nuances of any given terms of service or even recognizing the requesting entities may be an impossible challenge. It is therefore obvious that the 1:1 approach we employ today—in which each requesting entity presents a privacy policy to the engaging party, and then waits for the party to positively respond by accepting or rejecting the terms—no longer makes sense in this fast-paced future with a hyper mobile society.

Because current methods do not meet the needs required in a fair exchange, we must strive to create new systems that meet the needs of all interested parties. The basic options to solve this issue appear to be threefold: (1) limit information ecosystems to those that do not collect personal data and therefore do not require terms of service agreements and thereby forego the data, revenue, and quality of life improvements such ecosystems provide; (2) manage privacy offline such that permissions are granted to specific entities prior to their being requested; or (3) dynamically manage privacy in the moment, as we do today. Each of these options has its challenges, and in order to unlock the power of available data while maintaining privacy, we believe that a hybrid approach is required that transcends the individual's management of privacy choices at the moment of access.

A. The Need for Privacy Control—From Illusion to Reality

In addition to the fundamental belief that the user is entitled to an appropriately unencumbered experience when interacting

with the broad array of services that make up the digital life of today and tomorrow, there exists the need for a sense of user control over the types of data that are being shared with all entities involved in the digital services ecosystem.[45] Additionally, the ability to meaningfully maintain access after the fact through review, editing, and wholesale revocation must be respected. As the number of services users interact with on a regular basis become more and more digitized, the opportunity for these services to request and collect personal data increases. Additionally, as the number of digital entities a user interacts with on a regular basis goes from a small number to hundreds or thousands, the ability to understand and maintain an accurate inventory of what data is shared with which entity may become impossible, leaving the user with a feeling that they are no longer in control of their privacy. Even today, in a world of third party cookies we see concerns about privacy regarding what details entities or groups of entities know about a given person.[46] As technology has progressed without adequately keeping privacy in mind, consumers find themselves in an environment ripe for abuse or exploitation by unscrupulous actors. In today's new world even trusted entities may have knowledge of the individual that is described by the consumer as "creepy." The sense of helplessness and confusion the public experiences when realizing that someone knows too much is coupled with their belief that they are unable to meaningfully do something about it.[47] This then manifests in feelings of distrust and discomfort regarding data oriented systems in general, thereby creating a collective cry for help that gets the courts and regulators involved. There is a

---

45. *See generally* Glen Nowak & Joseph Phelps, *Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters*, 9 J. DIRECT MARKETING 46 (2005) (discussing the importance of control with respect to individuals' views of privacy).

46. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW. RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

47. IRINA SHKLOVSKI ET AL., LEAKINESS AND CREEPINESS IN APP SPACE: PERCEPTIONS OF PRIVACY AND MOBILE APP USE (2014), https://pdfs.semanticscholar.org/a9b0/e4481dfe588cf104baf7a8b7876dd94574d7.pdf.

compound complexity regarding personal data today: the general public is uninformed about what data is collected, the collecting entities are minimally transparent regarding why collection occurs, revocation is nontrivial, and solutions from courts and regulators are often overreaching, difficult to enforce, and circumventable. The consumer requires control of her data, a sense that she is ultimately granting access when appropriate and that she is able to rescind it at will, immediately and unapologetically in as simple a fashion as is possible.

B. The Need for Transparency

The concept of having a "trusted relationship" with a digital entity is abstract at best. The exchange engaged in is often a trade of individual and potentially private information for access to a helpful service. That information is then used, often in opaque ways, to later monetize the use of the service through advertising, lead generation, or other means.[48] The understanding of what is being exchanged and why is often vague, while the instant gratification of meeting a specific need suffices to distract the majority of consumers from too deeply considering the actions they have just taken. Privacy advocates and those devoting additional time to contemplating the quid pro quo in these digital exchanges have an uphill battle when the public appears not to care until some trigger experience occurs and suddenly they feel betrayed or victimized. Research has shown that the public is often unaware or misinformed regarding the specifics of what agreements have been made, what data is under the control of the offending entity, and what entity is actually involved.[49] In this way, it is reasonable to assume the user has little understanding of how to regain control of that data and therefore, the terms of the relationship (e.g. to edit, erase, or

48. *See* Laurence Ashworth & Clinton Free, *Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns*, 67 J. BUS. ETHICS 107, 111 (2006) (describing the "exchange model of online marketing").

