CompLex 1/2014

Dag Wiese Schartum,
with contributions from Gisle Hannemyr and Tommy Tranvik

Use of personal location data by the police

Technologies, experiences and assessment of effects

Report on basis of the FP7 project RESPECT, WP7; RFID, Geo-localization and Internet of Things

Senter for rettsinformatikk
Avdeling for forvaltningsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:
Senter for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 9788272261503
ISSN 0806-1912

Utgitt i samarbeid med Akademika forlag
Trykk: AIT Oslo AS
Omslag og layout: Akademika forlag

Innhold

PART II

1 Introduction/Preface

RESPECT[1] is a research project founded by the European Union (FP7), in collaboration between eighteen research institutions in sixteen countries, plus participation from Interpol. RESPECT addresses the role of surveillance systems and procedures in preventing and reducing crime, tracking evidence and prosecution of serious crime and acts of terrorism:

- Are the surveillance systems and procedures used in Europe in preventing crime effective?
- What are the social and economic costs involved?
- What is the legal basis for these systems and what procedures are in place? What best practices are available?
- What attitude do European citizens have toward surveillance systems?

The aim of RESPECT project is first and foremost to:

- Establish best-practice criteria developed on the basis of operational, economic, social and legal efficiency as well as citizen perceptions.
- Develop a toolkit of pan-European application (and beyond) that will balance citizens' privacy and security concerns.

Further information about the project could be attained from http://respectproject.eu/

This report contains results from RESPECT, WP7 "RFID, Geolocalization and Internet of Things". The objective of WP7 was:

> *"To assess the use of RFID and geo-location devices in the detection, prevention and/or prosecution of crimes across Europe and examine grounds for establishment, costs, density, on-going investment, amount of staff, crime solving rate using these techniques."*

The following tasks were formulated in order to attain the objectives:

> 7.1 Identify and classify RFID and geolocation devices already used or potentially deployable in crime detection, prevention and/or prosecution of crimes in participating member states and a number of non-member states where such systems are already deployed
>
> 7.2 Review of legal and political grounds for establishment given at the time when the particular RFID and/or geolocation system was set up and compare this to grounds given for the retention (and/or extension) of these systems over the years

1 Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies.

7.3 Identify degree of automated decisions based on data collected from RFID and geolocation devices

7.4 Identify the degree of interoperability between public and private RFID and geolocation devices

7.5 Impact Assessment following criteria established in WP3.

Challenges of complying with objectives and tasks regarding costs and technology are discussed in section 3.5.1 (costs) and 4.5.1 (technology).

Deliverables of WP7:

- Inventory of RFID and geolocation systems being used by the private and public sector in major European cities. D.7.1
- Cost and Convenience Report D.7.2
- Impact Assessment of the use of RFID and geolocation devices D.7.3

The two first deliverables are reported in Part I (this part) of the report, while D.7.3 is reported in Part II.

Most of this report has been written by Dag Wiese Schartum, partly on basis of national reports from partners of the RESPECT project (cf. Annex 1) and reports from various national Interpol offices procured through INTERPOL. Thank you! (None mentioned, none forgotten).

Important contributions to chapter 4 have been given by Gisle Hannemyr and Tommy Tranvik.

Thanks to Hannemyr, Tranvik and other members of the RESECT project for many valuable comments to the text.

PART I

Understanding how technology is used to locate and track people

2 Scientific approach of WP7

2.1 Position and Tracking technologies (PT technologies) and concepts to describe them

The statements of objects, tasks and deliverables are based on use of the terms "RFID and geo-location devices" and "systems", i.e. with one specific indication of technology (RFID) and more general devices and systems for geolocation. In order to establish a reasonable meaning for these expressions and thereby the meaning of objectives and tasks, the initial parts of our research involved discussions aimed at identifying more concretely other technologies with the potential of performing geolocalization. Thus, the technological scope has been made wider by identifying other technologies with important characteristics in common with RFID, all regarding geo-localization. In short, we designated these technologies "Position and Tracking technologies", abbreviated "PT technologies."

Thus, in this report PT technologies are characterized by:

I. Application of infrastructure/electronic communication (e.g. GPS,[2] GSM,[3] RFID,[4] WLAN,[5] WiFi,[6] Bluetooth,[7] ultrasound);
II. with the objective to locate and trace objects (e.g. vehicles, equipment, vessels, containers, small items (cloths, bags, people, animals);
III. which have a unique identity (e.g. RFID-tags, SIM-cards, license plates, QR-codes[8]).

This definition contains certain limitations which we will come back to in section 3.2.6 and 3.6. Moreover, use of PT technology is widespread and heterogeneous,[9] factors which constitute a methodological challenge, see section 4.5.1.

Position and Tracking Technology is a concept introduced for the purpose of this research. Research is a learning process, and in section 3.6 ("Overall classification of technology related to peoples' location") we widen the technological perspective and argue that more types of technology than those listed above (cf. I – III) should be of interest; both from the perspective of privacy protec-

2 Global Positioning System.
3 Global System for Mobile Communications.
4 Radio-frequency identification.
5 Wireless local area network.
6 Wireless exchange of data using radio waves over a computer network.
7 Wireless exchange of data over short distances using short-wavelength radio transmissions.
8 Quick Response Code, a type of matrix barcode.
9 Cf chapter 4.

tion and police investigation. As consequence, in chapter 1 of Part II of this report, we introduce "location-enabling technology" to denote this wider range of technologies.

In this report, "location" and "position" will be used as synonyms, but location will be the dominant term to indicate a certain place where a person or an object is.[10] Data used to describe locations are termed "location data", while data describing a physical persons whereabouts is denoted "personal location data". In several documents, "geolocation" is used instead of "location". Geo as prefix indicates that the location is geographic, which could be understood as something different, for example, from location within a building. We do not make a distinction between types of sites where people are located, and thus only make use of "geolocation" when we refer to documents which use this term.

2.2 Methods, sources and implementation

2.2.1 General

The investigation we give an account of in Part I of this report is based on information related to two groups of countries. One part relates to a selection of twelve identified (mainly) European countries ("national studies"). The selection of countries participating in the national study was made as part of the approved research design in the application to FP7. The second part of the investigation has been directed towards national Interpol offices all around the globe, included offices in Europe ("Interpol inquiry"). Since the research design laying the basis for WP7 was based on the condition that the identity of these offices should not be known, and that replies should only be classified as belonging to certain regions of the world, we have not been able to match results from the Interpol study with the national studies. Thus, the two parts of the investigation will be presented separately.

The research design of the Interpol inquiry was based on prior knowledge of the law enforcement sector where it was clear that law enforcement agencies are very reluctant to divulge information of the type required by the RESPECT project. In order therefore to encourage a number of national police forces to provide some information, it was decided to offer the possibility of using RESPECT partner INTERPOL as a trusted third party which would be responsible for acting as a filter and anonymising the data collected from any particular national police force. In this way it was possible to elicit a number of responses from European countries and beyond, though the anonymisation of the data would prevent the

10 We assume "position" may be best suited when we do not know name of the place.

RESPECT research team from achieving direct corroboration or any form of triangulation with the national reports obtained otherwise.

The following investigations were carried out as part of the national studies:

- Inquiry directed to the national telecommunication authorities ("telecom inquiry").
- Inquiry directed to the national data protection authorities ("data protection inquiry").
- Inquiry directed to Internet service providers operating in the national market of each country ("ISP inquiry").
- Document studies in government dossiers etc. in each country ("document study").

The list of national research institutions participating in the telecom inquiry, data protection inquiry and ISP inquiry is included as annex 1 to this report. From some of the countries, it proved difficult to collect information. Thus, most of this report concerning the national study is based on answers from eight of the twelve countries originally included in the research design.[11]

Nonresponse from the four countries listed in the table is due to different circumstances for which we have no full overview.[12] The major reason is probably that the national research groups did not succeed in getting responses from the relevant authorities and ISPs.

