The Federal Commissioner
for Data Protection and
Freedom of Information

Privacy considerations for C-ITS and the connected vehicle

Michael Kiometzis, BfDI

9th ETSI ITS Workshop, 2018, Berlin

The Federal Commissioner for Data Protection and Freedom of Information

The Federal Commissioner…

… is elected by the Bundestag

- Two 5-years terms at maximum

… shares her responsibilities with 16 State Commissioners

- No responsibility for the private sector except for Post & Telecommunications

… has the following data-protection-related responsibilities:

Advisory service to	Supervision of	Participation in
• Bundestag • Federal Government • Public bodies at Federal Level • Post & Telecommunications • Statutory Social Insurance • Citizens (Ombudsman)	• Federal Government • Public bodies at Federal Level • Post & Telecommunications • Statutory Social Insurance	• All legislative work at federal level touching her data protection responsibilities

Data Protection Principles and GDPR

Lawful basis for processing:

- Processing shall be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child..

Purpose limitation and data minimisation:

- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR, not be considered to be incompatible with the initial purposes (‘purpose limitation’) and adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).

Transparency:

- The controller shall take appropriate measures to provide any information relating to the legal basis and the purposes of processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

Privacy by Design and Privacy by Default:

- Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.
- The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Integrity and confidentiality:

- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Rights of the data subject:

- The data subject shall have the right to obtain from the controller information about the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; the right to lodge a complaint with a supervisory authority; where the personal data are not collected from the data subject, any available information as to their source; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Furthermore, data subjects have the rights to withdrawal of their consent, to rectification, to erasure, to restriction of processing and to data portability.

Data Protection Principles and GDPR

- There is no legitimate purpose where processing of personal data can not possibly be compliant with legal obligations.
- The rights of use of personal data can only be granted for a well specified purpose, to the extend required for that purpose and will hold for no longer than is necessary for the purposes for which the personal data are processed.
- Without any other legal basis, data subjects must have explicitly given their consent for the processing of their personal data and they must be in the position to exercise their rights to withdraw their consent, to rectification and erasure of their personal data.
- Technical and organisational measures must ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

• Furthermore, data subjects have the rights to withdrawal of their consent, to rectification, to erasure, to restriction of processing and to data portability.

Addressing consumer concerns for cyber security, privacy and data protection

Use personal data only for well specified and consented purposes and erase them when no longer needed!

Provide granular and easy to use privacy controls for vehicle users enabling them to grant or withhold access to different data categories in vehicles!

Cyber Security and Privacy by Design should be implemented in a verifiable manner (type-approval requirements regulation should set minimum standards)!

C-ITS and Connected Cars

Permanently broadcast CAMs and DENMs to contribute to a common traffic situation picture to improve traffic safety and traffic efficiency

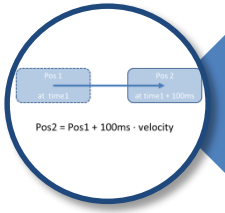
But especially CAMs might pose a severe privacy risk!

Cooperative Awareness Messages (CAM)

- CAMs include kinematic data to allow for calculation of car trajectories
- CAMs include static data like car length and width, accuracy levels for each kinematic data etc.
- CAMs are supposed to be sent quasi-continuously (each 0.1s)
- CAMs are signed to secure the CAMs authenticity
- CAMs are by design NOT supposed to be secured against eavesdropping

CAM-Data and Traceability

Given a long-time and area-wide collection of timestamped CAMs, there are three methods to calculate routes from these data