49. *See* TUROW ET AL., *supra* note 10, at 4 (finding "that large percentages of Americans often don't have the basic knowledge to make informed cost-benefit choices about ways marketers use their information").

completely rescind access permanently). An appeal to an authority is a likely response, with the courts and enforcement agencies weighing in on the apparent exploitative behavior in the worst cases and then further crafting policy and law to protect the offended public and punish egregious offenders.

Increased and true transparency for the user is one answer to these problems, both as a means to enable review of what has happened when a surprising situation occurs as well as to provide a method to reduce the likelihood of such a surprise occurring in the first place. Complete, consistent, and standardized transparency is sorely needed; not just within a given data collecting company or sector, but across entities and sectors. A common language, a standard format, and an accessible record can all go a long way in helping consumers feel comfortable and more importantly "in control" of their data, and the privacy oriented relationship they have with any given entity.

V. Privacy-as-a-Service: A Solution to Enhance Privacy While Promoting Data Sharing

A. The Complexity of Privacy

The number of services, the rate of changes these services experience, and the complexity and nuance of personal data access requested are only going to increase in the future. As such, it is not a stretch to assume that managing privacy will increasingly require a level of attention and knowledge that is a burden to the common individual. The resulting behavior due to ignorance and "privacy fatigue" is that the user is likely to give up and grant access to data they would otherwise never grant, and to entities that are not held to appropriate standards based on what they are requesting.[50] We are at a point in which our approach to permissions is exploitative and broken, but it remains successful only because the consumer cannot

50. *See id.* at 9 ("People we meet have decided they seriously cannot . . . do anything else that will allow them to manage their personal information the way they want. . . . They have slid into resignation—a sense that that while they want control over their data world they will never achieve it.").

meaningfully interpret what she is agreeing to. This is a fragile ecosystem, subject to massive disruption if the public protests too much due to the feeling that their control is overly threatened. In the interest of righting this imbalance, whereby services and products take advantage of the current ecosystem of ignorance, a Privacy-as-a-Service model makes sense.

B. A Configured Solution Can Address Privacy Complexities for Future Digital Services

Imagine a future scenario in which a driver enters her autonomous car, runs a number of local errands downtown, crosses a toll bridge to have lunch with a friend, and then returns home. During her time in the car she listened to music, browsed for clothing, and made a phone call. Throughout this scenario a huge number of vehicles and machines would have communicated with her vehicle for a wide variety of reasons. Infrastructure beacons collected information about her car to monitor traffic data and to understand that she is a local commuter, a routing service from her car connected to her digital task list in her cloud based computing system to plan a route for guiding the car on the most efficient path to run all her errands, the parking garages and tolling systems identified the vehicle and charged her accounts appropriately, and other vehicles traded data with her vehicle about road hazards, and recent hyperlocal map updates like street conditions. All of these things happened seamlessly, without interrupting her browsing, music listening, or phone call, though several of the services required negotiating permissions for access to different levels of personal data and many of the services were connecting to her car for the first time. Imagine further that this situation plays out in a way that she maintains complete control over what personal data is shared, at a granular level, with each requesting entity, and that she can review, update, and revoke all prior and future data collection (or edit her preferences) at any time. This transparent, configurable, privacy protecting methodology could be available if we abstract today's data permission interaction models into a robust Privacy-as-a-Service approach.

C. A Solution That Respects the Needs of Consumers with Varying Opinions Regarding Privacy

Personality differences will account for varied levels of interest and comfort in negotiating privacy and the granularity of information an individual is willing to share.[51] Additionally, the amount of time an individual wants to spend on such configurations will differ. A Privacy-as-a-Service system can provide coarse tolerance levels that create generic "risk level" defaults that a user can then manipulate as they see fit, if they so desire. After setting the preferences, the configured device (such as an automobile) will then negotiate privacy according to the service based on the user configuration. Machine management of personal data will be necessary, and this is one solution to maintaining privacy and giving the user actual control over what types of data are shared, how, and with whom. The balance of power is therefore restored to the user.