Some of the authorities which responded to our inquiry did not answer every question. Such omissions will be commented upon when we present the results.

Statements in the inquiries are to a large extent worded in ways which enable different interpretations. Such problems occur, of course, in most research questions expressed in natural language. Our inquiries are to a large extent exposed to this challenge. This is first and foremost due to three characteristics. Firstly, some statements are formulated by means of terms from the legal domain which do not necessarily have equivalents in each of the national languages applied. Secondly, and probably most importantly, several statements are worded on an overall level taking PT technologies as example. These technologies have many and very different uses, and thus answers may rely on specific conditions and situations. Thirdly, since questions highlighted issues regarding police investigation, secrecy limitations were foreseen. We were aware of these problems and thus stressed in the introduction of all inquiries that:

11 These eight countries are Austria, Bulgaria, Germany, Italy, Norway, Romania, Slovakia and Slovenia. Regarding response rates etc. of the Interpol inquiry, see section 2.2.3.

12 In Malta for example the data collection period coincided with the run-up to and the aftermath of national elections including a change of government, a process during which it proved difficult for data to be gathered since many officials were reluctant to take action about requests for information.

> *"We are fully aware that aswers to questions may be uncertain and thus based on approximate assessments of the respondent . Although we expect that our questions should be possible to answer within legal regulations of secrecy, we also respect that some issues may be too sensitive to answer. In these cases, please indicate that the information could not be given due to secrecy reasons."*

Regarding the two first problems, we seeked to counter unwanted effects by inviting respondents to give comments and additional information to every question. Some general statements from respondents expressed problems of answering our questions.[13] However, supplementary comments were very few. Nontheless, answers to some of the questions indicate that respondents may have based their replies on different conditions. In the presentation of results we will highlight such uncertainties, see in particularly in chapter 5 and 6.

2.2.2 National studies

All four questionnaires applied as part of the national studies were brief and mainly based on a multiple choice technique, often related to statements where respondents were asked to choose one or several alternatives by ticking off a box. Comments were allowed on all sets of statements, and in some instances even to each statement.

The use of a questionnaire makes it easy to compare answers from different countries, but was mainly chosen in order to increase chances of a high response rate from relevant national authorities and ISPs. Another concern was to minimize work load for the national research teams. Almost all teams were members of both the RESPECT and SMART project, each project with many work packages. The idea was that brief and simple questionnaires would make it simple for national teams to follow up and have responses from telecom authorities, data protection authorities and ISPs.

In order to facilitate high response rates, national questionnaires were translated into the respective official languages. Translations were organised by the WP leader and checked by the respective national research teams. Questionnaires were then communicated to national telecom authorities, data protection authorities and a selection of ISPs in each country.[14] We received answers from:

- Eight data protection authorities,[15] of which two (from Italy and Romania) were only brief statements;

13 For instance, the data protection authority of Slovakia commented to question 4 of the "data protection inquiry" (see below) that "We believe that results from this questionnaire may be difficult to interpret and may even lead to the wrong conclusion ...".

14 Our intention was to receive answers from a minimum of three ISPs from each country.

15 Authorities in Austria, Bulgaria, Germany, Italy, Norway, Romania, Slovakia and Slovenia.

- Nine telecommunication authorities in eight countries;[16]
- 20 ISPs, ranging from six to one ISP in each country.[17]

Some responses were incomplete in the sense that a few statements/questions were not answered, but this has no significant influence on the applicability of results. A few of the authorities made comments, but the main picture is that results almost only exist in the form of responses to multiple choice questions.

The scope of inquiry and the number of responses of course do not give a representative picture of the European situation, and percentages and average figures are thus not meaningful. It is of interest, however, to show similarities and differences on a country level of selected points included in the questionnaires. It is also of interest to see the degree of concurrence and dispersion of replies. Our investigation does not, however, allow us to explain similarities and differences.

2.2.3 Interpol inquiry

The *Interpol inquiry* was directed towards police authorities in all 190 Interpol offices, and carried out in collaboration with the Interpol headquarters in Lyon, France. Use of a questionnaire was mainly chosen in order to increase chances of a high response rate. This was particularly important with regard to the police inquiry because Interpol offices received several questionnaires in addition to those connected to RESPECT WP7, both other work packages in RESPECT and in the SMART project which was carried out according to a similar design.

A draft questionnaire was made by the WP leader, and sent to each national research group and the Interpol office in Lyon. Feedback from Interpol caused several changes of questions and design of the questionnaire. With Interpol as intermediary, these questionnaires were anonymised. Thus, the identity of the country of responding offices is not known to the WP leader or the research groups.

Before the questionnaire was sent to Interpol offices, it was translated into the four official languages of Interpol. Only information on the region of the world where the responding police offices are situated has been made known. The following regions have been used to classify results:

- Europe (12)
- Middle East and North Africa (6)
- West Africa (2)
- East Africa (6)
- North America (2)

16 Authorities in Austria, Bulgaria, Germany, Italy, Norway, Romania, Slovakia and Slovenia. We received reply from two relevant Italian telecom authorities.

17 Austria 1 ISP, Bulgaria 6, Germany 1, Italy 3, Norway 1, Romania 1, Slovakia 1 and Slovenia 4 ISPs.

- Central America (4)
- South America (2)
- Asia (3)
- Oceania (0)

Figures in brackets indicate the number of replies from each region; 37 replies in total, constituting a response rate of approximately 20 %. The figures are of course much too low to give any representative picture. Moreover, the fact that country identity is hidden from the researchers makes it impossible to draw upon context and other information to do analyses of specific countries. Therefore, conclusions on basis of this material could only be made with great prudence and only when very clear patterns are identified; in particular when answers are more or less unanimous or when there are sharp differences. Even when general conclusions may be drawn, the nature of them will practically be that there are indications in a certain direction etc. Moreover, we are not able to explain what seem to be identified tendencies etc. In that sense, the results are more of a prelude to further research than final results.

2.2.4 General methodological considerations

Above we have emphasised some of the limitations of possibilities to draw general conclusions on the basis of the two investigations of WP7, and of combining results from the two investigations. Notwithstanding this, and in addition to the concrete conclusions that may be drawn upon the existing material, the two inquiries have, in our view, proved fruitful to generate basic insight into the problem field. Examples from various countries – with known or unknown identity – have been very valuable in developing general understandings of questions regarding use of personal location data etc. in the fight against crime, and appurtenant privacy and data protection questions. Thus, one characteristic of the way we use results from the inquiries of WP7 is to extrapolate and suggest approaches and overall models to which all or most of our examples fit, and which thus should be tested as general vehicles for privacy and data protection authorities and advocates, as well as police authorities. Regarding these parts of the results, we refer to the sections titled "Concluding observations". Some elements of such general insights are even placed outside concluding sections of this report but are nonetheless a result of the project. The models in section 3.1 and section 3.3 (below) are typical examples of such results.

3 Positioning and tracking technology (PT technology)

3.1 Introduction

This chapter aims at communicating some basic knowledge and insights regarding technological issues particularly relevant to WP7 of the RESPECT project, i.e. positioning and tracking technologies, PT technologies. Our point of departure is a simple model which pictures main elements of the discussion in this report and places technological issues in the context of social effects and normative questions.

