



Data Protection – Personal Data

The Symposium on The
Future Networked Car

Geneva Motor Show 2016
3. March 2016

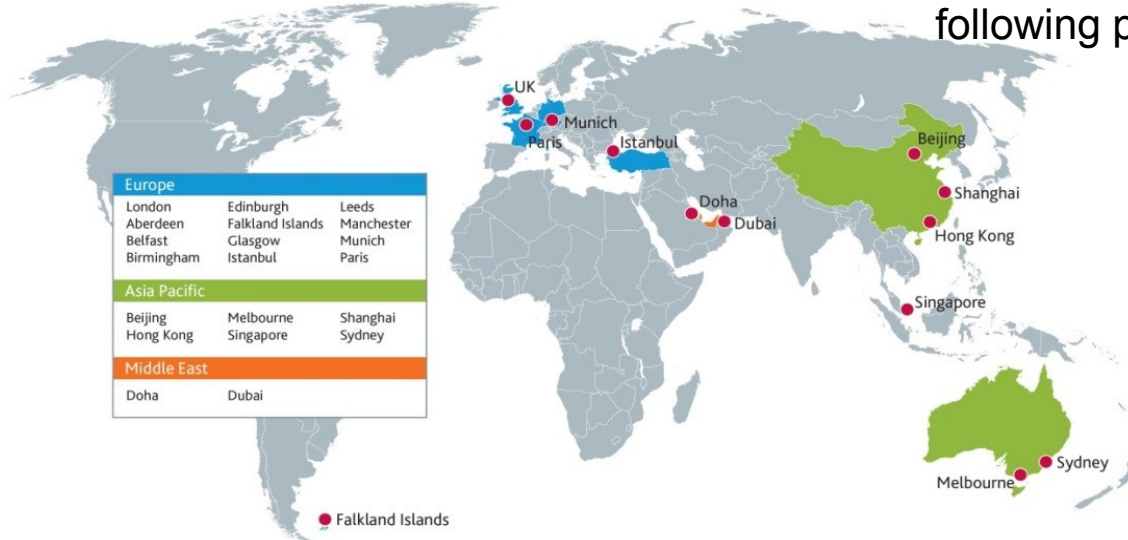
Pinsent Masons – Legal experts for Automotive & IT



Pinsent Masons

Pinsent Masons is an international full service law firm whose origins trace back to 1769. Today, the firm has a legal team of around 1,700 lawyers operating out of offices across Europe, the Middle East, Asia Pacific and Australia.

Our services are clearly defined, and the combination of sector experience and legal expertise ensures our clients receive the best commercial and legal advice for their needs. Pinsent Masons Germany provides legal services across the following practice areas:



- Corporate and M&A
- IT/IP & Outsourcing
- HR & Employment
- Litigation & Compliance
- Competition
- Real Estate & Property
- Banking & Finance
- Infrastructure & Energy Projects

- Introduction
- Privacy – A Personality Right
- Typical misconceptions about the term „personal data“
- Privacy Challenges
 - How to obtain valid consent
 - Pledges by Automotive industry bodies: US privacy principles and VDA
 - Specific challenges: EDR, embedded video cameras, eCall
- Big Data & Competition Law?
- Clashing principles: Does product liability require use of Big Data – despite privacy?

From Legacy to Digital – Disrupt the Automotive Industry

2019

- value of USD 131.9 billion
- 40 zettabytes of data
- 50 billion of connected cars
- 34.7% of annual growth rate