Similar to how consumers will vary in how much interest they have in general privacy, the amount of trust in each data requesting entity will also vary.[52] There can be no automatic consent, nor should there be the expectation of a wholesale sharing of a full privacy payload, even to a fully trusted actor. A person may be fine sharing their car model with a data-collecting stoplight (so that it can estimate weight and thereby provide data to a smart city for estimating road wear) but may not want to also provide a Vehicle Identification Number. For many of the current well-known data requestors in the mobile application and social media space, true granularity of data permissions is nonexistent.[53] In the future, granularity as an aspect of privacy

---

51. *See generally* Stefan Stieger, Christoph Burger, Manueal Bohn & Martin Voracek, *Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addiction, and Personality Between Facebook Users and Quitters*, 16 CYBERPSYCHOLOGY, BEHAVIOR & SOCIAL NETWORKING 629 (2013) (discussing the effect of personality on individuals' privacy concerns).

52. Matthew Quint & David Rogers, *What is the Future of Data Sharing?*, SLIDESHARE (Oct. 30 2015), http://www.slideshare.net/DavidRogersBiz/what-is-the-future-of-data-sharing-consumer-mindsets-and-the-power-of-brands (last visited Apr. 24, 2017) (on file with the Washington and Lee Law Review).

53. *See* Supriya Shinde & S. S. Sambare, *Survey on Privacy Permission Management Approaches for Android OS Applications*, 107 INT'L J. COMPUT. APPLICATIONS 14, 14 (2014) (arguing that "a new mode of privacy is needed in

control may be a key consumer expectation, potentially adding significant additional time-consuming complication to the common request-for-consent model, further revealing its inadequacies in the current state.

A primary contributor in today's asymmetry of information between consumer and data requester may be the false sense of choice (or the "illusion of control") a user is often given when making personal data sharing decisions with digital systems.[54] In many cases the user can only grant or deny wholesale access to classes of personal data (such as members of a contact list) with minimal insight into why this access is necessary and with the penalty that, by not sharing this information, the product or service is wholly unavailable for use.[55] The user is not provided with the ability to negotiate privacy at a more granular level but, rather, can only choose the more convenient, expedient, and potentially overreaching binary choice provided. The onus is on the user to either comply or completely forego use of the service. By contrast, in a managed solution to privacy there can be a re-empowerment of the individual user by taking advantage of the shared nature of the general management settings through a Privacy-as-a-Service provider. Overreach will be "punished" by denying the offending service the access to data the community has determined is overly sensitive or unnecessary for the requesting service and that is thereby suppressed through the Privacy-as-a-Service system by default. For those who want more fine-tuned control over their personal data, granular privacy settings can be employed to describe what each user is comfortable with sharing, when they are comfortable sharing it, and to which types of or with what specific entities these rules apply. In this way, a system requesting access rights across a

---

smartphones").

54. *See* Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 J.L. & POL'Y FOR INFO. SOC'Y 723, 745 (2008) ("Under the Federal Trade Commission's notice and choice regime, the operating assumption is that people will make good choices if they are provided with good information. Our studies have found that Americans do not have good, i.e., full and understandable, information about data practices that affect their privacy.").

55. *See* Masooda Bashir et al., *supra* note 8, at 2 ("Either the user agrees to give up all their personal information to the service or they choose not to use the service at all.").

broad body of individuals will be required to "play nicely" and remain sensible and transparent regarding data requests or else they will find themselves denied access to a majority of potential users. In popular Privacy-as-a-Service systems, this could prevent access to millions of users. In short, for the first time in the history of digital privacy negotiation relationships, Privacy-as-a-Service enforces that the types of data collected must make sense to the community and the Privacy-as-a-Service provider, lest the request be wholesale denied. As an additional benefit, granular control of data sharing provides a path for data markets or data exchanges to appear whereby a user has the option to provide specific types of non-crucial additional personal data to particular requesting entities in return for some tangible benefit.[56] No longer is the privacy negotiation quid pro quo simply "all of my privacy in return for your service."