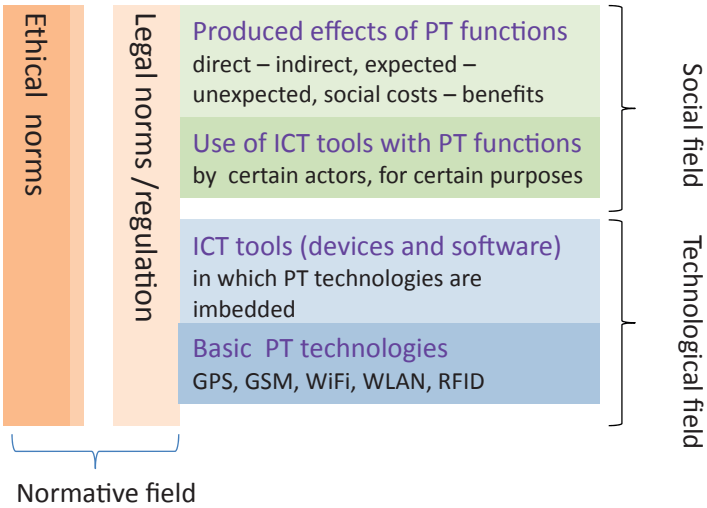


Figure 1 Overall model of technological, social and normative aspects of PT technology

The model consists of four horizontal layers, building from basic technologies to produced effects of ICT tools where these basic technologies are used. We have no strict definition of "basic technologies" and more examples than those mentioned in Figure 1 could be added. The point is that these technologies are basic in the sense that they are/could be combined and integrated in ICT tools/devices and thus be part of complex technologies. The model is of general nature. Here, in the context of WP7, we have narrowed it by selecting special types of basic technologies which could be used to locate and track people and objects. The

smartphone is a good example of a device which combines and integrates several such basic technologies.

Technologists may have problems accepting our classification of some technologies as "basic". There are, of course, technologies on which GPS, GSM etc. are based which are even more basic.[18] However, our point is only to – quite pragmatically – identify technological *construction bricks* for building advanced and complex ICT tools that may be applied to locate and track, not to tell the whole "technological truth".

The second layer in the model should be largely self-explanatory. It represents devices/systems (hardware, software) in which basic positioning and tracking technologies are combined and integrated with other technological elements and features. An important background for this is the experiences in TRANVIK (2013), and research on fleet management systems in the business sector. Here, we have seen a development from quite simple systems based on, for example, GPS for the purpose of tracking vehicles, to much more advanced and complex systems where tracking cars etc. is one of many functions integrated with back-office systems etc.[19]

We choose to denote the two first layers the *technological field*, among other reasons because we believe regulatory/normative strategies should be/must be/are different in this field than in the *social field*, cf. next two layers. The layer "use of ICT tools" represents descriptions of actual application of the technology, an object of study enabled by describing functions, asking about purpose for use, etc. In WP7, for instance, we have mapped areas of application where location and tracking is a part (e.g. payment, access control, marketing etc., see sections 4.3, 4.5, 5.6 and 5.7).

The top layer in the social field is about the effects of PT technology use. We may talk about social (and other) costs, but also of various types of benefits – and of course effects which are hard to classify as "good" or "bad" (because people disagree, because "time will tell" etc.). Some effects can be directly and simply observed, while others are indirect and are often the results of complex synergies. Many effects are anticipated, but because technologies will be introduced in many different and complex social patterns and processes, occurrences of unanticipated effects should be expected. We may also make a distinction between intentional and unintentional effects (which could be both expected and unexpected) etc. The point here is not to present a complete inventory of social effects of ICT tools with PT functions, but to emphasise that it may be useful to have some common subcategories to introduce as starting point of analyses.

18 For instance microchips.

19 Tranvik (2013).

The second main element of the model is on the left hand side (vertical) and represents three *normative aspects* ("normative field"). The main point here is that every layer is/should be subject to some sort of norm system, be it ethical, social or legal norms. An important aspect is the interplay and synergies between different types of norm systems. Choice of regulatory strategy should be based on knowledge of such normative interactions. Effective regulation would probably require different normative strategies on different layers. The overall question is of course: *which normative strategies work* if we want to protect life, health and property from criminal acts and at the same time safeguard privacy and legal protection?

Aspects linked to the social and normative field will be discussed in Part II of this report. The remaining portion of this chapter will be used to provide some fundamental information regarding the selected basic technologies that may be used to position and track objects and people (PT technologies). In section 3.2 we will first and foremost be on the first layer in the model presented above, but even some examples of more concrete application of these technologies will be mentioned (cf. second layer). Thereafter, in section 3.3, we will develop some general views on how PT technologies may be used to pursue the objectives of positioning and tracking.

3.2 Basic technologies

By and large, the very brief descriptions of basic technology in this section follow at least a common list of issues:

- What the technology does
- How the technology works
- Main cost elements
- Questions related to technological interoperability

The level of detail of our technological explanations below is low and adjusted to the purpose of our elucidation, namely to communicate the nature and potentials of each technology. To the extent that more in-depth information is required as basis of specific discussions later in this report, this will be given in that context.

3.2.1 GPS

The Global Positioning System (GPS) is a satellite-based navigation system that provides a receiver on the ground with location and time information.

The current system uses a total of 24 satellites (plus three spare) and 12 ground stations spread around the globe. To function, the receiver requires unobstructed

view to at least four GPS satellites. The system does not work inside buildings or in tunnels. The resolution accomplished with the current system is on the order of 10 metres (Kaplan 2005).

The current system is operated and maintained by the United States government's Department of Defence. However, GPS is freely accessible and usable by anyone around the globe with a GPS receiver. It serves both military and civil uses.[20]

To remove the dependency upon the goodwill of the USA, other governments are developing alternative satellite based navigation systems, including *GLONASS* (Russia), *Galileo* (European Union), *BeiDou* (China), and *IRNSS* (India). These systems are still under development.

Since the non-US systems do not yet exist, there is no way of predicting the extent to which these systems will be interoperable with each other. However, the International Committee on Global Navigation Satellite Systems has expressed a strong commitment to interoperability[21]:

> *Interoperability refers to the ability of global and regional navigation satellite systems and augmentations and the services they provide to be used together to provide better capabilities at the user level than would be achieved by relying solely on the open signals of one system.*
> - *Interoperability allows navigation with signals from different systems with minimal additional receiver cost or complexity.*
> - *Multiple constellations broadcasting interoperable open signals will result in improved observed geometry, increasing end user accuracy everywhere and improving service availability in environments where satellite visibility is often obscured.*
> - *Geodetic reference frames realisation and system time steerage standards should adhere to existing international standards to the maximum extent practical.*
> - *Any additional solutions to improve interoperability are encouraged.*

The initial civilian use of GPS was in the form of a dedicated physical device that received positioning data from satellites and showed the user his or her current location on a digital map. These devices were usually mounted as an aid for navigation in a boat or a vehicle, but handheld dedicated GPS devices also exist. While there is no need to retain any data to perform this mapping function, most dedicated GPS devices also allow the user to automatically record the current

20 Most of GPS commercial devices currently on the market use either the *SiRF Star III* chip (20 tracking channels) or the newer *MTK MT3329* (aka. *MTK v2*) chip (66 searching, 22 tracking channels). Both chips have a good reputation for accuracy, but the *MTK MT3329* is supposed to consume less power, be more sensitive, and provide a faster fix than the older *SiRF Star III*.

21 Third Meeting of the International Committee on Global Navigation Satellite Systems, 8-12 Dec. 2008, Pasadena, California, http://www.insidegnss.com/auto/ICG-3_Joint_Statement_&_PF_Report.pdf

position (waypoint) to a log file a regular intervals. The purpose of the waypoint file is to show the user's *itinerary* on a map at a later date.

The waypoint file created by a consumer GPS device is on a standard format. It is *not* hardened against manipulation by encryption or other means. In other words, it can be inspected and tampered with by anyone who has access to the file.

Most dedicated GPS devices have an USB port that allows them be connected to a computer by cable. When they are connected, the GPS-device file system appears as a removable USB disk. Waypoint files can then be transferred between the computer and the GPS-device by drag and drop. Most producers of GPS devices provide free software to access and visualise waypoint data, but since the format is standard and not encrypted, third party software exists that also does this. Some third party programs allow extensive analysis of movement patterns and may also let the user edit the file.