2025

- 100% of cars will be connected

2035

- 75% of cars on the road will be autonomous

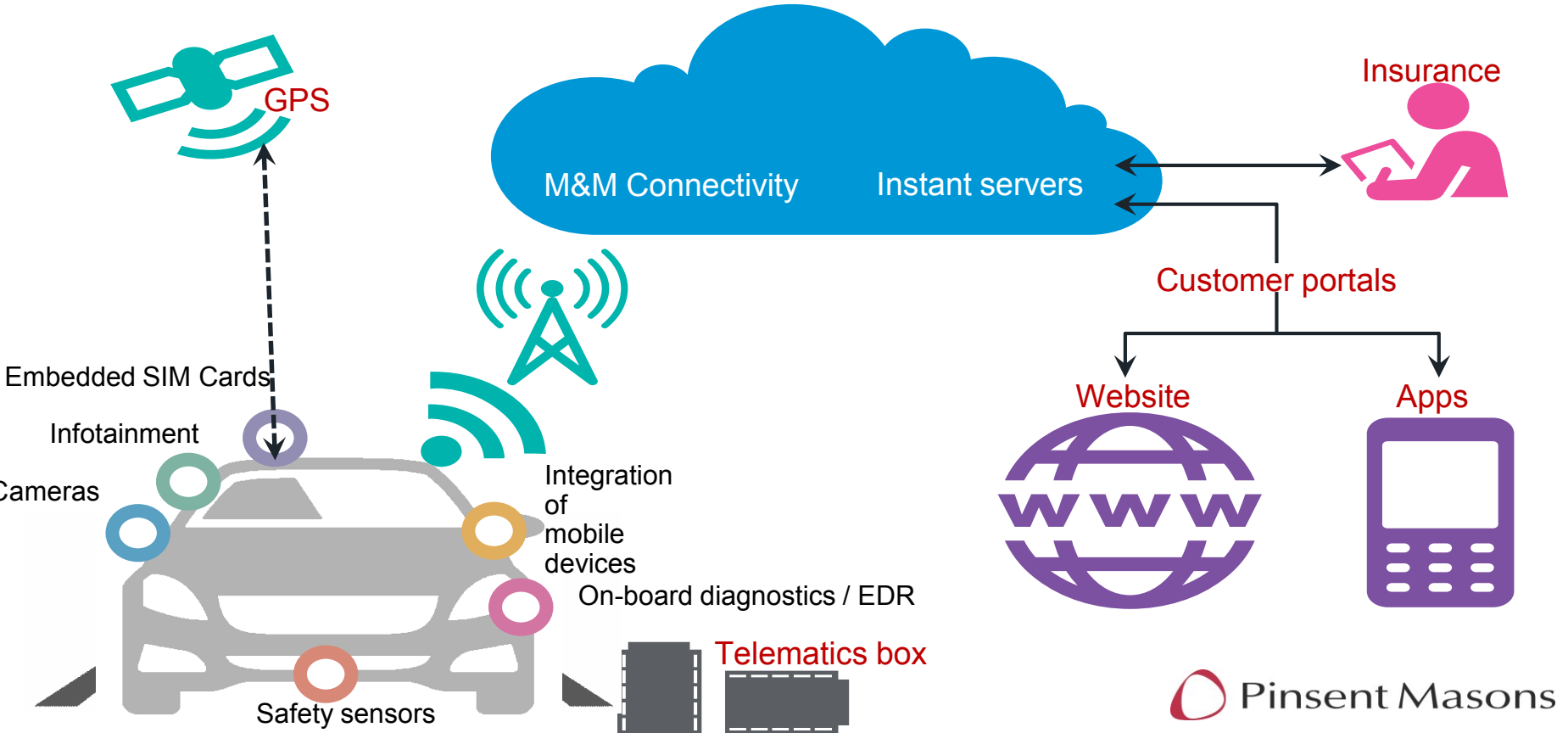


Legal Issues

- Data ownership
- Privacy
- Cyber attacks
- Telecom: Embedded SIM cards
- Competition Law
- (Product) Liability



