Fully connected, but transparent

WHAT THE EXPERTS FEAR …

Andrea Voßhoff, 58, is Germany's Federal Commissioner for Data Protection and Freedom of Information. It is particularly important to her that people be able to decide for themselves what is done with their data. Andrea Voßhoff holds a law degree and was a member of German Parliament from 1998 to 2013, where she was active on the judiciary committee.

For many of us, our car is an important symbol of our individual mobility and personal freedom. Accordingly, we have high expectations regarding the management of the data generated in connection with our cars. People don't want others to observe their driving style or the routes they take. There is no question that such data – which could be brought together via the car's registration number, for instance, and used to construct a detailed personality profile – falls into the category of personal information. Automakers, who are responsible for the IT systems in their vehicles, therefore have a duty to provide technical and organizational measures for data protection.

These days, however, this data doesn't stay in the car, to be accessed only in the repair shop. The increasing connectivity of vehicles poses the greatest challenge today. Two developments, especially, cause me concern. One is the penetration of the data-hungry world of the smartphone and all its apps into vehicles via cars' technical interfaces. The other is the standard which is currently being developed for communication between vehicles and with the transportation infrastructure, and which must conform with data protection principles. In both cases, we must intrude as little as possible into the privacy of vehicle users.

… AND WHERE THE GROUP STANDS TODAY

Data protection

At Volkswagen, the protection of personal information is a key part of the foundation upon which we shape our relations with our employees and customers. We want to fulfill our customers' expectations in terms of the advantages of connected driving. This will require us to process larger data volumes than before – while continuing to uphold our values of transparency, self-determination, and data security. In principle, anyone who gets into one of our vehicles should be able to determine how their personal information is shared and used. But not all data collected by vehicles is personal information, and customers can't decide on all services themselves. For instance, European law stipulates that the eCall emergency call system be installed in all new vehicles from 2018 onward. In an emergency, the system has to be able to send location data to rescue services.

and vulnerable to attack?

Cars have become rolling computers, from entertainment electronics to piloted driving systems. As with any digital product, the question is: how secure is it? With computers, security is always just a present state that can change at any time. With cars, on the other hand, people's lives are at stake, so the demands in terms of IT security are considerably higher than for household appliances in the Internet of things.

We've got used to cars lasting for 20 or more years through several generations of users. Will there be security updates for the entire lifetime of the vehicle? Or will a manufacturer be able to say after ten years that, from now on, a car will be driven at the driver's own risk? Who will be liable if a piloted driving system causes an accident? And, above all, who will assess this independently of the manufacturers? So far, it does not look as if independent assessments are being carried out to establish whether computers might be partly to blame in the case of accidents. Nor are there any independent investigations into how frequently autonomous systems help cause accidents. This means that any liability is shifted onto the drivers, even if they were the innocent victims of computers. The only explanation for this state of affairs is incompetence or a collective decision to look the other way. The government needs to issue clear rules and to introduce compulsory notification requirements. We also need clear recall rules for software.

Markus Beckedahl, 40, is the founder and editor in chief of netzpolitik.org and has been studying the impacts of digitalization on society and policies for 20 years. He is a cofounder of the Re:publica conferences and was a member of the German Federal Parliament's cross-party working group on internet and digital society.

Data security

In our increasingly interconnected cars, assistance systems are already being used to defuse dangerous traffic situations, helping drivers recognize them sooner or avoid them altogether. As automation advances, the car will take on more and more of these tasks, first intermittently and later perhaps completely. This will call for a high level of security in the corresponding systems, possibly necessitating regular security updates. We strictly separate the systems designed for comfort and entertainment from those that concern road safety, making for significantly better protection of safety-relevant systems in the event of a hacker attack on information and entertainment functions. We are additionally working on technical mechanisms to identify attempted attacks in and on internal vehicle networks.

Porträts: Uli Knörzer