Since *dedicated* GPS devices are only capable of transferring data to other devices by cable, physical access to the device is required to get access to the positioning data stored on these devices. For the police, this means that to gain access to the data recorded by a standard consumer dedicated GPS device owned by, and carried by, the subject, they need to have physical access to the device.

In fiction, covertly planting a tiny GPS-tracker with the capability to "phone home" is sometimes shown as a police method for tracking a suspect's movements. It should be noted that given *current* technology, the size and weight of the battery that will be needed to power such a device for more than a few hours precludes hiding the GPS-tracker in the suspect's clothing, but it will be possible to hide the tracker inside a car or another large and heavy object.

In addition to dedicated GPS devices, GPS chips are now often embedded in cars, smartphones and digital cameras. Some of these devices also have the capability to communicate wirelessly. The pan-European eCall system for cars is discussed in a later section. As for smartphones, they have wireless communication capabilities and are capable of reporting GPS personal location data to a cloud service. Some digital cameras have similar capabilities. Some of devices are even shipped with the function to upload position data to a cloud service enabled. If the owner does not want this to happen, he or she needs to *disable* the function that uploads GPS data to the cloud. Popular cloud services for storing GPS data are *Google+, Apple iCloud, Facebook, Instagram. Flickr, Nikon Image Space,* and *Glympse*. While these cloud services provide some privacy settings that let the device owner control who gets to see the GPS data by default, all these positioning records can, by *subpoena duces tecum*,[22] be handed over to the police for analysis. In other words, for the police to be able to access the data, physical access to the GPS device is only necessary if the data is not stored in the cloud.

22 I.e., subpoena for production of evidence.

3.2.2 GSM: Digital cellular networks

Digital cellular networks provide wireless service to cellular phones. The set of protocols used by digital cellular networks are most often referred to as "GSM", which refers to *Global System for Mobile* communications. This was initially a set of protocols for mobile telephones originally developed by the European Telecommunications Standards Institute (ETSI) for so-called second generation (2G) networks first deployed in 1991.

Since it first appeared, GSM has been extended with *Universal Mobile Telecommunications System* (UMTS) for third generation (3G), and *Long Term Evolution Advanced* (LTE 4G) for fourth generation (4G) cellular networks.

In addition to voice telephony, it offers packet data transport via General *Packet Radio Services* (GPRS) and *Enhanced Data rates for GSM Evolution or EGPRS* (EDGE).

A digital cellular network works by using radio to communicate between a portable computer, tablet or telephone (UE - user equipment) and an antenna radio tower (BTS - base transceiver station) nearby.

The technology of positioning is based on measuring power levels and antenna patterns, taking advantage of the fact that the user equipment always communicates wirelessly with one of the closest base transceiver stations. This means that knowledge of the location of the BTS implies the UE is nearby.

More advanced tracking can be done either via triangulation of radio signals between (several) radio towers of the network and the UE. To locate the UE using triangulation of radio signals, it must emit at least the roaming signal to contact the next nearby antenna tower, but the process does not require an active call.

The cost of setting up and maintaining a BTS is split between the cost of buying the necessary hardware (tower and electronics), and the annual lease of the location where the tower is mounted.

The cost of a tower mounted Motorola HDII BTS was in 1990 USD 450 000. In 2010, a successor model named Motorola Horizon II cost USD 40 000[23]. The reduction in cost follows the general trend of electronics becoming smaller and cheaper. The cost of leasing a location to place the BTS varies with the location, being higher in urban areas than in rural areas.

The area covered by a BTS is known as cell size. The maximum cell size for GSM where the BTS is transmitting at the maximum allowed 8 watts is about 35 km radius around the BTS, assuming an undisturbed line of sight between the BTS and UE. This cell size is only used in sparsely populated rural areas.

In urban areas, cell size is usually determined by landscape, architecture and access to suitable mounting locations, and the number users that are assumed to exist within the cell radius. Urban cell sizes range from about 2 km to as few as 10

23 Md7: Cell Site Rents Must Line Up with Other Costs, http://www.md7.com/assets/001/5073.pdf

metres (the latter only operates indoors, for instance inside an office, and is served by an inconspicuous low power and low cost wall mounted radio transmitter).

Obviously, the smaller the cell size, the more accurate the GPS position identification.

The initial GSM networks were incompatible between continents, mostly due to different radio frequencies being used. This meant that a handset sold on the European market would not work in the USA or in Japan, and international travellers needed to carry several handsets with them to be able to use them in all locations. This is no longer the case, both because the industry has become more standardized, and because handset manufacturers make sure devices have the required radio frequency circuits built-in to work all over the world.

All digital cellular networks share the property of recording information that links the UE to the BTS it communicates with. This means that it is impossible for the user to avoid positioning data from being collected as a side-effect of using cellular technology.

The positioning data collected by the service provider is, as a rule, stored in database records that also contain a link to the identity of the subscriber that uses the service. There are no specific requirements for the service provider to maintain the integrity of the data (for instance by physical barriers or cryptographic means), but there is obviously an implied trust that the data will not be manipulated in the EU and EEA data retention directive[24], which requires the service provider to retain this data for police purposes for a specific period (from six months up to two years, depending upon the implementation of the directive by the member state).

The police can possibly get access to this data by *subpoena duces tecum*. However, there is no standard for how this data is to be formatted, which means that analysis of this data must be done "by hand", or by means of custom software.

3.2.3 WLAN and Wi-Fi

Wi-Fi is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as «wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards». However, since most modern WLANs are based on these standards, the term «Wi-Fi» is used in general English as a synonym for «WLAN». Only Wi-Fi products that complete Wi-Fi

24 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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.

Alliance interoperability certification testing successfully may use the «Wi-Fi CERTIFIED» trademark.

A device that can use Wi-Fi (such as a personal computer, video-game console, smartphone, digital camera, tablet or digital audio player) can connect to a network resource such as the Internet via a wireless network access point. A single access point has a range of about 20 metres indoors and about 250 metres outdoors. The total area served by a particular WLAN is called a hot-spot. Hot-spot coverage can comprise an area as small as a single room where walls blocks access to the radio waves from any outside location, to large area covering many square miles. The latter is achieved by using multiple overlapping access points to extend the hot-spot.

The cost to establish and operate a single Wi-Fi access point is low. Most smartphones already have a built-in Wi-Fi wireless router, and can be used as an access point for a few (usually two) additional devices. A standalone wireless router for home use supporting several devices simultaneously may cost from 25 EURO and upwards. The equipment used by public Wi-Fi hot-spots, such as those found in pizza parlours and airport lounges, usually cost up to 400 EURO per access point. To set up multiple access points to cover a larger area, multiply this cost with the number of access points.

Most new devices satisfy the Wi-Fi Alliance interoperability requirements and will connect to any equipment that uses one of the Wi-Fi protocols defined by IEEE.

Wi-Fi enabled devices are discoverable without being used. The information that is discoverable *without* making use of the hot-spot provider's service is the device's identity (often referred to as a MAC-address or media access control address). This is an address unique to the network interface of the device. It is allocated when the device is manufactured and is not supposed to be changed during the device's lifetime.[25]

Many providers of public Wi-Fi access points record and retain the MAC-addresses of *all* visitors, including non-users. This is, for instance, to keep a track of the individuals that visit their location in order to spot repeat visitors and to monitor the length of individual visits.

In Denmark, there is a legal obligation for public Wi-Fi access points to log and retain the MAC-address of user's that connect to their network along with the physical location of the access point, re. § 5 (stk. 3):

25 It should be noted that most current devices allow people with root access to the device to change or spoof the MAC-address. However, obtaining root access to most mobile devices is not trivial and also voids the device's warranty. As a result, few people who are not privacy fanatics or criminals do root their devices to change its MAC-address.