The setting

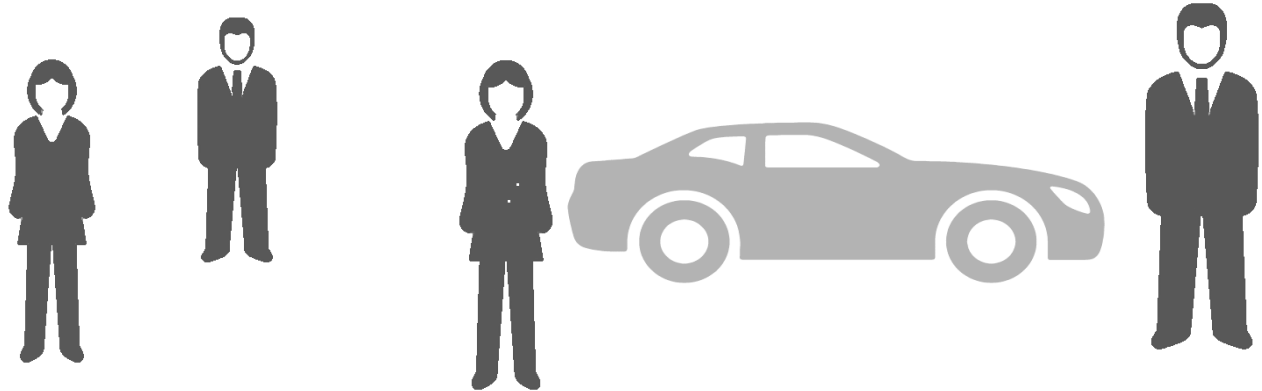


Introduction

The affected players

Who is involved?

- Customer, driver, passenger
- Car manufacturers, distributors, car dealers
- Tier 1, Tier 2
- Other hard- and software and infotainment providers
- Insurers
- Etc.



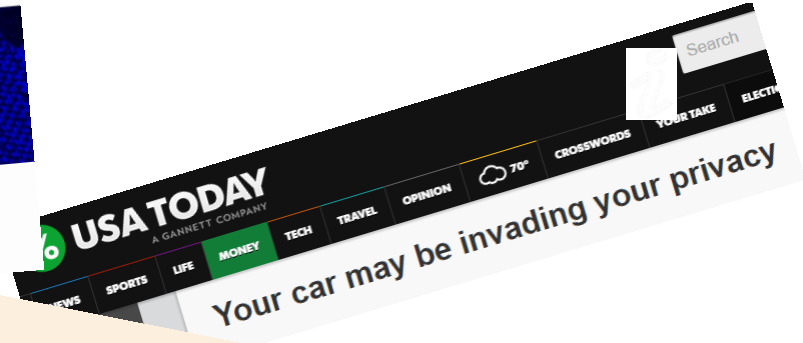
Who owns the data?

Who owns the data?

- Many stakeholders interested in data (OEMs, Providers of Infotainment, Insurance etc.)
- OEM's talk about "their fleet": No legal concept of ownership of data as such (according to German law), but
 - data carrier can be owned
 - customer owns data
 - IP rights: Data base right



Privacy is on top of mind



DIE WELT
Volkswagen-Chef warnt
"Datenkrake Auto"



The Washington Post
Technology

Web-connected cars bring privacy concerns

Some typical misconceptions... “*We have no issues with privacy, because...*”

“...we do not identify the user while using the data”

"Personal Data" means data which relates to


- an individual (not a company)
- who can be identified:
 - (directly) from that data (whatever information); or
 - (indirectly) from that data when collated with other information (theoretically !)
available to the data controller

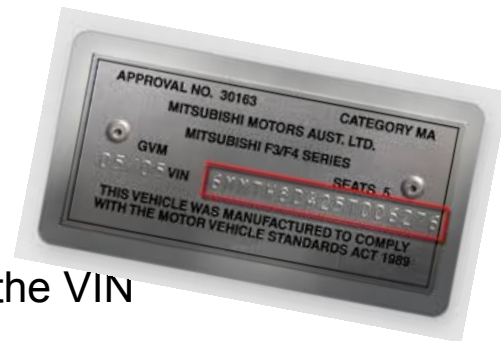
Note: The German Data Protection Authorities also consider data "personal data", if a person can (theoretically) be identified with additional other information that can be linked to the data.

Some typical misconceptions... ***“We have no issues with privacy, because...”***

“...we only use the serial number of the users device, so the data is anonymous.”

Examples of personal identifiable data

- IP addresses (123.456.78.90)
- Device IDs (DPAs: IMSI, IMEI, UDID are personal data)
- license plate no. 
- technical vehicle data is typically collected together with the VIN



“...we encrypt the data, so we are no longer using/receiving/sending personal data”

- encrypted data is still considered personal data -> someone has the key to decrypt!

