



**INTERNATIONAL WORKSHOP  
ON GEOSPATIAL DATA QUALITY**  
*Legal, ethical and technical aspects.*

***Changes in the EU legal framework***

Dr. Colette Cuijpers

Tilburg Institute for Law, Technology, and Society (TILT)  
Tilburg University

[cuijpers@uvt.nl](mailto:cuijpers@uvt.nl)



## Structure

- Complexity of the EU legal framework on data protection
- Developments since 2009
- Current/future research

29/05/2012

2

# Geo information and data protection; European legal framework

- **Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data**

*Regulates the processing of personal data*

- **Directive 2002/58/EC (as amended by 2009/136/EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector**

*Regulates the processing of personal, traffic and location data, in connection with the provision of publicly available electronic communications services in public communications networks*

- **Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC**

*Regulates retention of traffic data and location data and the related data necessary to identify the subscriber or user of a publicly available electronic communications service*

29/05/2012

3





## Four types of data defined

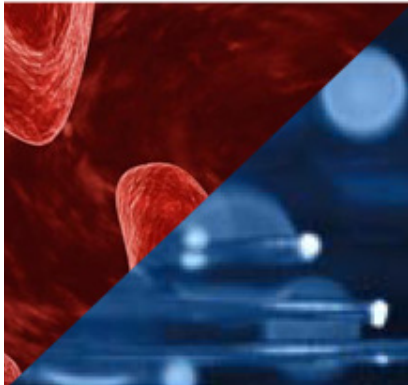
- Personal data: any information regarding an identified or identifiable natural person.
- Sensitive data: special categories of data in need of stricter protection.
- Traffic data: any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.
- Location data: any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.



## Main problem of the legal framework

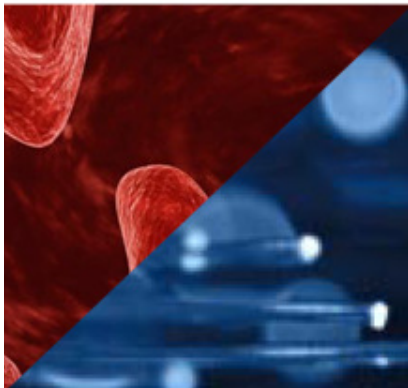
- Too complex! Too many uncertainties due to overlap and vague definitions, e.g. What technologies fall within the definition of: **public communications network** or **publicly available electronic communications service**?

To give just one example: public is not defined within any of the EU regulatory mechanisms.