> *Providers of electronic communications networks or services to end users providing wireless access to the Internet, must also record information about the local network's exact geographical or physical location and the identity of the means of communication employed.* (our translation)26

While the above requirement is part of the Danish executive order implementing the EU data retention directive[27], this requirement is not part of the directive and, as far as we know, no other EU or EEA member state has made it mandatory for providers of public Wi-Fi access points to register the MAC-address of user's equipment.

If the user makes active use of the service, a lot more information than the MAC-address is discoverable by the hot-spot provider (everything, in fact, which is why users concerned about privacy and security should be careful when using public Wi-Fi access points).

The amount of user data that is actually discovered and retained is left up to the owner of the hot-spot, but it is not unusual to make hot-spot providers record the MAC-address, the IP-address, the unique username assigned for the session, and session time.

While the MAC-address identifies the equipment and not the person, there are a lot of registers that record the MAC-address along with data that is considered personal, such as an IP-address. This means that an entity with access to a log of MAC-addresses and another register that connects the MAC-address to personal data will be able to use the MAC-addresses retained by a Wi-Fi hot spot to track an individual.

Data retained about visitors' proximity to, or use of, a Wi-Fi hot-spot is stored in a database by the provider of the Wi-Fi hot-spot. There is no standard for the format of this data. The integrity and security of this data is completely dependent upon the provider.

It appears that there has been little interest from the data inspectorates in the EU and EEA to monitor the extent to which providers of public Wi-Fi services retain personal data about users of their system.

The police can possibly get access to this data by *subpoena duces tecum*.

---

26 Original quote (Danish): «Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere, der udbyder trådløs adgang til internettet, skal endvidere registrere oplysninger om det lokale netværks præcise geografiske eller fysiske placering samt identiteten på det benyttede kommunikationsudstyr.»

27 Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen).

3.2.4 RFID

Radio Frequency Identification (RFID) is a tracking technology that is based upon small, inexpensive microchips ("tags") that can be attached to consumer goods, pets and farm animals, vehicles and other objects – and indirectly or directly to people.[28]

In the initial phase of RFID adoption, there was little emphasis on interoperability, and names, tags and readers from different manufacturers were not compatible with each other. This was a major problem, since tagged goods where moving about, and tags created at one location could not, as rule, be considered meaningful or readable at another.

Around the year 2000 the Auto-ID Center at MIT initiated a research programme directed towards the development of RFID standards in order to foster more widespread adoption of RFID. The project's vision was the creation of an "internet of things", i.e. a tight coupling of physical items and digital information flows based on inexpensive RFID tags (Brock 2001).

This work resulted in a global standard known as the *Electronic Product Code* (EPC) that classifies the name-spaces, types and protocols used by RFID tags. The standardization ensures that name-spaces do not interfere with each other, and that standard compliant tags and readers can communicate. There are five classes, numbered from 0 to 4. These are:

- Class 0: Read only, 64 bit, passive, programmed by factory.
- Class 1: Write once read many (WORM), ≥96 bit, passive, programmed by user and locked.
- Class 2: Read/write many, ≥96 bit, passive, (re-)programmed by user.
- Class 3: Read/write many, bulk memory, semi-passive, (re-)programmed by user.
- Class 4: Read/write many, bulk memory, active, (re-)programmed by user.

While the standard only ensures that devices belonging to one class are compatible with other devices of the same class, most readers of a higher class also work with devices of a lower class.

A passive tag contains no radio transmitter, but reflects a small fraction of the power emitted by the RFID reader. Passive tags have no battery power, and they only work in close proximity. Typical RFID tags used for electronic tickets for mass transport systems and attractions need to be closer to the reader than 10 cm to be read, while tags used for merchandise tracking need to be closer to the

28 Direct attachment to people would imply some sort of integration with the human body, a measure which rarely occurs (see bulletpoints below for some examples). Thus indirect connection between RFID and people is the normal situation; for instance an RFID card used as a key to unlock doors.

reader than 4 metres to be read. However, passive tags exist that can be read from as far as 10 metres.

A passive RFID tag cannot be switched off. This means that the communication between the tag and the reader cannot be controlled by the owner in ways other than putting it inside a container that shields it from radio frequency emissions. Also, there is no visual or other indication that a passive RFID tag is communicating with a reader, making it ideal for covert information collection.

A semi-passive tag also contains no transmitter, and is in that way similar to a passive tag. However, it has an embedded power source (battery) that may extend their range to about 15 metres.

To poll a passive or semi-passive RFID tag, the reader transmits radio waves that activate an antenna in the RFID tag. The antenna then transmits information back to the reader via a pre-determined radio frequency. This information is captured by the reader.

Active tags have an embedded transmitter and power source. It can communicate two-way with peers and readers, using standard Wi-Fi protocols such as IEEE 802.11b. Since active tags emit their own radio signal, they can communicate without line of sight and they may work well at ranges up to 250 metres or more (outdoors). Unlike passive and semi-passive tags, active tags may have their range extended by peers acting as repeaters. The amount of data that can be retained on an active RFID tag also varies.

The cheapest class 0 passive tags may consist of a 64 bit EPC inlay (i.e. chip and antenna printed on a substrate). The cost for the cheapest Class 0 tags in volume starts around 0.05 Euro. Such passive tags may only store a single serial number that must be programmed by the factory as part of manufacturing process.

At the time of this writing, Class 1 tags are the most widely used RFID tag; these cost around 0.10 Euro in volume, and user used to tag products and other objects for various logistics purposes.

Class 2 tags are used for the holding the biometric data embedded in a so-called electronic passport, for contactless ticket systems for mass transport, and for contactless payment cards. These cost from about 0.50 Euro in volume.

Class 3 and 4 tags may have extensive read-write memory and advanced data recording and processing capabilities. The prices of these tags starts at around 20 euro. Class 4 tags with protective housing, special batteries, long range and integrated sensors can cost more than 100 euro.

Generally speaking, the cost of an RFID tag depends on a number of factors, including the order volume, the amount of memory on the tag, and the packaging of the tag (for instance whether it's a proper electronic circuit encased in plastic and have a wire antenna, or the circuit and antenna is printed on a substrate), and whether it is active or passive.

The use of semi-passive and active tags is not widespread. However Class 1 and Class 2 RFID tags abound. More and more objects ("things") in the physical world are being equipped with such tags. Their low cost makes them attractive for a number of uses, including what is referred to as the "Internet of Things" (IoT), where the core idea is to integrate the physical world with the virtual one.

We shall return to the IoT towards the end of this section, but first we shall mention some examples of popular uses of RFID Tags:

- Product RFID tags are for instance used for stock control in shops and warehouses, which means that each product being tracked has an embedded tag. This tag may be generic (all samples of a certain object carry the same tag) or unique.
- Another example is in so-called "electronic passports", where a unique RFID tags will communicate the identity and miscellaneous biometric information about the bearer when read.
- A popular use of RFID tags is for Electronic Toll Collection (ETC) on roads and bridges, where a vehicle is identified by having a unique RFID tag and use is metered by means of a central database that keeps track of the vehicle's movement. A related use of RFID is for electronic tickets for mass transport systems and attractions. These systems may be designed to be used anonymously, by having some means of collecting pre-payment that is associated with the unique RFID tag. However, many operators of these systems seem to have a strong desire to collect data about their customers, and deliberately design the system so that it is not possible, or very inconvenient, to make anonymous use of the system.
- A very radical use of RFID identity tags is offered by a company named *Verichip*. They have developed a RFID tag that is encapsulated in a glass capsule the size of a grain of rice and designed to be implanted inside the human body. So far several uses of this technology have been reported, for instance:
  - In one project, the tag is implanted in the arms of Alzheimer patients. When an unresponsive patient enters a hospital equipped with a *Verichip* RFID reader, the staff can use it to scan the patient's arm, identifying the patient and thereby get immediate access to the patient's identification and health records *Verichip's* database (RFID journal 2007).
  - In a second project, the company *CityWatcher* have *Verichip* RFID tags implanted in the arm of their employees as a means to secure that only authorized personnel have physical access to certain areas (WorldNetDaily.com 2006).
  - In a beach bar in Barcelona, RFID chips have been inserted under the skin of customers in order to allow payment and access to the VIP area. The

rationale behind this arrangement was to allow customers in bikinis and swimming trunks to avoid having to bring their wallets.[29]

- In Mexico, RFID chips inserted into the fatty tissue of the arm between the shoulder and elbow have been sold as a safeguard in case of kidnapping. In combination with a small GPS device, the technology facilitates localization of kidnapped persons.[30]
- RFID is widely used as part of home detention curfew arrangements. In these cases, the RFID device is usually integrated in an ankle bracelet, but it could also be placed under the person's skin.