D. A Wiser Use of Privacy Cycles

The last thing consumers should be expected to do is to increase their time spent on the minutiae of managing privacy. As a majority of consumers are neither privacy experts nor versed in legalese, expecting them to fully comprehend a Privacy Policy or Terms of Service and thereby make an informed choice, is somewhat absurd. The time an individual spends thinking about and managing privacy efforts (their "privacy cycles") would be better spent researching professional entities with whom they can trust the management of their privacy. The onus would be on these private management entities (PMEs) to determine an individual's privacy requirements and then provide a management service layer with which to facilitate the permissions and data transfer in M2M communication where privacy payloads are concerned. In other words, an individual

---

56. *See* Mark van Rijmenam, *Monetizing Your Personal Data: From Data Ownership to Data Usage*, LINKEDIN (Sept. 1, 2014), https://www.linkedin.com/pulse/20140901120954-15537165-monetizing-your-personal-data-from-data-ownership-to-data-usage (last visited Apr. 24, 2017) (discussing "Big Data startups that are developing personal data marketplaces" and "empowering consumers to determine what's done with their data and receive monetary rewards for the usage of their data") (on file with the Washington and Lee Law Review).

would give the managing entity the rights to make decisions on her behalf, such that the distractions and time sensitivity of data permissions would be abstracted away from her while allowing her to remain in control of the rules governing privacy decisions. In this way, the user focus on privacy is extremely efficient and meets many needs rather than requiring a fragmented and interruption-driven focus from specific information seeking entities at time of product or service use.

E. An Audit Trail

An additional requirement of such a Privacy-as-a-Service ecosystem could be to create a standardized audit trail via request logging in which each requesting entity must identify itself with a consistent and public unique user identifying number (UUID), include an additional unique "request ID" per request, and explicitly enumerate the types of data requested. This request information is then written to a local (to the user) audit log along with a timestamp and location (e.g. GPS). The Privacy-as-a-Service provider and the individual will then have full transparency into who has asked for information at what point in any given journey and what the outcome of that request was (e.g. what was shared in return). The UUID would be registered publicly to a responsible and separate neutral third party in charge of maintaining the identification mapping of UUIDs to organizations. Additional good-faith functionality that could increase the likelihood that an entity is considered trusted by a privacy management service would include the ability to easily request a personal record of what is known about the user and automated "right to be forgotten" options such as programmatic privacy data editing, single entity data erasure, or complete removal of all information from all known entities. As such, an engaged individual utilizing Privacy-as-a-Service could easily retrieve (either from the vehicle or machine that was utilized or through the Privacy-as-a-Service provider) and understand all data they have shared at any point with any given entities as well as request that all or specific personal data be completely erased in one single command. This audit trail reduces traditional asymmetry of information issues that users

experience in modern systems whereby it is difficult or impossible to understand the who, what, and why regarding their personal data footprint.[57]

F. A Managed Service

Privacy-as-a-Service could function in a manner similar to a virus protection service where a user subscribes to a fee based service or one managed by a nonprofit organization focused on privacy principles such as the Fair Information Practice Principles for privacy (FIPPs). A user could research available Privacy-as-a-Service providers, subscribe to their service and create an account, register vehicles or machines that the service would manage, select privacy configurations for any or all registered objects (including default settings based on risk tolerance), and then connect each machine to the service.

Such trusted providers would maintain a database of white and blacklisted entities for purposes of negotiating the sharing of privacy data based on users' configurations with this database being updated frequently. Organizations who choose not to register could be summarily denied when making a data request to any subscriber of that (or any) service. Bad actors that get blacklisted for not behaving appropriately could have access rights immediately rescinded (a powerful, crowdsourced trust revocation function) as Privacy-as-a-Service providers remove them from their configured whitelists, compelling them to behave or suffer reduced or fully rejected access rights to a huge population of users. Never before has the user had the power to be a part of a managed privacy system that benefits from multiple sources of input (e.g. other users) in order to collectively bargain for privacy in a "unionized" way. Akin to reputation systems in other contexts, the white or blacklisting of given entities based on the input of many independent "subscribers" can function to quickly modify offending requestors' behaviors and promotes more careful and mindful future behavior on the part of the requesting entity. No longer would blanket access be

57. *See* Masooda Bashir et al., *supra* note 8, at 2 ("Because most users do not take the time to read and understand privacy disclosures, their comprehension of service providers' policies is likely to be low.").

acceptable, or nuanced terms buried in a Terms of Service document suffice. Such a service is a powerful, independent check on the behavior of requesting parties and can function as a self-governing system, reducing the need for oversight.

