Automated driving

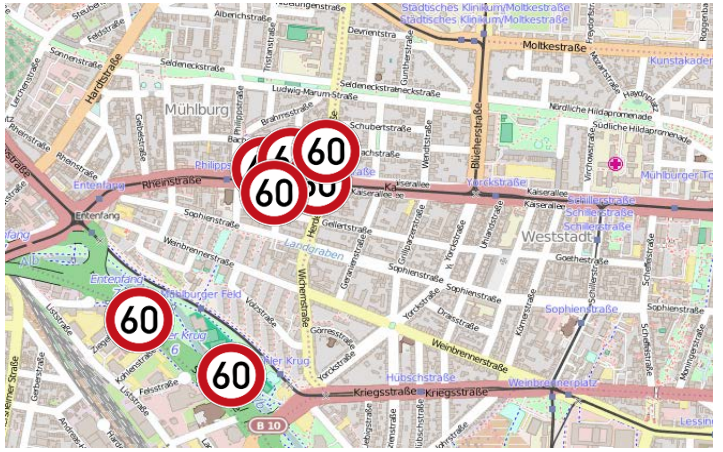
Data security, data privacy and liability questions in real life use cases

Dr. Alexander Duisberg, Bird & Bird LLP

Dr. Christian Winkler, mgm technology partners GmbH

Modern cars can detect traffic signs

- Modern cars use cameras for recognizing traffic signs
- Detected traffic signs are saved and shown to driver
- Data can be read later and are sent anonymously to servers
- Clustering can lead to improved maps
  - Road work
  - Variable signs (including time dependency)

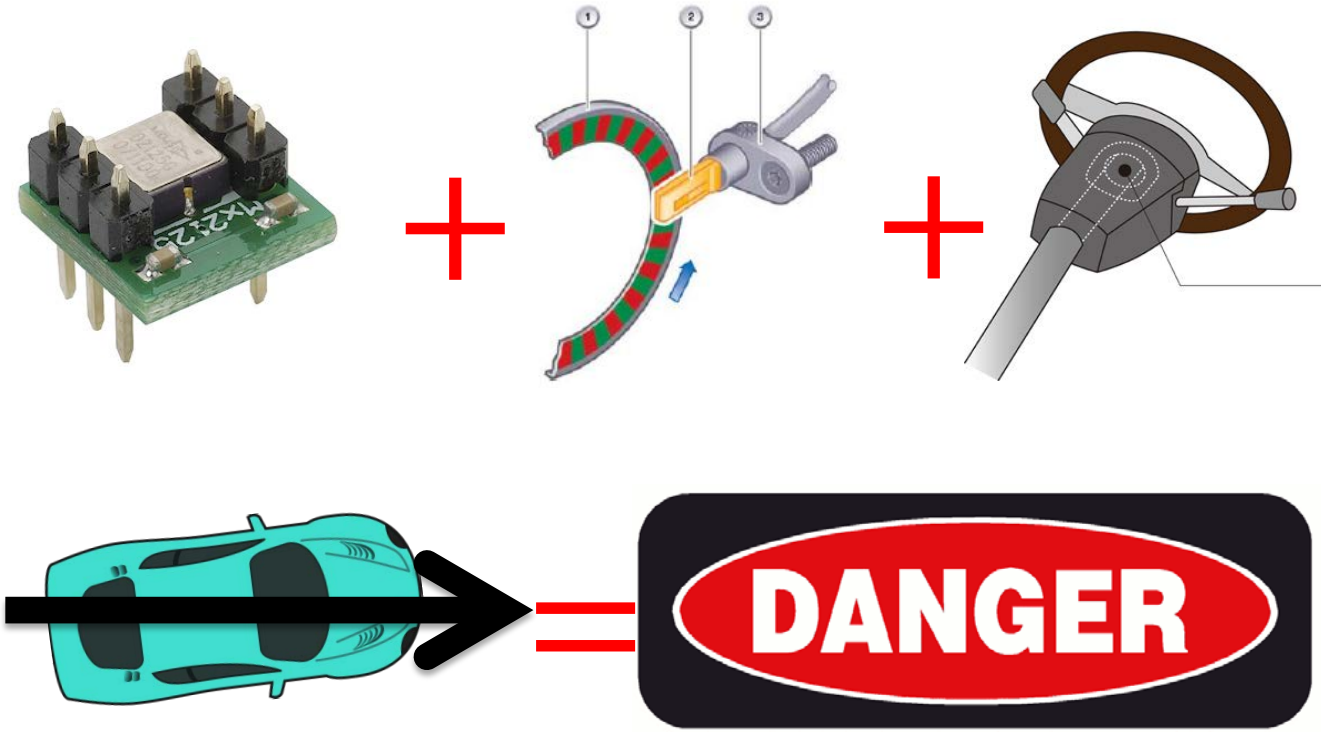


Interesting questions

- What happens with „speedy“ drivers?
  - Traffic signs have been seen by the camera
  - Driver should also be able to see the signs
  - Relevant for police?
- Who owns the sign detections?
  - Vehicle owner? Individual drivers?
  - OEM? Service provider?
  - Privacy consent (unambiguous, „informed“ consent)
  - Protection against disadvantageous disclosure
- Wrong detections
  - Reliance on improper maps?
  - (Product) Liability if map has changed?