Unlike keys and codes, RFID implants in the human body cannot be lost, compromised by theft or leaked.

Already, RFID is extensively deployed in the shape of electronic passports, electronic toll collection, and in various contactless ticket systems. The data collected from all these systems are retained in databases that are maintained by system operators. With the exception of records of cross border travels that are retained for security reasons, most of these databases exist for accounting purposes and their formats are not standardized beyond what is prescribed by the EPC. As with the data coming from GSM and Wi-Fi systems, the integrity and security of the data depends on the entity that collected it.

There is no legal requirement to retain RFID data for police purposes. In the EU and EEA, the data inspectorates requires the data collected for accounting purposes to be deleted as soon as they are no longer required for that purpose.

The police can possibly get access to this data by *subpoena duces tecum*.

3.2.5 Internet of Things (IoT)

In addition to widespread use of RFID-tag due for purposes that are *not* immediately associated with the IoT (as described above), a number of IoT researchers have set up projects where users are asked to tag their personal belongings with RFID tags and also provide an infrastructure (typically in a department or building within their research institution) to track those tags.

To track objects in the IoT, the tag identifiers attached to each object is recorded, along with the object's profile in a central database. Then, by having RFID readers positioned at key locations (such as doorways and stairs) in the physical

29 See The Guardian, "I've got you under my skin", 10 June 2004 (http://www.theguardian.com/technology/2004/jun/10/onlinesupplement1)

30 See The Washington Post, "Scared Mexicans try under-the-skin tracking devices", 14 August 2011 (http://www.washingtonpost.com/world/americas/scared-mexicans-try-under-the-skin-tracking-devices/2011/08/14/gIQAtReNUJ_story.html?hpid=z4).

environment, it is possible to track both the object's current location and its history in the database.

There are obvious privacy risks associated with the IoT. In addition to information leakage from the objects themselves (such as identifying the title and subject matter of a RFID-tagged book carried by a person), a very detailed record of a person's physical movements can be extracted from the waypoints, resulting in a log of information from a particular RFID tag attached to an object belonging to a specific individual.

In a four-week experiment at the University of Washington, 67 participants carried a "personal" RFID badge and RFID-tagged in total 324 personal belongings such as wallets and laptops. The participants were given full access to the database, including the right to delete data collected about them. The experiment explored several aspects of IoT, including privacy control. There was only one instance where a participant deleted data (and the user who did so said in the exit survey that he did so merely to verify that this tool worked). However, the users where focused upon defining access control rules to protect their data. The users had few privacy concerns because the data was collected as part of a controlled experiment. However, 76 per cent of the users said that they would be concerned if their employer had this data, and 84 per cent said they would be concerned if the government had the data. (Welbourne et al. 2009)

3.2.6 Auxiliary technologies

In addition to the core technologies discussed above, modern life involves frequent encounters with a large number of electronic devices that retain a visual record or log interactions such as:

- Automatic number-plate readers
- POS (Point of sale) terminals
- ATM (Automated Teller Machine)

These technologies are not discussed here because they are not positioning or tracking technologies as this concept is understood in this project. They are technologies with a known location that record events taking place at that location. As such they can be used to link humans and artefacts such as cars or credit cards to that location at a specific time.

There are also technologies useful to the police as methods by which to identify individuals from biometric characteristics, such as:

- Facial, retinal or gait recognition (all based upon Closed Circuit Television)
- Fingerprint based entry systems

These technologies may be useful when the police want to place (or eliminate the presence of) a certain individual at a certain location at a specific time as part of a police investigation. However, according to the design of WP7 of the RESPECT project and the concept established to support relevant technology, they are not positioning and tracking technologies, and are therefore outside the scope of the empirical investigations in this report.

Finally there is a broad class of positioning and tracking technologies which are currently useful only in environments that have been prepared for their use with sensors for the technology (e.g. Bluetooth, infrared or ultrasonic sensors).

These technologies may be classified as PT technologies, but are not discussed in this report because the sensors necessary for this type of technologies are currently only deployed in limited and very specific environments (e.g. inside a warehouse for tracking the goods stored there). However, in the future, we may see that sensors for some of these technologies may be more widely deployed (for instance integrated is a mass transit ticketing systems). Such a development, with widespread adoption, may also put these technologies on the list of items that may be used as positioning and tracking devices for surveillance and police work.

3.3 Overall model of positioning and tracking technology

WP7 of the RESPECT project is about technologies that may be used to track persons and objects moving freely around in the world. In the previous section we have briefly presented the basic technologies which is the emphasis of this research, namely

- GPS (Global Positioning System)
- GSM (Global System for Mobile communications)
- RFID (Radio Frequency Identification)
- WLAN (Wireless Local Area Network)

When these technologies are used for positioning and tracking purposes, we assume that some common features may be identified as illustrated below.

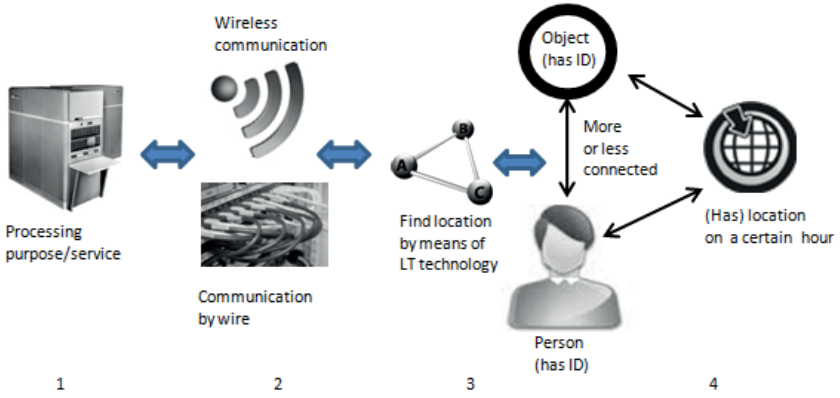


Figure 2: Basic chart of PT technology use

Figure 2 is divided into four steps in a positioning process. First, someone initiates the process for a certain purpose. The actor who carries out the positioning could, for instance, be the police with the aim of locating, surveying or arresting a person. Such direct use by the police, i.e. use where the police apply their own technology, is indeed practical and important. Notwithstanding, we emphasise here the use of these technologies as part of the production of services and execution of functions in the civil society. Thus, in our context direct application of PT technology *by persons other than the police* is important, i.e. use by various actors in the civil society, included government agencies. Our point is that the use of such technology in the civil sector has a considerable potential for collecting data regarding positions and movements of people and objects that later could be accessed by the police. The police may, in other words, make both primary (direct) use of PT technology and secondary use, based on services and functions in civil society. The rapid growth of ICT tools and devices in the consumer market and other parts of civil society which integrate location and tracking functions clearly expands the potential use of derived data by the police.