G. Better Protected and More Open With Data

When citizens are comfortable in their privacy choices and are given the transparency they desire, their sense of control is increased. There is an argument to be made that this will actually increase the types of data a citizen is willing to share with trusted entities due to the comfort and security in knowing they or a trusted partner can review an audit trail and that their data can be deleted or modified on command.[58] The opportunity to regain control at any point in time, to realize a mistake, or to modify one's choices about any or all aspects of her personal information is a key missing element in our modern privacy systems. The consumer should feel a sense of relief and privacy control when engaging with an established Privacy-as-a-Service provider, secure in the knowledge that a highly specialized service is managing her privacy needs. The outcome of this comfort may be that, in the right circumstances, consumers are willing to share even more data than they were previously. A managed privacy service model provides users with the comfort to share only the data of their choosing with specific responsible and transparent third parties, who may then have access to in-depth data that is user-certified as accurate, current, and available for use—the type of data these parties can only dream of taking advantage of today. This also broadens innovation possibilities and could spawn new ecosystems not yet imagined. No longer is the conversation between a user and the opaque end product. Instead, a professional service stands in the middle, maintaining a much-needed balance of power, and providing a constantly vigilant and mindful approach to the valuable asset—both monetarily and psychologically—of one's personal data.

---

58. Quint & Rogers, *supra* note 52.

H. Current Challenges to Employing Privacy-as-a-Service

Employing an automated privacy management service in V2V communications is not without its challenges, and may require specific adjustments or agreements on key interpretations of legislature such as the GDPR.[59] For example, the requirement of a "clear affirmative act" must be understood to include a preconfigured or algorithmic rule set. The concepts of users making "informed" and "specific" agreements as a part of consent also may be considered challenging in an automated approach.[60] These challenges, however, are surmountable if it is interpreted that the consumer, through careful configuration of her personal privacy policy regarding consent is merely abstracting the choices she would otherwise make to an automated system.

As mentioned in Part I of this paper, current settings in a web service apply this functionality regarding acceptance of tracking cookies, though, recently, many websites ask for explicit user agreement as well. As methods of the communication of private data change, the industry must take a best effort approach to respecting and enabling all phases of the privacy lifecycle: consent acquisition, appropriate data use, review, revocation and editing options. So long as this remains true, current (and near future) privacy law may be interpreted to allow for a configured Privacy-as-a-Service system. If such interpretation is not possible, it is believed that ideas around automating and managing consent can be used as guides for the improvement of future privacy laws in a world where "privacy payloads" become ubiquitous and interaction and decision times may be reduced to milliseconds.

VI. Conclusion: Control, Transparency and Improved Opportunity

Privacy is about control of personal information, and today's approaches to privacy management, originating from analog interactions, no longer fit with the realities of rapidly evolving

59. Recital 32 of the GDPR is one example. Council Regulation 2016/679, *supra* note 21, at L 119/6.

60. *Id.*

digital services. Terms of Service are overly complex and voluminous and so are rarely read and understood by the average user. Future advanced services, which promise additional levels of abstraction and complexity, also demand a need for a more tenable approach to privacy management. As time goes on, and current systems are built on outdated underpinnings, the paradigm of digital privacy becomes a convoluted system of court-ordered restrictions, illusions of user control, and feeds into a public paranoia over the lack of understanding about what personal data a shady and rarely understood "they" are collecting and what "they" are doing with it. A sense of defeat becomes a common response for a public that simply wants to interact in the digital communication economy. The complexity and obfuscation of today's consent systems for sharing private information are a result of organic evolution and adaptation rather than a planned and controlled holistic approach to privacy outcomes.

In the short term, to enable V2V, V2I, or any other M2M communications with privacy payloads in a high frequency or even a constant stream, the requirements for valid informed consent in a dynamic and communication based mobility ecosystem need to be more generally applicable. A suitable and user-friendly solution is the device (vehicle) configuration stage, where a driver can choose, or opt-in, connectivity functions and, thus, grant consent based on a level of transparency similar to "accept all third party cookies" as a comparable setting to control the flow of information to and from a device. But, in the longer term, especially as the age of V2V and M2M communication is upon us, this methodology will need to improve.