Some typical misconceptions... ***“We have no issues with privacy, because...”***

“...we can use the users’ data for anything we want, as long as we keep the data to ourselves”

- Collection of data already needs legal justification, not only processing and transfer to third parties

“...Look: Facebook, MS, Google and Apple do the same, so we are OK...”

“...we anonymize the data, so we are not using personal data.”

- ⇒ Only when no reasonable way exists to
- identify (“single out”) a person
 - even when requiring correlation with other data sources (e.g. Big Data, phonebooks, information of third parties etc.)
 - by anyone (!) with the right resources

Uniform laws for a Global cross-border business?



“After 35 years, I have finished a comprehensive study of European comparative law.

In **Germany**, under the law, everything is prohibited, except that which is permitted.

In **France**, under the law, everything is permitted, except that which is prohibited.

In the **Soviet Union**, under the law, everything is prohibited, including that which is permitted.

And in **Italy**, under the law, everything is permitted, especially that which is prohibited.”

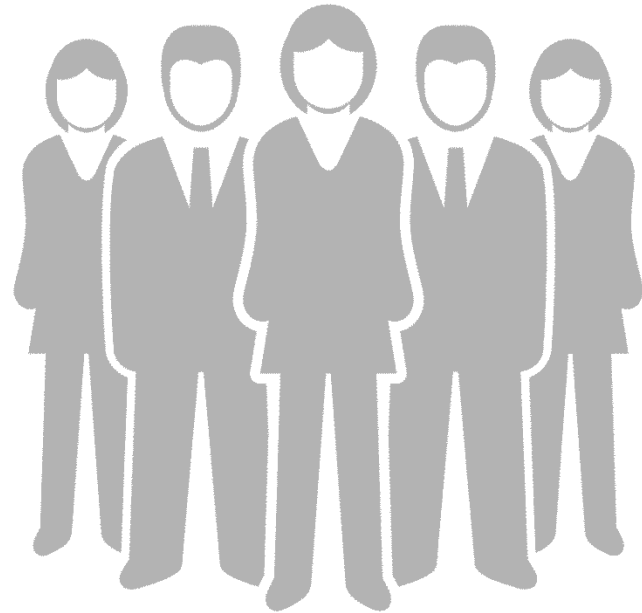
Privacy challenges

When is personal data processing permissible?

- **Soon:** General Data Protection Regulation: **One** law applicable for **all** Member States
- **EU:** Privacy laws are **harmonized** (Directive EC 95/46) but some differences in local laws of Member States remain

Straight forward rule:

- The Processing of Personal Data is forbidden unless:
 - **explicitly** permitted by data protection laws; or
 - the data subject has declared **consent** in advance to the processing concerned
- **Be careful:** Additional requirements for **international** data transfers to recipients outside



Privacy challenges

Consent requirements

Consent needs to be freely given:

- make sure services absolutely necessary for the customer can be used, even if consent is not provided.
- Problematic in a relationship of subordination: e.g. track employee's use of a company car

Issue: Requirement for vehicle owner to consent to a transfer of his/her Personal Data to companies abroad for general marketing activities or otherwise he is prevented from using his/her car's infotainment services



Privacy challenges

Consent requirements

Consent needs to be informed:

- explain to data subject, which data will be used by whom for which purpose.







Examples:

- Targeted advertising/offerings
- “Drive like a girl”: Black box insurance, pay as your drive
- Remote car diagnosis
- Swarm data use
-



Privacy challenges Transparency!

Informing data subjects via privacy policy / consent declarations...Bad examples by:

	PAYPAL 36,275 words
	HAMLET 30,066 words
	APPLE iTUNES 19,972 words
	MACBETH 18,110 words
	WINDOWS LIVE 14,714 words
	FACEBOOK 11,195 words

Privacy challenges

Consent requirements

Consent needs to be expressly given:

- make sure that consent is given in an **explicit** (“unambiguous” but hidden in T&C is not sufficient) way and documented.