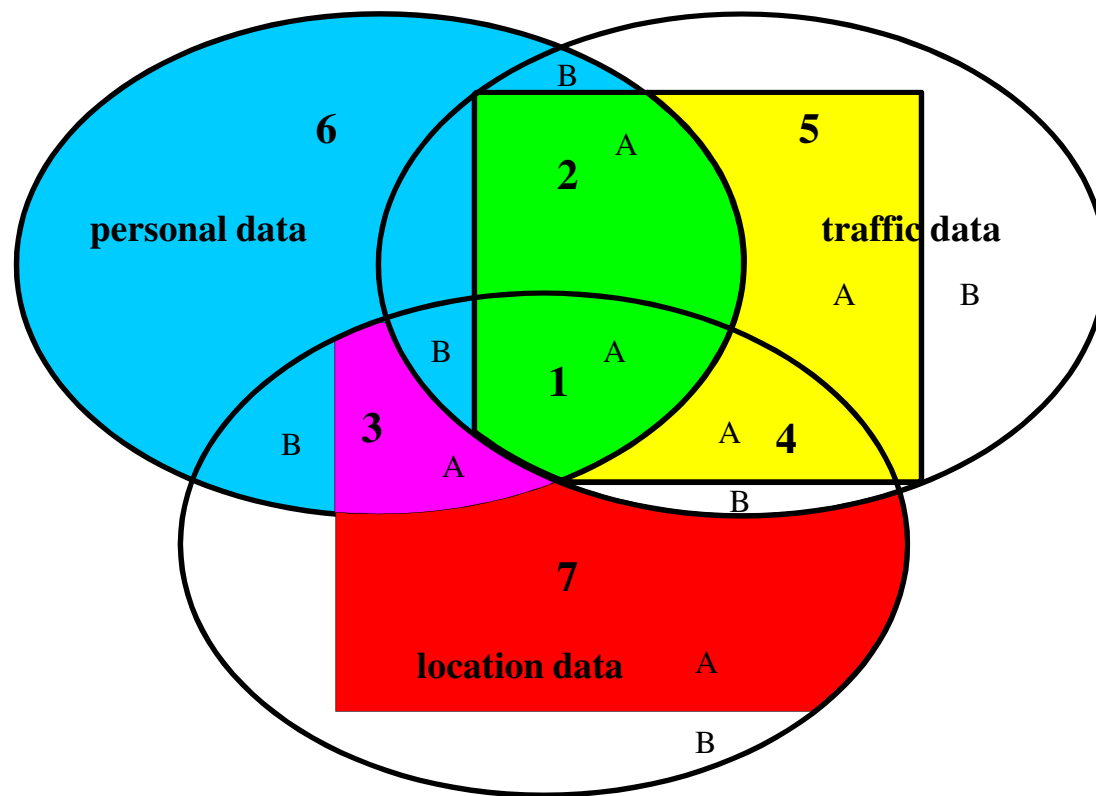


## Technologies covered?

	Satelite Based	Sensor Based	RFID WIKI Blue-tooth	Cell Based Mobile Networks	Chipcard Based Payment
Electr. Comm. Network	Yes	No (?)	Yes	Yes	No (?)
Electr. Comm. Service	Yes	No (?)	Yes	Yes	No (?)
Public (disc. to abolish req.)	Yes (but technical limitation possible)	?	?	Yes (but technical limitation possible)	Yes
2002/58 Applic.? 29/05/2012	Yes	No (?)	If public yes	Yes	No (?)



Yellow: app. of Art. 5 and 6 of the E-P Dir.  
Red: app. Article 9 of E-P Dir.  
Blue: scope of the DP Dir.  
Purple and Green: specific provisions of the E-P Dir. + DP Dir. app., which  
is only the case in public networks or services; indicated with 'A'  
'B' indicates that data are generated in private networks or otherwise fall  
outside the scope of the E-P Dir.



## Importance of qualification:

As a principle rule:

It is only allowed to process sensitive data, location data and traffic data with (prior) consent of the data subject.

Personal data also other legitimate grounds for processing. E.g. when the interest of the data processor outweighs the interest of the data subject.

For location data it is furthermore stated that: only to the extent and for the duration necessary for the provision of a value added service, with an obligation to inform and a right to temporarily refuse.

Several exceptions, e.g. for traffic data when necessary for transmission of communication or billing.







## So providers of LBS need to answer a lot of difficult questions:

- 1. Are the data to be processed 'personal data'? (see Art. 2(a) of Directive 95/46/EC)
- 2. Are the data to be processed 'traffic data'? (see Art. 2(b) of Directive 2002/58/EC)
- 3. Are the data to be processed 'location data'? (see Art. 2(c) of Directive 2002/58/EC)
- 4. Do the data relate to users or subscribers of public communications networks or publicly available electronic communications services? (see Art. 6 and 9 of Directive 2002/58/EC and Art. 2 (a), (c) and (d) of Directive 2002/21/EC)
- 5. Is one of the exceptions applicable? (see Article 13 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC)



## Conclusion 2008

### Three layers of complexity:

1. Different rules for different types of data
  2. Rules also depend on qualification of LBS technology
  3. Uncertainties and grey areas regarding terminology used to qualify these technologies
- In the current fragmented legal regime, legal certainty is virtually absent, both for LBS providers and for LBS subscribers.

### Question:

- Are existing differences justifiable in view of current practice? E.g.
- Private vs. Public
  - Telecom Provider vs. Information Society Service Provider

29/05/2012



## Telecom Operator vs. Information Society Service Provider:

The meaning of *publicly available electronic communications network and service* can be derived from a combination of several definitions in different Directives (2002/58/EC: Art. 3, 2002/21/EC: art 2 (a) and (c), 98/34/EC: Art. 1 (2)).

For this presentation it is relevant that: *Telecom operator* is synonym to *public electronic communication services*, from which definition information society services are explicitly excluded.

Information society services are defined as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services” (98/34/EC: Art. 1(2)).



## Directive 2009/136/EC

Some changes were made to Directive 2002/58/EC, but nothing to cope with the existing complexity.

Two main changes:

1. Introduction of opt-in for non-functional cookies.
2. Introduction of data breach notification.

1. A lot of debate:

- Is consent always necessary? Relation to 'private sphere'?
- How to obtain PRIOR consent? (art. 6 (3) for traffic data, location data consent with prior information).
- if practical implementation of the new rule is unclear, (how/what should be the role of supervisors be)?