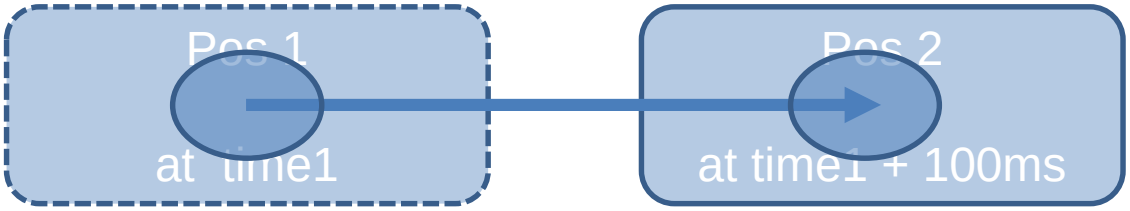


Concatenating CAMs via Timestamp, position, velocity and driving direction

Concatenating CAMs via MAC, stationId or signature

Concatenating CAMs via included static data

Concatenating via kinematic data 1

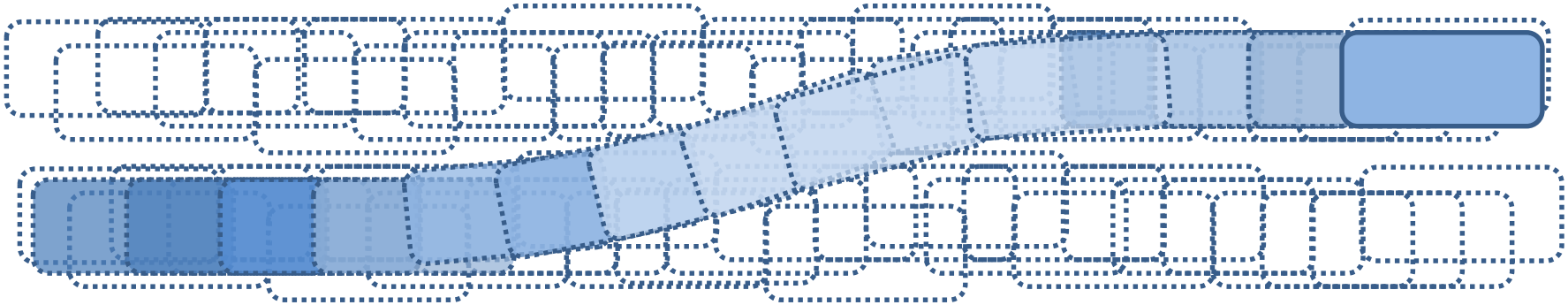


$$Pos2 = Pos1 + 100ms \cdot velocity$$

$$Pos1 = Pos2 - 100ms \cdot velocity$$

- Given a reasonable accuracy of kinematic data the position of a car 100 ms forward in time can easily be calculated.
- E.g. a car driving at 50 km/h will move forward 1.4 m
- Given the typical dimensions of a car and reasonable accuracy of kinematic data only one car is supposed to be in the vicinity of the calculated position at the same time.

Concatenating via kinematic data 2



- In a collection of timestamped CAMs those connected to a certain car can easily be discerned by linking CAMs via their kinematic data.
- From a long-term and area-wide collection of CAMs e.g. commuters‘ routes should be easily discerned.
- From the start and end points of a commuter‘s route or in connection with a car plate recognition system or by other means routes driven might be connected to the identity of a car holder or car driver.

Concatenating via signature, MAC or stationId

- CAMs are signed to ensure their authenticity.
- The signature accentuates the problem of traceability as it couples the CAMs undeniably to a certain identity.
- The identity tied to the signature will be pseudonymized and the pseudonym is supposed to change after a certain period of time, but the signature at least allows for concatenating CAMs to route segments which again might be linked via the use of kinematic or static data.
- In a sensor network with incomplete coverage signatures might allow to bridge distances between two reception areas, if the pseudonym change frequency is low.
- The same reasoning holds for the station identifier and the station's MAC-address which both a supposed to be changed with the pseudonym of the signature.

Imagine a 25km² city area with a 100 km road network

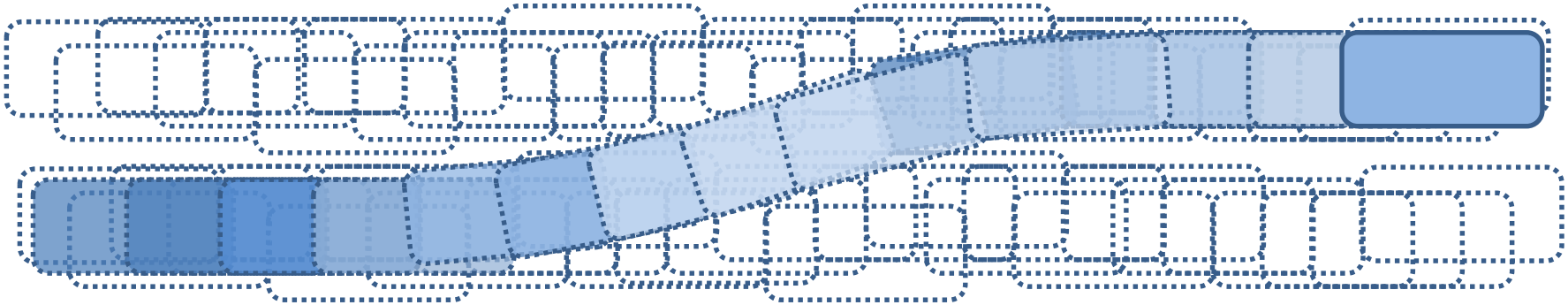
- One ITS station at every 4th crossroads sum up to 50 stations
- Reception radius of 200m results in 600m mean distance between two reception areas
- For a vehicle riding at 30km/h it takes 72s to bridge 600 m

- Any pseudonym change frequency lower than 1/72s will considerable improve traceability in this case!
- => A low pseudonym change frequency will allow for longtime-tracking even in sensor networks with incomplete coverage!

Concatenating via static data

- CAMs include static data like car width/length and accuracy levels for kinematic data.
- While car width/length is specified within an accuracy of 10cm there are 128 different accuracy levels allowed for each of the 7 obligatory kinematic parameters.
- A combination of different static data might be unique for a certain vehicle thus also allowing to link its CAMs correctly.

Conclusions



If CAMs can be concatenated…

… they allow for tracking drivers!

