Legal Issues of Geo Information: A Short Introduction to the Privacy aspects

Paul De Hert & Colette Cuypers

Tilburg Institute for Law, Technology, and Society (TILT)
Law Science Technology & Society (LSTS, Brussels)

Overview workshop

- Background
- Privacy framework: case of Uzun v. Germany (2010)
- Data protection framework

UNIVERSITEIT VAN TILBURG

TILT
Tilburg Institute for Law, Technology, and Society

Background: a legal perspective on geo information

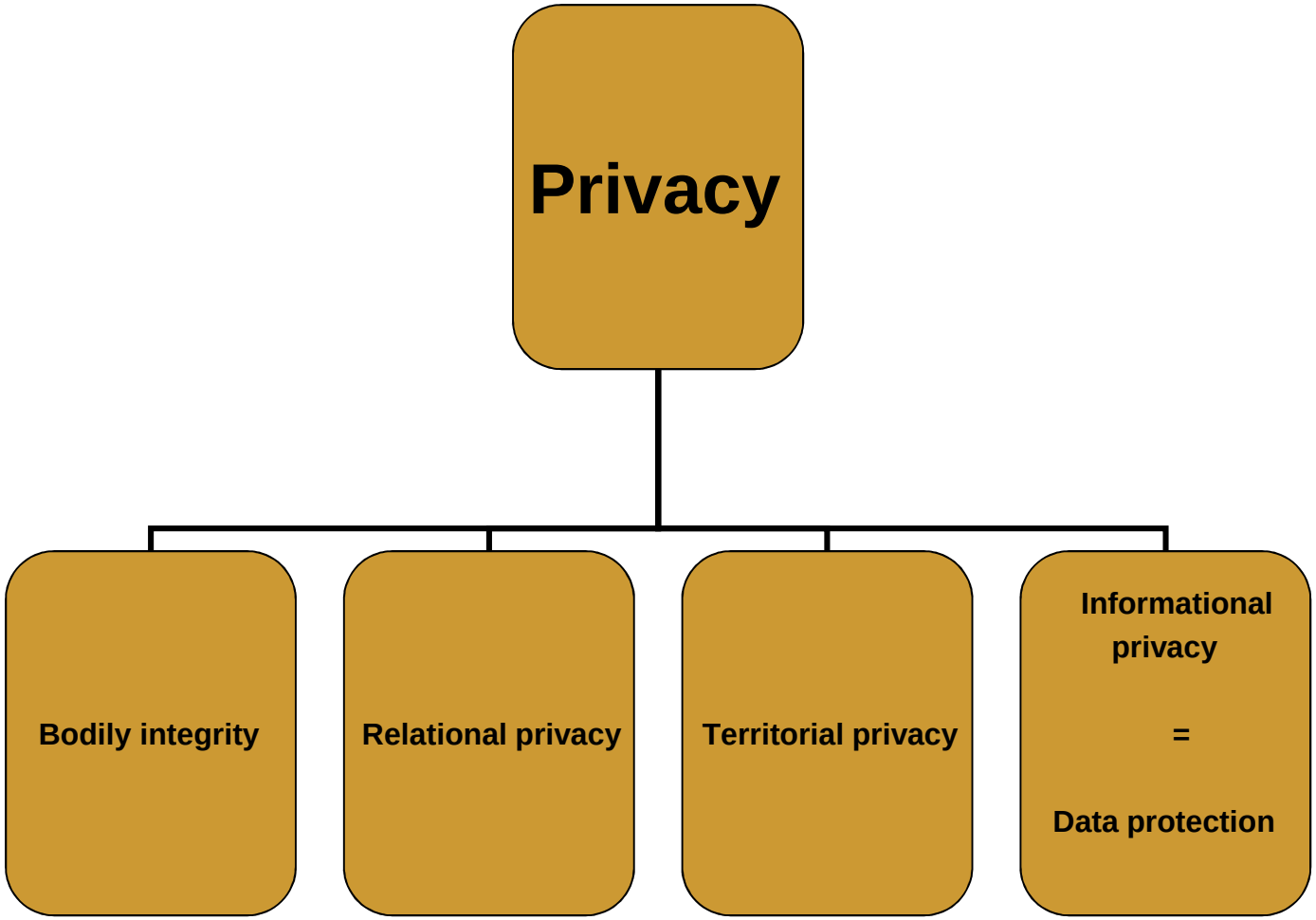
Picture by Dr. Ingo Baumann

In view of time and expertise focus on Privacy, IP and Liability

Data protection and geo information

- Trend: geo information is used more and more to track, trace and locate people in real time, using different technologies (e.g. satellite based, cell based, sensor based. Examples of applications: sns, sms-alert, electronic detention, medical research)
- Growing market for those who want to provide services based on location information
- Question to be asked before designing LBS; What is legally allowed, what are the legal requirements?
- From a privacy perspective: Even though people want to make use of LBS, they want to remain 'in control' over their privacy = fundamental human right
- Other fundamental human rights can strongly relate to invasions of privacy, such as the right to non-discrimination and equality
- Informational privacy put down in data protection legislation

The Privacy framework



CASE OF UZUN v. GERMANY (2 September 2010): GPS surveillance

- 42. The Government took the view that there had not been an interference with the applicant's right to respect for his private life under Article 8 by the surveillance via GPS. This surveillance had not directly concerned the applicant in person as the GPS receiver had been built into the car of his accomplice S. and as the data collected had only revealed where the receiver had found itself at a particular time and not who had been travelling in S.'s car.

The Court's view