## Data breach notification

2. Also not directly relevant for topic, but interesting recital 59:

Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), **regardless of the sector, or the type, of data concerned.**

29/05/2012

13



## However, the general scope remains:

### Article 3:

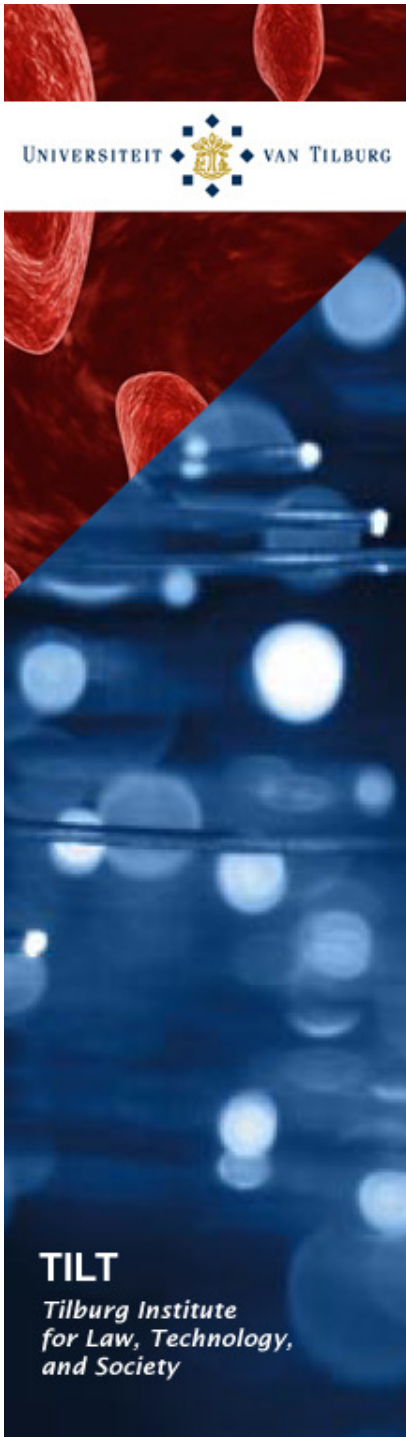
This Directive shall apply to the processing of personal data in connection with the provision of **publicly available electronic communications services in public communications networks** in the Community, including public communications networks supporting data collection and identification devices.

Recital 56: when such devices (ref. to RFID) are connected to publicly available electronic communications networks or make use of publicly available electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply.



## **Scope still explicitly does not include private networks and services:**

Recital 55: In line with the objectives of the regulatory framework for electronic communications networks and services and with the principles of proportionality and subsidiarity, and for the purposes of legal certainty and efficiency for European businesses and national regulatory authorities alike, Directive 2002/58/EC (Directive on privacy and electronic communications) focuses on public electronic communications networks and services, and does not apply to closed user groups and corporate networks.



## Conclusion

- Still differences regarding different types of data (exception data breach notification...)
- Still no clarity regarding technologies to be included
- Still difference public vs. private
- Still differences regarding telecom operators and information society service providers:

So hopefully the Art. 29 Working Party will provide some clarity....





## Art. 29 Opinion on geolocation services on smart mobile devices (2011)

“Directive 2002/58/EC (as revised by 2009/136/EC) only applies to the processing of base station data by public electronic communication services and networks (telecom operators)” (WP 185: 7, 20).

However, this statement implies two questionable limitations regarding the scope of the ePrivacy Directive:

1. Why limitation to base station data?

- Not necessary as location data is defined technology neutral.

2. Why differentiate between telecom operator and information society service provider?

Don't they provide the exact same service?

Don't they 'blend' in practice?

29/05/2012

17



## Cuijpers & Pekárek (2011):

1. Clear separation between different actors and their roles has become unrealistic, and particularly the practical differences between telecom operators and information society service providers are quickly becoming merely theoretical.
2. Location data used in LBS is increasingly the result of an amalgamation of other data, which sources cannot be practically traced anymore. Thus, the approach to apply different regimes to different types of data is increasingly less tenable.



## Some examples

- WiFi at Mac Donalds, in EU provided by T-mobile, is telecomoperator, but is it public if access depends on the consumption of a hamburger?
- In the Netherlands hotels offering WiFi do not need to adhere to the same strict market rules as telecom operators, while offering the exact same service.
- Fon: Every participant can share the capacity of their WiFi access point at home with other members by buying and installing a piece of additional hardware. In return the participant gets free roaming at over 4 million Fon spots worldwide. How to qualify an individual 'Fonero' within this network?
- Google and Facebook offer locationservices (Google Latitude and Facebook places) but are qualified as information society service providers: ePrivacy Directive not applicable (....?....)