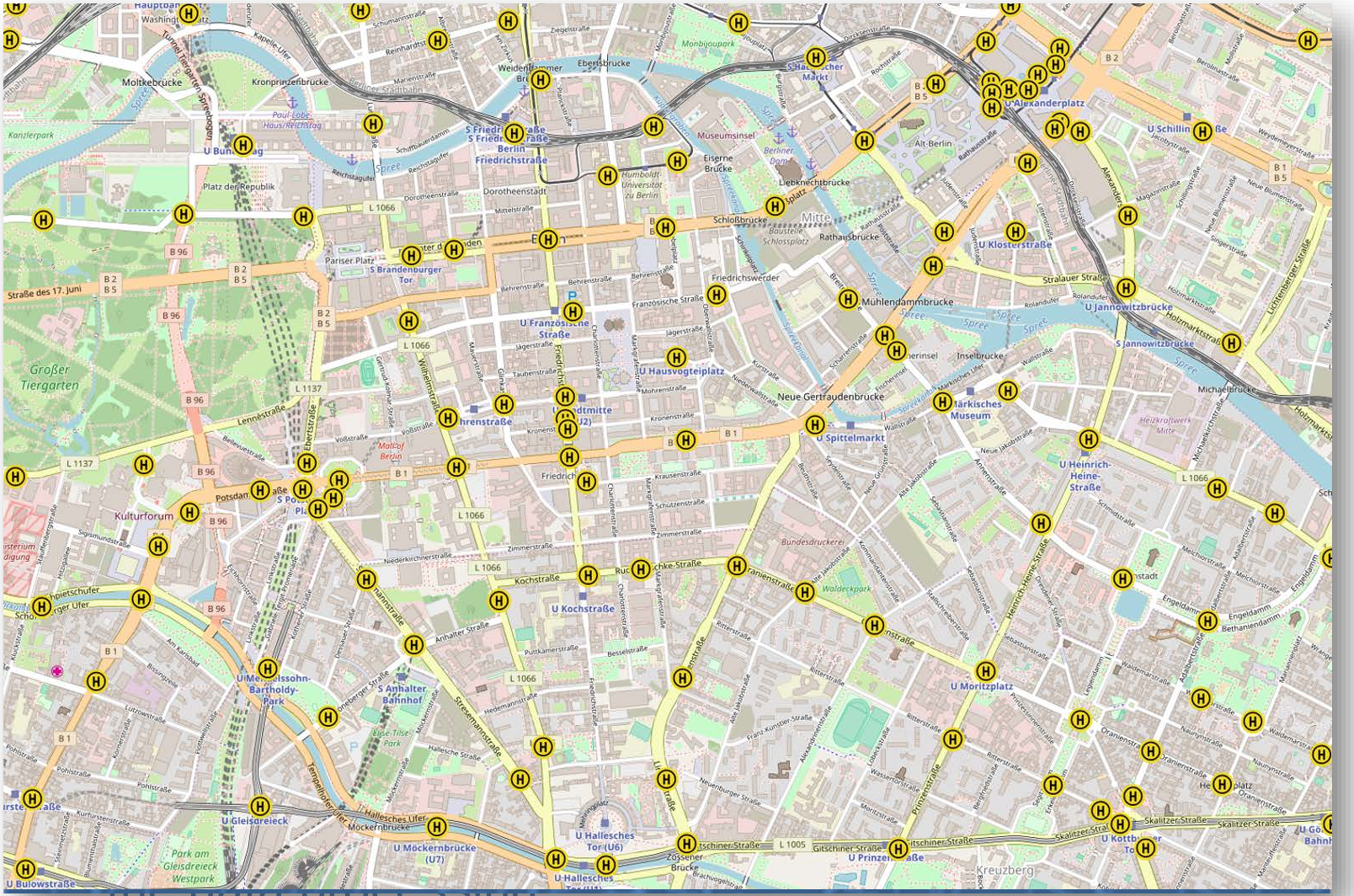
… they allow for the analysis of driving behaviour!

… they allow for fingerprinting and thus can NOT be anonymized!

How serious is the ITS privacy risk?

- Easy availability of high-quality data
  - In a dense sensor network with overlapping reception areas long-time tracking is always possible.
  - With a defective sensor network there is still a serious risk of of longtime-traceability.
  - Due to the high frequency of CAM broadcasting already short-range tracing allows for measuring of driving behavior (e.g. only one sensor near a busy crossroads with traffic lights will deliver a few hundred datasets per vehicle which might be personalized using other broadcast identifiers or even a number plate recognition system)
  - Presumable low costs for receiving equipment and high profit expectations from trading CAM-data might justify investments in sensor networks to “harvest” CAM data
- Due to the broadcast character of the communication concept underlying ITS without any technical safeguards users cannot rely on the lawfulness of all the data processing

How serious is the ITS privacy risk?



the data processing

Recommendations

- Further reduce the amount of personal data in CAM (*really 128 accuracy levels required for position, velocity etc.?*).
- Have a pseudonym change frequency as high as possible (*should be limited by the requirements for short-time-tracing only*).
- Implement safeguards to prevent unauthorised use of CAM/DENM data (*closed system approach?*).
- Allow for user control (*e.g. consent markers*).

Questions and Discussions

Thank You!

mailto:michael.kiometzis@bfdi.bund.de
tel: +49 (0)30 18 7799 2102