Making Smart Use of Geo-location Data

Using geolocation in a trustworthy and compliant way

Simon.Hania@tomtom.com
Trends that threaten trust
Connected cars with downloadable apps

Location services, cloud, internet-of-thing, big data
TomTom: more than Satnavs...

Consumer products

Automotive products

Fleet Management Services

Maps, Traffic info etc.
Revolutionising navigation

In 4 steps

1. Base maps
2. Map Share
3. IQ Routes
4. TomTom HD Traffic
TomToms trip archive
Anonymous location and speed information from the TomTom user community

5 billion $\text{(10E9)}$ speed measurements per day
5 trillion $\text{(10E12)}$ speed measurements to date!
by customers driving 50 billion kilometres
and visiting every spot over 1,000 times
Creating TomTom HD Traffic: data sources

Range of high-quality real-time data sources
TomTom Traffic coverage

It covers up to 99.9% of all roads
Intersection analysis

Obsoletes time-consuming, expensive and inaccurate methods
Travel times to hospital
The reality check that can help to save lives

LONDON

Map showing access to a hospital in London using the default speeds in Accession

Map showing access to a hospital in London using daily average speed data from TomTom

Based on theoretical maximum speeds

Based on real world measurements
Origin/Destination analysis
Example: Trips with Frankfurt Airport as destination

• Where are your customers coming from?
• What routes do they take?
• How many drivers are passing?
• Etc.

• Combine with other geo-based data sources for additional analysis
Location privacy is top of mind
With bloggers, press, regulators, enforcers, legislators and many users alike

- TomTom investigated by leading European Data Protection Authority in 2011

- TomTom’s use of location data is in accordance with EU Data Protection Laws

- Processing and delivery to third parties 100% OK

- Informing users needed to be more explicit, including opt-in
Drivers, police & TomTom

An explosive mixture
Community input – with permission

We profile roads, not people
**TomTom & Privacy**

**Vision:**
Community input (crowdsourcing) is strategic

Privacy helps to realize business objectives by **ensuring trust**

Privacy is integral part of business continuity above and beyond legal compliance

**Principles:**

1. Avoid unpleasant surprises:
   - Customer insight is paramount
   - Be open and explain – hesitation is an omen
   - Keep it simple

2. The customer remains in control of his personal data: we have it “on a loan”
Privacy Policies, Standards & Guidelines

7 key objectives

1. We **asses** our intended use of PD early **to drive** requirements

2. We **document** PD: purpose, legitimate ground, retention, access, jurisdiction(s)

3. We ensure we have obtained or will **obtain** informed user **consent**

4. We **minimize** the amount of PD (volume and time) and who has access: we de-personalize or destroy PD as soon as possible

5. We **keep** ensuring **adequate security** measures based on risk assessment of confidentiality, integrity and availability

6. We do **not expose** PD to any **third party**, unless the third party contractually agrees to comply to our policies (or law forces us)

7. We enable the user to **exercise** his **rights** (information, access/download, correction, deletion)
Typical personal data misconceptions
very often present in technology companies

• We do not identify the user while using the data, so we have no issues with privacy law
• We only use the serial number of the users device, so the data is anonymous and we have no issues with privacy law
• We encrypt the data, so we are no longer using/receiving/sending personal data
• We use hashes to replace all serial numbers, so the data is now anonymous and we have no issues with privacy law
• We anonimize the data, so we are not using personal data
• We can use the users’ data for anything we want, as long as we keep the data to ourselves
• Look: big name companies are doing the same, so we are OK
Can location data be anonymous?

Research indicates: hardly ever

How Access to Location Data Could Trample Your Privacy

The smartphone revolution will include unprecedented surveillance by companies hoping to make money from user data.

In addition to making it easier to stay connected, the smartphone boom seems likely to bring with it another, less welcome, result: unprecedented surveillance by companies hoping to make money off of your whereabouts and behavior.

A new research paper shows how easily supposedly anonymous location data can be used to identify individuals; the findings promise to have profound importance as businesses seek new ways to make money from mobile users.
Avoiding re-identification is key
TomTom has a strict code of conduct to adhere to privacy laws

- Historic trip archive only to be used for road, traffic and related purposes
- No access to raw data outside TomTom, ever
- TomTom performs processing
- TomTom ensures re-identification is impossible e.g. through sufficient aggregation
Location data: use case matters

Risks to the right to privacy depend on context – as always

1. Smartphone
   24x7 collecting and transmitting location data to various controllers – hard to avoid

2. Connected car
   collecting and transmitting location data while driving – eCall drives it, commercial, traffic management and law enforcement opportunities (try to) piggy-back on it

3. Navigation app or device
   collecting and transmitting location data to navigation provider – only when actually driving unknown routes

4. One off location service app
   Occasional disclosure of location to app/service provider
Location data: granularity matters

Think in 4D

1. Spatial granularity
   1. Accuracy of the positioning service - GPS, cell tower, WiFi
   2. granularity of the underling grid – map matched or not
   3. Characteristics of the area: population density & composition

2. Temporal granularity
   1. Time stamp accuracy - synchronisation, drift and jitter
   2. Granularity of the time buckets
   3. Period/time window of correlated positions ("trace")
Location data: who is the data subject?
Who are we actually dealing with?

1. Smartphone
   1-on-1 relationship with user

2. Tablet
   Multiple users (iOS) versus multi-user (Android 4.2+)

3. Personal navigation device
   Multiple users in a household versus multiple users in a rental

4. Connected car
   Dealing with changing drivers. How about the passengers?

5. The “children dimension”
   Is the drivers’ license sufficient to presume non-minors?
References


- The report on the Dutch Data Protection Authority investigation on TomTom's use of location data (in English): http://www.dutchdpa.nl/Pages/en_pb_20120112_investigation-tomtom.aspx

- “How we use your data”: TomTom’s explanation on its use of location data http://www.tomtom.com/yourdata