Examples:

- **hand-written** signature on a consent form;
- “**opt-in**” tick-box in the car or online portal.

Note: Mere silence may not be considered as a valid declaration of consent; Unlike in other jurisdictions, “opt-out” is not recognized in Germany (except for specific



Privacy challenges

Different “standards” internationally



ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC. ASSOCIATION OF GLOBAL AUTOMAKERS

CONSUMER PRIVACY PROTECTION PRINCIPLES

The Principles are subject to change over time. When they do change, the Alliance and Global Automakers will post the updated Principles at www.automotiveprivacy.com and [\[redacted\]](#). The Principles are not intended to replace inconsistent or conflicting applicable laws and regulations, where they exist. So, the Principles should be interpreted as subject to and superseded by applicable laws and regulations. Participating Members may implement the Principles in different ways, reflecting differences in technologies and other factors. And Participating Members may choose to incorporate into their privacy programs elements that are not addressed in the Principles and are free to take additional privacy steps. But regardless of how Participating Members design their privacy programs and implement the Principles, Participating Members affirm the following fundamentals, as detailed in the relevant sections that follow:

- **Transparency:** Participating Members commit to providing [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of [Covered Information](#).
- **Choice:** Participating Members commit to offering [Owners](#) and [Registered Users](#) with certain choices regarding the collection, use, and sharing of [Covered Information](#).
- **Respect for Context:** Participating Members commit to using and sharing [Covered Information](#) in ways that are consistent with the context in which the [Covered Information](#) was collected, taking account of the likely impact on [Owners](#) and [Registered Users](#).
- **Data Minimization, De-identification & Retention:** Participating Members commit to collecting [Covered Information](#) only as needed for legitimate business purposes. Participating Members commit to retaining [Covered Information](#) no longer than they determine necessary for legitimate business purposes.
- **Data Security:** Participating Members commit to implementing reasonable measures to protect [Covered Information](#) against loss and unauthorized access or use.

2



Global Automakers Privacy Principles:

- common set of privacy standards
- implicit consent
 - by mere usage of services and technologies
 - shall be sufficient for the use of personal data for purposes beyond what might be necessary for the performance of vehicle technologies and services
- using and sharing personal data for advertising seems to qualify as “*reasonable and responsible use*”, apparently includes without explicit consent.

VDA Datenschutz-Prinzipien:

- Transparency
- Self Determination / Choice
- Data Security

Privacy challenges: Examples: Embedded cameras

Embedded Cameras

- Data protection authorities have recently **prohibited** the use of **dash cams** in cars.
- § 6 b BDSG:
 - Issue: “Observing” public space
 - Data subjects interests typically outweigh
 - Must be clear for people on the road/sidewalks that (i) camera is running and (ii) information about the data controller needs to be provided
- Authorities **tend to prohibit** embedded cameras to the extent cameras “use” live footage of the surroundings of the cars.



Note: The use of **cameras installed in a vehicle** requires very specific processes. Data minimization concepts might need to be applied, e.g. using **pixel footage** instead of full video mode.

Privacy challenges: Examples: EDR

Event Data Recorder (EDR)

- Required in the US
- Problematic in Germany:
 - Collection of personal data?
 - Who may read/obtain EDR data?
 - Consent required? But from whom?
 - § 6c BDSG: Are OEMs required to inform car owners about the fact that EDR stores data?



eCall

- European Council approved in December 2014
- Standard feature by March 31, 2018
- Was delayed due to privacy concerns / debate:
 - Not to be used for monitoring purposes
 - No constant tracking: “sleeping application”
 - Switch on /off ?
 - Must data set really include VIN?
 - Consent required?
- Draft Regulation by European Council:
 - Data (VIN, time and location of accident, number of passengers and direction of travel)
 - must only be used for purpose of handling the emergency situations
 - Delete thereafter
 - not traceable and is not subject to any constant tracking
 - No access before ecall is triggered
 - safeguards to prevent surveillance and misuse
 - Full and permanent deletion must be possible