29/05/2012

19



## Some examples II:

- <http://www.skyhookwireless.com> a service that uses a combination of different data types to pinpoint locations, although the informational output is clear (a geographic location) for the customer it is not visible which types of data have been used.



## To make matters even more complicated:

Even though the final conclusion in the Opinion states that Directive 2002/58/EC only applies to the processing of base station data by telecom operators, this conclusion seems to be challenged by one of the clarifications given by the Working Party itself:



## Clarification ....

“[i]f a telecom operator offers a hybrid geolocation service, that is also based on the processing of other types of location data such as GPS or WiFi data, that activity qualifies as a public electronic communication service. The telecom operator must ensure the prior consent of its customers if it provides these geolocation data to a third party.” *2 sentences later*

“Typically, companies that provide location services and applications based on a combination of base station, GPS and WiFi data are information society services. As such they are explicitly excluded from the e-Privacy directive, from the strict definition of electronic communications service (Article 2, under c, of the revised Framework Directive (unaltered).”

29/05/2012

22



**So:**

1. This makes that the current limitation to base station data in view of current practical developments will render the Directive to a large extent obsolete.
2. In addition, it creates a situation in which telecom operators are placed in an even worse position compared to LBS providers not being telecom operators as the opportunity to 'evolve' to an information society service provider is effectively eliminated by the Opinion.



## Conclusion 2011

The types of data, the sources of data, the availability of the services and networks (either public or private), the qualification as a telecom operator and/or an information society service provider as well as all possible exceptions must be assessed before it is clear what rules apply to the processing of data in providing LBS in practice. When combined with the described trends of hybridisation, this leads to a situation in which it has become difficult, if not impossible, for both the providers of LBS and its users to understand the rights and obligations set out in the legal framework, thus effectively creating a legal vacuum.

In short: The EU legal framework is still too complicated and embodies unfounded differences depending on data, technology and actor.

29/05/2012

24





## Two options for improvement

- Extend the current ePrivacy regime by making it data, technology and provider neutral.
- Abandon the current special regime for location data completely in favour of a more general protection of personal data, thus bestowing more weight to the General Data Protection Directive.

We conclude our paper with expressing our hope that the current revision of the EU Data Protection regime will choose one of these two options, or at least will improve the existing complexity.



## January 25, 2012: Proposal General Data Protection Regulation

Recital 24 (...) It follows that identification numbers, **location data**, online identifiers or other specific factors as such *need not necessarily be considered as personal data* in all circumstances.

How does this relate to Opinion Art. 29 Working Party???

It would have been more in line with previous explanations if these data were deemed even 'higher' than personal data = sensitive data (in view of similar consent requirements and the previous statements that all location data are personal data)



## However, sensitive data are:

Data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetic data or data concerning health or sex life or criminal convictions or related security measures.



## So conclusion 2012

Confusion has even increased....at least when speaking for myself....

And in my opinion this is a bad development, especially in view of the ever extending possibilities of identification, also on the basis of location data (See also Scassa and Campbel *Data Protection and Spatial Data*) and impossibilities of factual anonymization.

For Canada:

*“Data protection law suggests that information will be personal information where there is a ‘serious possibility’ or a ‘reasonable expectation’ that an individual may be identified using that data or other data available.”*

29/05/2012

28



## EU proposal definition Personal Data:

'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, **by means reasonably likely to be used** by the controller or by any other natural or legal person, in particular by reference to an identification number, **location data**, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.



So

More research is needed, especially regarding practical implications:

Currently working on two papers:

1. Together with research master student Paul Marcelis regarding the implications of an extensive interpretation of the concept of personal data (In Dutch).
2. Together with computer scientist Yucel Saygin: The rise of identifiability, the downfall of personal data protection? (LBS as illustration, to present at APC October 2012).

29/05/2012

30



## Sources:

- Colette Cuijpers and Bert-Jaap Koops (2008), **How fragmentation in European law undermines consumer protection: the case of location-based services**
- Colette Cuijpers and Martin Pekárek (2011), **The Regulation of Location Based Services: Challenges to the European Union Data Protection Regime**
- Directive 2009/136/EC, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF>
- Opinion Art. 29 Working Group on geolocation services on smart mobile devices, WP 185, [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm)
- Proposal for a Regulation of the EU Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012) 11 final, 2012/0011 (COD), [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)