- 49. In determining whether the surveillance via GPS carried out by the investigation authorities interfered with the applicant's right to respect for his private life, the Court, having regard to the above principles, will determine first whether this measure constituted a compilation of data on the applicant. It notes the Government's argument that this was not the case, given that the GPS receiver had been built into an object (a car) belonging to a third person (the applicant's accomplice). However, in doing so, the investigating authorities clearly intended to obtain information on the movements of both the applicant and his accomplice as they had been aware from their previous investigations that both suspects had been using S.'s car together on the weekends of previous bomb attacks where it was considered irrelevant to the finding of an interference with the applicant's private life that the telephone tapping in question had been carried out on the line of a third party).

The Court's view

- 50. Moreover, the fact that the applicant must, just as S. was, be considered to have been the subject of the surveillance by GPS, is not in question, because information on the movements of S.'s car could only be linked to the applicant by additional visual surveillance to confirm his presence in that car. Indeed, none of the domestic courts expressed any doubts that the applicant had been subjected to surveillance via GPS

Small reservation by the Court

- 52. In the Court's view, GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings. Having regard to the principles established in its case-law, it nevertheless finds the above-mentioned factors sufficient to conclude that the applicant's observation via GPS, in the circumstances, and the processing and use of the data obtained thereby in the manner described above amounted to an interference with his private life as protected by Article 8 § 1

Geo information and data protection; The European legal framework

- **The general 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 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