Privacy Challenges

Breach consequences

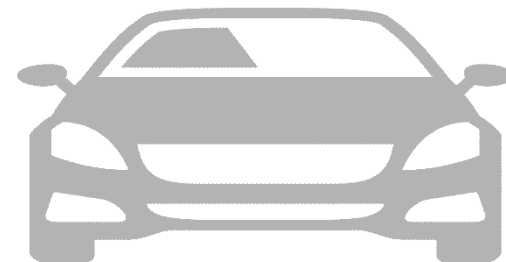
Risk of non-compliance with data protection requirements

- Fines up to EUR 300k (Draft GDPR: up to 4% of global turnover!)
- Enforcement action, including a prohibition on conducting the relevant data processing;
- Damages to affected individuals;
- Negative publicity and reputational damage - risking loss of future business and goodwill.



Data and Competition law

- Similar to sharing of technical information under Regulation (EC) No 715/2007 and Regulation (EC) No 595/2009: Will OEMs be required to share connected car data with independent garages?
 - OEM owned server vs third party managed shared server?
- Big Data: Abuse of dominance if OEMs generally keep connected car data for themselves?
- Exclusive access to unique source of data to boost after sale services: Fight between car manufacturers and independent repair sector: Who should have access to driver/car data?
- Lock-in consumers/suppliers by refusing data portability



Liability challenges

Product liability for automated cars

OEM/Suppliers must **ensure safety** of the product by

- using **objectively** required **technical measures**
 - Current **state of the art science and technology** and
 - What customers can **reasonably** expect (NB they can expect product safety even in cases of misuse (not: abuse)!)
- Vehicle **Big Data**: what is actually “objectively” required nowadays?
 - **Product development**: requirement to use vehicle Big Data for self learning systems?
 - **Instruction** of customers: Obligation to warn and instruct via **augmented reality** in real time and requirement to use **any available source** of data for risk minimization?



Product liability vs privacy

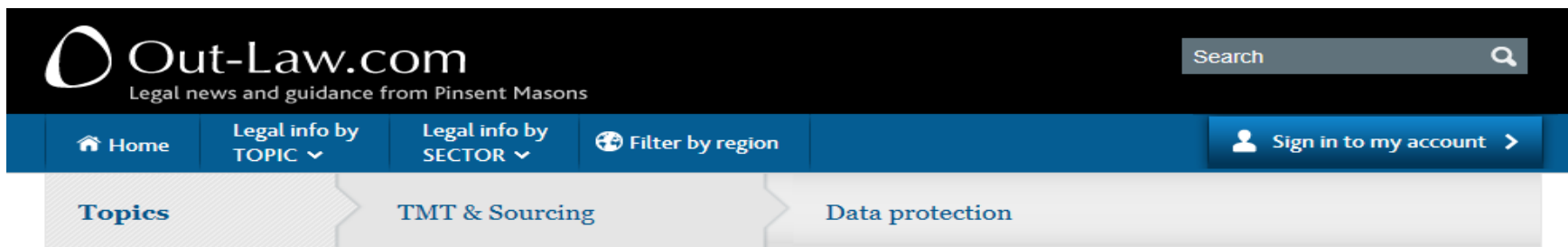
- *Product Monitoring (after sale):*

- requires manufacturer to monitor products after placing on the market to detect risks
- Required reaction: Warn + instruct and recall, but also requirement to collect “Big Data” from cars?
 - Required to link up data from CRM, technical service, quality assurance, R&D etc. as quickly as possible?
 - How to react: real time warning in MMI required?
- **Clash between Product Liability and Privacy requirements?**
 - Use of **VIN** inevitable = Personal Data
 - collecting car data must be based on permission by privacy law → disputed whether there is any
 - **Consent?** Informed?
 - Data minimization principle?




Legislative action required!

More info on Outlaw.com!




The screenshot shows the top navigation bar of the Out-Law.com website. It features the Out-Law.com logo and tagline 'Legal news and guidance from Pinsent Masons' on the left, and a search bar on the right. Below this is a blue navigation menu with options: Home, Legal info by TOPIC, Legal info by SECTOR, Filter by region, and Sign in to my account. A secondary navigation bar below the menu highlights 'Topics' and includes 'TMT & Sourcing' and 'Data protection'.

