Privacy4Cars is pleased to present this statement to the European Data Protection Board's (EDPB) "Guidelines 01/2022 on data subject rights - Right of access." Data subjects in Europe are demanding to know how and where their personal information is being gathered and stored. The EDPB has been diligent in focusing on the protection, transparency, and use of personal data and we commend the EDPB for inviting comments from the public.

I founded Privacy4Cars to provide simple and pragmatic ways for businesses in the automotive industry to respect individual privacy. For consumers, we offer a free service for asserting their data rights over the information collected about them by today's vehicles. We have first-hand experience in the industry and we work with many industry players who are frustrated with how modern vehicles, services, and apps retain personal information and the significant risks associated if not properly protecting the data stored in vehicles and transmitted by vehicles.

The EDPB previously clarified in their guidance on connected vehicles that deleting personal information of consumers (including minors) stored in cars is mandatory and CARA, the association of European remarketers, subsequently published a whitepaper stressing that this data clearing is obligatory before reselling or re-renting vehicles. Yet, there is no evidence to date that this requirement is being addressed at any scale by the main vehicle rental or remarketing companies in Europe. Audits continue show nearly 4 out of 5 used cars still contained personal information of previous owners, a clear violation of GDPR and ePrivacy rules.

At the same time, privacy and security risks to consumers continue to grow as a direct result of companies in the automotive ecosystem refusing to offer consumers more granular choices for consent and control over how their data will be used. Privacy policies and terms of service agreements are written by auto manufacturers and third party service providers to give themselves ownership of personal information, often with the right to use it in perpetuity and for whatever purpose they see fit.

Vehicle manufacturers and service providers collect massive amounts of personal information through sensors in the vehicle, like precise geolocation, biometrics, detailed behavioral profiles of drivers and occupants (including minors), video and voice recordings, garage codes (associated with home addresses), and, when people sync their phones - a safety requirement in the Union to enable hands-free controls - a

treasure trove of personal information is sucked out from the phones into the vehicles, including contacts, call logs, text messages, unique identifiers that make it easy to re-associate this data with specific individuals, and in recent vehicles much more, including social media account information, photos and files present on the phone, calendar entries, financial and health information, etc.

Even more sensitive information is collected via mobile apps and a robust ecosystem of third party data brokers who buy and sell personal data to a variety of organizations beyond the auto industry, including law enforcement and government. There is a growing breed of companies that collect and share personal data collected by cars. Privacy4Cars, currently tracks more than 500 companies that have access to data collected from consumer vehicles, many of whom use this data for profiling and automated decision-making.

For example, many vehicle telematics-based services are advertised to consumers with phrases such as "drive with confidence, knowing an Emergency-Certified Advisor is ready to help no matter what happens out on the road." In reality, when consumers sign up for those safety services, they typically don't realize they are also granting companies the right to use their personal information for personal profiling, advertising, or even selling it to insurance companies and data brokers.

Below are 5 critical lessons we learned by working with European citizens who used our free consumer service, which we hope the EDPB will take into consideration. Consumers using our service have the option to appoint Privacy4Cars as an agent so that we may act on their behalf to reach out to data controllers in the automotive industry to confirm who is in possession of their personal data and to exercise their right for it to be deleted. Unfortunately, in our role as appointed agent, we've seen numerous instances of organizations struggling to respect data subject rights.

1. First, we often receive a generic, automated response that does not address the data subject request even as their designated agent. For example, Apple simply responds with a reference to the privacy policy for Apple CarPlay, yet there is no such section in their privacy policy. Knowledge about what data is collected by Apple's product remains completely opaque to the data subject.
2. Another common response to agent requests sent on behalf of a data subject is for data processors to remove the agent from communications, sending unexpected and confusing emails directly to the consumer. The additional friction and harm caused by circumventing a data subject's legally appointed agent is prohibitive for many consumers trying to exercise their rights under GDPR.
3. Third, some organizations, including data brokers that collect personal

information directly from a consumer's vehicle, claim they have no obligation to respond to data subject requests, leaving a significant volume of personal data beyond the reach of data subjects, to whom it belongs. In certain cases, these data brokers push the request off to the vehicle OEM, claiming they are just a data processor.

4. We've also encountered unreasonable friction on behalf of data subjects in regards to identity confirmation. While GDPR requires data controllers to verify the identity of an individual before disclosing any personal data, demands that data subjects provide even more personal information such as a passport, a national ID, or a recent utility bill (sometimes via parcel post) before engaging with a legal agent is an undue obstruction of consumer data rights.
5. Finally, a misleading or misunderstood use of "anonymized" data is frequently cited as a justification for being unable (or unwilling) to locate or delete the personal data requested. We strongly believe that organizations claiming the inability to delete personal data that has been repeatedly proven to re-identify data subjects (e.g. biometrics, precise geolocation, etc.) lack sufficient understanding to responsibility and legally collect it in the first place.

The above lessons we've learned from helping consumers in Europe points to a troubling and increasing trend toward manufactured obstacles that make impossible for consumers to understand who may have access or possession of their data, and by extension, the ability to exercise their rights under GDPR. I hope the EDPB recognizes the barriers all of this creates for consumer protection.

Thank you for your consideration and please feel free to contact me if you need additional information.

Sincerely,

Andrea Amico

Founder & CEO, Privacy4Cars

andrea@privacy4cars.com

https://privacy4cars.com