The first step of Figure 2 presupposes the determination of one or several purposes of the processing of which application of PT functions is a part. If used by the police, the purpose will most likely be to locate and track; for instance as part of monitoring, investigation or arrest of a person. However, in civil society, although positioning and tracking is integral part of processing, the purpose will be of another type, for instance to carry out payment and execute access control to a building. This is an important point: Production of PT data may in some

situations be apprehended almost as a side-effect of the service or function that is carried out, and is not necessarily linked to the purpose of the processing.[31]

Step 2 of Figure 2 illustrates that purposes/services in question require some sort of electronic communication. Communication could be by wire or wireless. All PT technologies identified and listed as basic technologies of WP7 are wireless, and in this report clear emphasis will be put here. Even wired communication, however, is included in Figure 2, for at least two reasons. Firstly, both wired and wireless communication may be used to locate and track people. The total capability of the police to use sources in civil society to locate and follow people could therefore only be assessed if we consider both groups of technology. Secondly, even communication processes which are primarily wireless may be reliant on wired communication systems. Signals to a GPS or RFID receiver may, for instance, be transmitted further though a cabled network. Thus, in practical terms it is often impossible to strictly exclude wired communication.

A central and basic observation is that every real world object has a time and a position. Step 3 in Figure 2 illustrates that PT technologies perform a positioning process. In this step it is firstly important to clarify how we use the terms "positioning" and "tracking". By positioning we mean the process of deciding where an object or a person is located. We will not make the question of preciseness part of this notion, and positioning may thus imply everything from very exact to very rough pinpointing of a location. Provided we know the position of the RFID reader, registration of passive RFID tags implies that we know exactly where the tag is. Positioning by means of GSM with low coverage may, in contrast, make positioning very approximate and unsure.

By tracking we mean the determination of two or more (a series of) positions of the same object. Thus, tracking implies the determination of movements (from A to B to C etc.), including assessment of the time and speed of these movements. Accuracy of tracking depends of course on the accuracy of each established position.

GSM, GPS, Wi-Fi/WLAN and RFID are all examples of technologies with the potential to position objects and connected persons. How this may be done differs from technology to technology, cf. the brief explanations in section 3.2 (above). Our second general point here is that there is a marked difference between the technologies we have grouped here as PT technology. For GPS and RFID, location and tracking could be said to constitute primary and major functions. For GSM and Wi-Fi/ WLAN, location and tracking could hardly be seen as primary functionality. Instead it is more a result of the basic qualities these technologies have in order to fill their primary function; namely to communicate various types

31 The main purpose of an RFID-based payment system is payment, and registration of where payments are made is not a prior goal for the use of this technology.

of data. These differences illustrates that "PT technologies" constitute a heterogeneous group which is defined in the context of this report for purely pragmatic reasons.

Regarding step 3 of Figure 2 it should be remembered that the types of PT technologies listed is far from a complete inventory of relevant technologies. Bluetooth, ultrasound and automatic number plate readers are examples that could perform wireless communication and thus be parts of services and functions which imply location and tracking of people and objects. Given the currently rapid technological development, it could therefore be claimed that our indications of PT technologies are first and foremost important as *examples* of such technologies, and that other future technologies may be just as important to the basic questions regarding positioning and tracking as part of police work. The fact that each type of technologies may comprise a range of capabilities helps to underscore the point that general technology designations (RFID, GPS, GSM, etc.) are not necessarily the most important. For instance, RFID comprises everything within the range of passive tags with very limited range to the most powerful wide-ranging active RFID tags (cf. section 3.2 above).

Step 4 of Figure 2 illustrates that objects and people are located and tracked by means of GSM, GPS, Wi-Fi, WLAN, RFID etc. Our first point is that the technologies we deal with here are *device based*. This means that in technical terms, the target of positioning and tracking is always an object and never a person.

What is targeted and located are different kinds of *devices.* Some of them are multifunctional and advanced, for instance vehicles (cars, boats etc.), portable PCs, smart phones etc. Others are unifunctional and relatively simple, such as RFID tags and GPS receivers.[32] The point here is that what we here denote as PT technology never reads the person itself; even if RFID tags are placed under the skin of a person – what is targeted, in a technological sense, is the device, not the person carrying it. The technology we deal with in this report is based on *non-biometric techniques*.

Various types of sensor and imaging technologies may be used to *identify persons directly* instead of identifying devices. Facial features, fingerprints and gait recognition are some examples of technologies which may be used to locate and track people. These technologies are not made part of this study, but must be taken into consideration if the whole discussion of positioning and tracking is to be addressed.

Some technologies could in other words be said to function through a biometric interface, while in the case of PT technology the interface is "techno metric". Technically assessed, there are probably sufficient reasons to make a clear distinc-

32 Such unifunctional units may of course be integrated parts of multifunctional devices, for instance in cars.

tion between technologies that may be used to position and track people directly by means of biometrical techniques, and technologies which may be used to position and track people by technometrical means, directed to objects.

From a normative, social and political viewpoint, the distinction between biometric and technometric techniques of positioning and tracking is probably also clearly relevant: Because biometric techniques read the body directly, it could be maintained that biometric techniques imply an annulment of the persons' right of self-determination. In our view, differences regarding effects for individuals and social effects make it important to maintain a distinction between biometric and technometric techniques, and in the following discussions we will not go further into questions particularly relating to biometrics. It is important, however, to bear in mind that there could be "innocent" applications of biometrics and "bad" applications of technometrics, indicating that differences between the two groups need not be very marked.[33] An RFID tag placed under the skin or a GPS bracelet locked around the ankle have strong negative effects for autonomy as do, similarly, biometric and unavoidable biometric sensors, but as opposed to the use of biometric techniques, the person in question will always be aware of the intervention.

Regarding PT technology (and technometric techniques), only objects with a unique identifier are relevant: A car has a registration number, and phones, PCs and similar devices have a SIM card, i.e. a subscriber identity module in the shape of an integrated circuit where the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers are stored. Similarly, RFID tags have integrated circuits with identification information.

These uniquely identified objects are more or less connected to a person.[34] Connections could be rather loose; a car, for instance, is often linked to the owner of the car being driven, but other family members, friends etc. might also be driving it; and in the case of company cars, a number of people may be driving. Unless additional information is available regarding who is actually driving the car or is a passenger, the identity of the persons that you locate and track when you follow the vehicle is in doubt. Smartphones are an example of a much more personal type of device where it is very probable (but not certain) that the registered owner actually is carrying the phone. Moreover, in contrast to cars, phones are seldom left far from their owners, and it is thus likely that the owner is located close to where the phone is. A third group of devices is strictly linked to a specific person's body. For instance persons under home detention wear ankle bracelet locked to their body; hospitalized people may wear a wrist bracelet with

33 Placing RFID tags under the skin of people is for instance an example of a very problematic use, while use of "anonymous biometrics" (which for instance only recognises individuals as customers or members) is example of a use which probably is quite acceptable to most people.

34 Or to an animal, but here this use will not be elaborated on.

ultrasound sender; and RFID tags may in extreme cases be inserted under the skin of a person (similar to what is done with farm animals and pets). In such cases it is very likely that the person is where the identified object is, but one can never be 100 per cent certain (in the absence of additional information).

The next point is that the persons to whom identified objects could be linked must be identifiable. One thing is, in other words, to establish links between the object and a person, another thing is to establish the formal identity of the person having the object under his or her disposal; for instance bring to light the person's national identity number, name and address etc. of the person in question. This is in contrast to situations where you only have an image of "someone". Police work could of course benefit from both levels of connection between the object and persons, but ultimately the goal will usually be both to identify the object and the person.