As such, a new approach is called for. This approach must be fair, must return the power of privacy to the consumer, and not be used as a tool of coercion for common service use. This approach should meet the needs of the user first, but also allow for a robust ecosystem of information sharing in order to improve our world by enabling innovation, make living easier, and make lives more enjoyable. The solution must also fit easily into a world in which multitudes of permissioned communications are occurring at a rate that is beyond the power of an individual to react to in a meaningful manner. If such an approach is not taken, we will soon come upon a point of "privacy fatigue" (if we are not already there) in which a user's privacy management

becomes little more than background noise; not because it is unimportant, but because the user can no longer bear to expend the time needed to meaningfully manage her permissions and the allowances made to the long list of requestors. Such a reality is an unfair outcome, a failure of a system, and a nightmare for privacy. We believe that a future that will incorporate large numbers of M2M communication use cases requires a more open and easily managed permissions system than exists today. This system must, however, first be in line with the user's needs and rights.

The future of digital privacy depends on returning control to the user in a respectful, sane, and manageable way that is tailored to the realities of new advanced services, with a sensitivity for the expected burdens of privacy management. A user should not be forced to trade undue amounts of time and effort in order to preserve privacy. By the same token, control of privacy must be returned to the user and made easier for them, lest the courts and regulators step in and tighten the regulations at the cost of innovation and economic opportunities. A balance must be struck, and users must be protected and in control.

Privacy-as-a-Service—an independently managed method of granular privacy control—can meet the needs of both the individual user and the industry at large. By algorithmically maintaining privacy functions through whitelists, blacklists, complex situational settings and real-time updates, the user can inherit the privacy expertise of a crowd-sourced and professionally managed service. A robust audit trail can provide an additional level of security, allowing users to feel comfortable in their privacy configuration choices and the choices they have shifted to the privacy management service. Any discomfort at the realization that unwanted actors or unwanted information has been shared can be addressed through the provided opportunity for immediate revocation, update of configuration, and removal of offending data from the collector. Due to this, data collectors will behave in transparent, ethical manners since their rights to access personal data are at risk at all times, contingent on their behaving ethically.

In addition to the ease of audit that compels data collectors to behave and be mindful of the data they collect, the power of a managed service is further enhanced by the critical mass of

subscribers it maintains. A bad or abusive actor in a managed system is not only blacklisted by the person experiencing the abuse, but may be added to the blacklist pool inherited by all subscribers with those particular settings. As such, industries are kept in check regarding the types of data they collect and are forced to justify this collection at risk of losing access to some or all information from a critical mass of users. This mechanism acts as a governor of sorts, and can be adjusted over time as new industries are created, allowing for adaptation within the defined system such that new and unimagined ecosystems are allowed to flourish.

While the net benefits seen by such a system of managed privacy are difficult to quantify, it is believed that by giving users a greater sense of true control over their private data through the inclusion of a professionally managed service, an audit trail, crowdsourced and automatic updates, and choice at whatever granularity they choose, consumers will be far more comfortable sharing additional data with trusted entities. As long as the trusted actors remain trusted, more data will be shared and available for the development of ever-more innovative services. If this trust relationship changes through an inherited change from the managed system or through the opinion of the individual, a simple process takes place: preferences are updated, permissions revoked, and users will demand that their data be deleted. The opportunity to expand the types of data gathered as the markets, society, and privacy attitudes change represents a bold new approach to an age old topic: how to maintain users' control of their privacy while allowing them to exist within their modern world. Privacy-as-a-Service meets this need, is adaptive to the future's next challenges, and represents an answer to the data sharing and permission onslaught we expect to see in emerging M2M technologies such as V2V communication. Such a solution maintains, expands, and increases the value of personal data while preserving privacy, not through applying an algorithmic obfuscation to a current framework, but rather through a more basic and fundamental approach. By redefining the way in which privacy interactions occur and the relationship between the user and the requesting entity, we provide a way forward in which privacy is maintained while innovation is allowed to continue (mostly) unfettered.