Dangerous driving conditions

- Sensor data can be combined
  - Acceleration (longitudinal, lateral)
  - Braking, steering angle, yaw velocity



- Driving conditions can be calculated
  - High acceleration
  - Strong braking
  - Frequent drifts

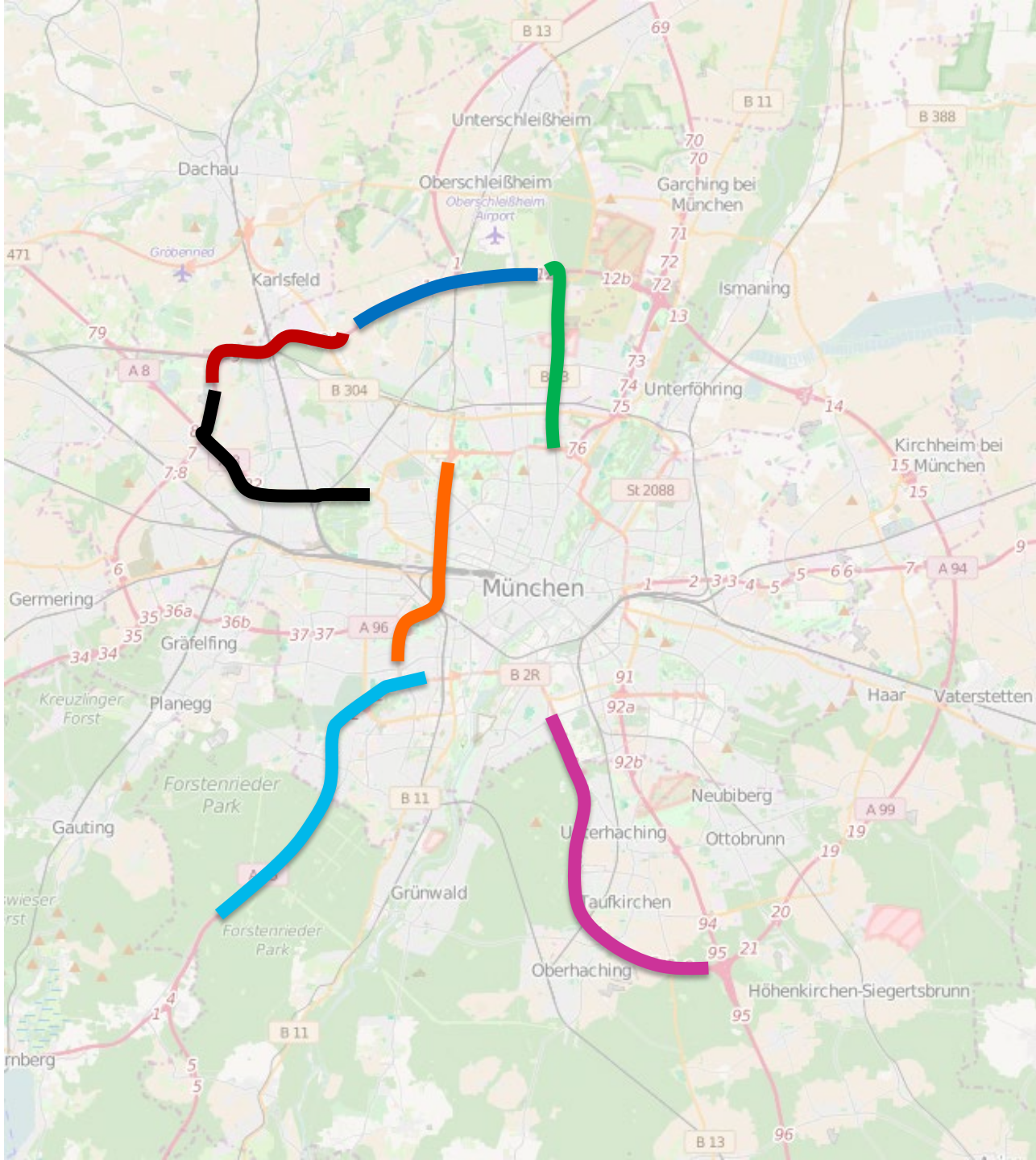
- Associate with geo coordinates

Interesting questions

- Who has access to the data records?
  - Control over data collection and search system?
  - Right of database maker
  - Who can make correlation with map information on traffic signs and danger warnings?
- Insurances might increase rates for drivers
  - High risk scenarios
  - Uncontrollable vehicles
- Dangerous places can be identified
  - Interesting for everybody?
  - Who „owns“ this data?
  - Valuable knowledge for insurances (again!)

Detection of driving „sessions“

- Data from vehicle is properly anonymized
  - Only time, coordinates and payload are sent
  - No personal data ever transmitted
  - Short session need to be preserved (map-matching)
- Whole sessions (start to end) can be reconstructed
  - Use periodic timestamps
  - Use machine learning to identify driving behaviuour
  - Use map data to find places where cars can park
  - Identify home (and work) location of cars
  - Identify potential drivers



Interesting questions

- Is anonymization (pseudonymization) enough?
  - If time and coordinates still are there
  - Risks of cross-fertilization with other data sources?
- Who is allowed to de-anonymize data?
  - OEM?
  - Police?
  - Included in privacy consent / terms & conditions?
- More general
  - Proper manners to avoid de-anonymization?
  - Relevance of encryption?
  - Server locations relevant?
  - Data retention and deletion – what does the law say?

Contacts

Dr. Alexander Duisberg
Bird & Bird LLP
Maximiliansplatz 22
80333 Munich, Germany

phone +49 89 3581 6239
email alexander.duisberg@twobirds.com

Dr. Christian Winkler
Mgm technology partners GmbH
Vordere Cramergasse 11
90489 Nuremberg, Germany

phone +49 911 710 4029 0
email christian.winkler@mgm-tp.com