French data protection authority to focus attention on connected cars and smart cities

 Tweet 53

 Empfehlen 19

 Share 28

Join My Out-Law

- See only the content that matters to you
- Tailor Out-Law to your exact

1. 'Connected cars' age presents opportunities for manufacturers to improve recalls process, says expert (<http://www.out-law.com/en/articles/2015/may/connected-cars-age-presents-opportunities-for-manufacturers-to-improve-recalls-process-says-expert/>)
2. 'Connected cars' phenomenon raises data ownership and liability issues, says expert (<http://www.out-law.com/en/articles/2014/february/connected-cars-phenomenon-raises-data-ownership-and-liability-issues-says-expert/>)
3. US automakers agree new 'privacy principles' for connected car data (<http://www.out-law.com/en/articles/2014/november/us-automakers-agree-new-privacy-principles-for-connected-car-data/>)
4. White Paper on Connectivity in the Automotive Sector:
<http://www.pinsentmasons.com/en/media/publications/connectivity-in-the-automotive-sector/>

Thank You!



Dr. Stephan Appt, LL.M.

Partner

T +49 89 203043 561

M +49 174 333 2856

E stephan.appt@pinsentmasons.com

Dr. Stephan Appt advises national and international companies in commercial, intellectual property and information technology law matters, with a particular focus on the Automotive and IT sectors. His practice includes advising on the negotiation and implementation of all types of IT related agreements (including software development, licensing, maintenance services, software distribution and software-as-a-service) and outsourcing transactions, as well as providing strategic advice to clients concerning IT law matters (e.g. open source software, cloud computing and e-commerce) and related regulatory issues (including data protection and data security matters). Stephan assists clients in IT and IP disputes before regular courts and in arbitration proceedings.



Pinsent Masons Germany LLP Ottostraße 21 80333 München
T: +49 89 203043 500 F: +49 89 203043 501

Bank: Barclays Bank PLC, Frankfurt IBAN DE59503104000737438501 SWIFT BARCDEFF Amtsgericht München PR 1154

Pinsent Masons Germany LLP ist eine Gesellschaft in der Rechtsform einer in England und Wales eingetragenen Limited Liability Partnership (Registernummer: OC373389) mit Sitz in London, 30 Crown Place, Earl Street, London EC2A 4ES, Vereinigtes Königreich. Die Gesellschaft hat eine deutsche Zweigniederlassung mit Geschäftssitz in München an der oben angegebenen Adresse, eingetragen im Partnerschaftsregister des Amtsgerichts München (Registernummer: PR 1154). Bezogen auf die Pinsent Masons Germany LLP, bezeichnet der Begriff „Partner“ Gesellschafter (Members), soweit sie als Rechtsanwalt zugelassen sind, oder Angestellte oder Berater der Pinsent Masons Germany LLP oder mit ihr verbundener Gesellschaften, soweit ihre Stellung der eines Gesellschafters entspricht. Ein Verzeichnis der Gesellschafter (Members) der Pinsent Masons Germany LLP und der Personen, deren Stellung der eines Gesellschafters entsprechen, liegt am oben angegebenen Geschäftssitz in München und am oben angegebenen Sitz in London aus. Der Name „Pinsent Masons“ wird verwendet zur Bezeichnung der Pinsent Masons LLP und mit ihr verbundener Gesellschaften, einschließlich der Pinsent Masons Germany LLP, die tätig sind unter dem Namen „Pinsent Masons“ oder einem Namen der diese Worte enthält. Je nach Kontext bezieht sich „Pinsent Masons“ auf die Pinsent Masons LLP und/oder eine oder mehrere mit ihr verbundenen Gesellschaften.

© Pinsent Masons Germany LLP

Eine vollständige Liste der weltweiten Standorte findet sich unter: www.pinsentmasons.de



www.pinsentmasons.de



www.out-law.com



www.pinsentmasons.com