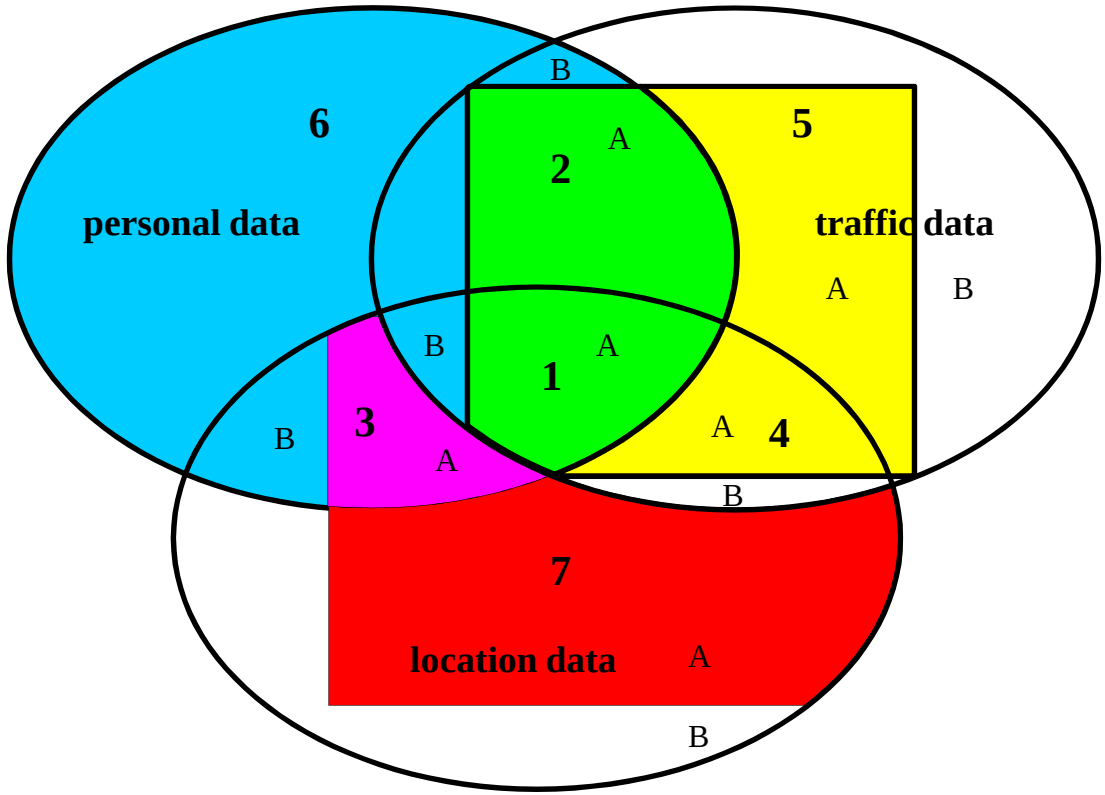
Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection 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.

16/02/2011

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?

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.



The definition of 'personal data'

- The applicable definition is to be found in Directive 95/46/EC, Article 2(a)
- Crucial issue (determining applicability), but different readings and approaches:
  - Art. 29 WP interpretation: Opinion of April 2007 on the concept of personal data
  - Divergent practices, notably from the industry
  - EDPS: Art. 29 WP view as eventually revised by courts
- A proposal for specific revision in the context of the Telecoms Package has met strong opposition
- Challenge: provide effective protection for the ubiquitous information society without undermining the general legal framework.

Traffic and location data (I)

- Traffic and location data are specific to personal data and privacy protection in the electronic communications sector: not regulated in Directive 95/46/EC but in Directive 2002/58/EC
- They benefit from special protection:
  - Traffic data: defined in Article 2(b), regulated by Article 6 (+ clarification of Recital 35).
  - Location data: defined in Article 2(c), regulated by Article 9 (+ clarification in Recital 14).
- However, the discussed limitations of the applicability of Directive 2002/58/EC have a direct impact on the provisions on traffic and location data.

Traffic data: confidentiality

This directive obliges Member States to guarantee the *confidentiality* of communication through national regulations prohibiting any unauthorised listening, tapping, storage or other kinds of interception of surveillance of communications **and the related traffic data** by persons other than users, without the consent of the users (except when legally authorised to do so).

The confidentiality of communications applies both to the contents of communications and to the data related to such communications.

Traffic data: three levels of protection (continuation)

The level of protection of traffic data depends on the purpose of the processing:

(1) transmission of communication,

(2) billing or

(3) marketing electronic communication as well as providing of value added services, e.g., tourist information, route guidance, traffic information and weather forecasts.

Traffic data for transmission and billing

- (1) For the purpose of the *transmission* of a communication, traffic data relating to subscribers and users may be processed and stored by the service or network provider but must be erased or made anonymous when it is no longer needed for the purpose of the transmission. The obligation to erase or anonymise traffic data does not conflict with procedures such as caching or using log-in information for access control.
- (2) Traffic data, *necessary* for the purposes of subscriber *billing* and interconnection payments, may be processed and stored up to the end of the period during which the bill may lawfully be challenged or payment pursued.

Traffic data for marketing

- (3) Traffic data, *necessary* for the purpose of *marketing* electronic communications services or for the provision of *value added services*, may be processed by the service provider to the extent and for the duration necessary for such marketing or services, if the subscriber or user to whom the data relate, has given his consent after he has been informed about the type of traffic data processed, the purposes and the duration of the processing. Users/subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

- In any of these cases, processing of traffic data must be restricted to what is necessary for the purposes of such activities and must be restricted to persons acting under the authority of the network or service provider. In any of these cases, if data are processed for a longer time than for the transmission, the user or subscriber must be informed of the duration of such processing.

Traffic data & IP addresses

- A type of traffic data particularly relevant in the context of the information society: Internet Protocol (IP) addresses.
  - IP addresses are increasingly processed outside the scope of application of Directive 2002/58/EC by entities that do not consider IP addresses to be personal data
  - Article 29 WP suggests Internet Service Providers shall treat all IP data as personal unless sure of being able to determine that the data corresponds to users they cannot identify.
  - To be noted: traffic data can include data on geographic position of equipment.

Location data other than traffic data

- Use of location data constantly increasing.
- Definition of Article 2(C) explicitly limited to "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*"

- Location data other than traffic data are data that "indicate the geographical position of the user without being processed for the purpose of the conveyance of an electronic communication or the billing thereof".
- (1) Such data may only be processed (a) when they are made anonymous or (b) with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a *value added service*.

Location data and how to obtain consent

- (2) When consent must be obtained, the service provider must – prior to obtaining the consent – inform the users or subscribers of (a) the type of location data other than traffic data which will be processed, (b) the purposes of the processing, (c) the duration of the processing and (d) whether the data will be transmitted to a third party for the purpose of providing the value added service.

Location data & withdrawal of consent

- (3) When consent has been obtained, the user or the subscriber (a) shall be given the possibility to *withdraw his consent* for the processing of location data other than traffic data at any time and (b) must continue to have the possibility, using a simple means and free of charge, of *temporarily refusing* the processing of such data for each connection to the network or for each transmission of a communication.

Loopholes?

- Return to definition
  - Definition of Article 2(C) explicitly limited to "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*"
  - Location-related data can be left outside of the scope of the definition: for instance, data obtained through content-based image retrieval (CBIR)

Other relevant categories of data

- Currently: protection for personal data, traffic data, location data.
- There might be other categories of data requiring regulation for ensuring privacy and trust in the ubiquitous information society
- Current challenges
  - Leakages of data through (wireless) connections: for instance, iTunes shared libraries
  - Metadata: data embedded in digital files
- Ambient Intelligence (AmI) / Internet of Things developments:
  - increased use of identifiers, every single object might be ‘identifiable and addressable’
  - Data mining and profiling practices to be implemented processing such identifiers without the need to relate to an identified or identifiable person.

Questions that need to be answered to provide LBS without infringing data protection legislation:

- 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)

Reading materials

- Dr. Sjaak Nouwt, Reasonable expectations of Geo-Privacy? Scripted volume 5, Issue 2, August 2008
  http://www.law.ed.ac.uk/ahrc/script-ed/vol5-2/nouwt.asp

- Cuijpers, C.M.K.C. and Koops, E.J., How fragmentation in European law undermines consumer protection: The case of Location Based Services. Source European Law Review, vol.33 (2008) nr.6 p.880-897 (Fidis report on which the article was partially based available at:
  http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP11-del11.5-legal_framework_for_LBS.pdf