In some cases, objects do not have a special link to any particular person or all such links are loose and unreliable. For instance, containers may be identified with RFID tags which make it possible to locate and track them and their contents (goods, postal items etc.). In these situations object does not supply the police (or others) with a direct link to a physical person. However, also in such circumstances identified objects that may be followed could be of great value to police work. It may be of interest to follow specific persons' movements *in relation to* the movements of such an object (cf. smuggling), and the knowledge that a container has arrived at a postal office or customs office may make it possible for the police to manually survey people coming to collect postal items, goods etc. Here, we will not elaborate further on such possibilities, but remind the reader that this use is relevant and closely related to location and tracking of persons by means of objects.

3.4 Interoperability

There are two different types of interoperability issues with respect to the PT technologies discussed in this report:

- Device interoperability.
- Data interoperability.

Device interoperability is a measure of the how well the devices implementing a certain technology are interoperable with each other. As learnt from the early attempts to deploy RFID, the lack of standards for interoperability was a huge barrier for the deployment of a universal RFID infrastructure. Only after standards were implemented to ensure the integrity of identifier namespace, and robust protocols for communication between readers and tags from different manufac-

turers was it possible to make use of RFID on a scale that made it an "interesting" technology for tracking purposes (as well as a number of other uses).

Regarding the four basic technologies (GPS, GSM, Wi-Fi/WLAN, and RFID) that are the focus of this report, we assess the present degree of device interoperability to be high. This is probably not a coincidence, but a major reason behind the fact that all four technologies are widely deployed, are used for a rich set of services, and are backed by robust infrastructures.

While device interoperability is important to ensure adoption of PT technology, it is not important in terms of suitability of this technology for police work. For the police, data interoperability is important, i.e. that the data that is discovered, collected and retained by the entities (both devices and service providers) is available on standardized, tamper-resistant and well-documented formats. Data interoperability helps reduce costs associated with procurement, extraction and analysis of the data. Moreover, it facilitates to some extent use of already tested standard software for processing of data instead of making necessary expensive and error-prone custom software development. It will also help with upholding high standards for data integrity and data quality.

For two of the basic position and tracking technologies (GPS and RFID), standards exist for data interoperability. For waypoint data, there is *GPS eXchange Format*, and for locations embedded in images, there is EXIF Geolocation format. The latter is not a real standard, but supported by enough devices and software to be treated as a de-facto one. For RFID, there is EPC, as already discussed.

It should be emphasised that the data interoperability discussed above is not a complete solution to meet all police requirements. In the case of GPS and RFID, only a subset of the data that the police will need to procure, extract and analyse will be covered by the standards. The police will typically be interested in linking the location data to things and to persons, and this will require combining the structured standard data with other data that have less structure and probably much less documentation (cf. next section).

In the cases of GSM and Wi-Fi, as well as the data the police may want to utilise in conjunction with GPS and RFID (beyond the standards already mentioned), required data are collected by the operators typically as part of their internal accounting procedures. In those cases, there is no public documentation available about the data formats used. It is likely that each individual service provider uses a proprietary format that may or may not be properly documented. While the Data Retention Directive obliges the service providers to retain (some of) this data for police purposes and to make it available to the police pursuant to court order, the directive does *not* oblige the service provider to ensure data integrity or quality, nor does it oblige the service provider to document the data formats used so that the retained data can be used by the police without expending huge resources to transform the data into something that is usable for police purposes.

3.5 Costs

3.5.1 General perspectives

Costs of positioning and tracking technologies are difficult to assess for many reasons. The following discussion is based on the fundamental recognition that every person and object in the world has a place and time. Nothing and no one is "nowhere", and where they are at what time will often be of interest to someone and could be registered provided that something or someone makes the necessary arrangements. One such arrangement is to introduce and apply technology with features that make it possible to log or in other ways register location. Various types of technology have such features, and in this report we have particularly highlighted possibilities linked to GSM, GPS, Wi-Fi/WLAN and RFID.

It is an important fact that positioning and tracking *in itself* could have an economical value. Thus, these technologies are not first and foremost a matter of costs. Positioning and tracking services could have an economical value; for instance because it is part of a service in the consumer market which people are willing to pay for (e.g. use of GPS to embed personal location data in images uploaded to social media or to keep track of route, distance, time etc. as part of a training device). Also, the economical value of PT services could be more indirect: A service provider may both have profit by selling the service and at the same time utilise data from the service to develop, market and sell new or existing services and products. Last, but not least, PT technology which is imbedded and integrated in devices which have other purposes than positioning and tracking, will obviously be one of many bricks among many which is basis of profitable economic activities of various types: Use of RFID in locks in hotel doors is obviously a small element in the activity of running a hotel business, and payment by means of the same technology could of course be integral part of various businesses.

Seen from a police viewpoint, PT technology may easily be seen as cost. Use of PT technology by the police will incur expenses connected with acquisition of devices, collection of positioning and tracking data from civil society etc. The degree of interoperability will also influence the level of costs, cf. section 3.4 (above). In these situations, the technology is not used as part of an economical activity which generates income. On the other hand, to the extent that PT technology is effective as part of police work, it may of course reduce other costs.[35]

In the discussion of costs, it is important to make a distinction between costs for police and for the various services and functions in civil society that may be sources of personal location data for the police. An important point is that there

35 Cf. section 5.3 and results regarding inquiry of usefulness and cost-efficiency of these technologies, assessed by police respondents.

is a big and growing sector outside the police domain where PT technology is in use and which may serve as a reservoir of data in case of legitimate police needs. Thus, unless the police make requests for collection of such personal location data, the coming into existence of this data is without cost to the police. However, collection and further processing by the police will of course create costs for law enforcement.

It is hardly meaningful to try to assess the costs connected to all the many and increasing number of services and functions in the civil society which generate data revealing location and whereabouts of people and objects. Here, we only refer to the small selection of examples and descriptions in section 4.3 (below). Our first point is that the current number of different devices and services are too many to make reasonable assessments of costs across Europe and other parts of the world. In other words, we refrain from trying to assess costs of purchase and use of smart phones, various GPS-based and RFID services etc. The answer is that "it depends" on an over-complex range of circumstances. The main point in our context is that devices and services generally have costs which make them available to a large portion of the population, and they are accessible at costs ranging from free to expensive. Our second point is that no assessment of costs would be valid for more than a very limited time period and is thus of little value for discussions of police use of this personal location data in the future.

Extra costs to civil society may of course occur if the legislator or another legitimate authority has the power of imposing special requirements on the technical features of devices and services which are bought and used by citizens. Some services and functions are under special technical requirements because, for example, they are part of payment systems, other systems with special security requirements (access to buildings and documents), or because data from the technical system are intended to be used as basis of prosecution and conviction (e.g. speed control). Several technological and other requirements could be topical, but requirements regarding secure data storage and communication are probably the most important source of costs. Mere storage costs are generally low and have thus probably relatively little significance, both regarding volume and duration of data storage. Of much greater influence is probably costs related to secure storage and communication of data.

Data security costs will normally either rely on a concrete or a "standard" risk analysis and are thus basically results of discretionary considerations. The outcome of such analyses may thus be difficult to predict. The result could be to introduce measures of technological, economical, organisational, pedagogical and juridical nature. The concrete costs that will be generated for each type of services and functions producing personal location data depend on individual circumstances, and this falls outside the possible scope of this study. The Data Retention Directive implies storage of data on a location for a period of at least

six months and therefore represents a relevant problem area for secure storage of personal location data from other sources.

3.5.2 Cost – benefit

Basically, all parties using PT technologies may be regarded as taking on costs in order to gain some benefits. The benefits from the technology may, for instance, be the ability to document that a certain payment has been made (at a certain place); it may be for the pleasure of individuals to know and document that they have run their personal training trail in a certain time, etc. There is obviously no need to try and exemplify all the possible economic and non-economic types of benefits that can be associated with the application of a variety of devices, services and functions that are based on PT technology in civil society.

Cost-benefit considerations of the police are probably more homogenous compared to civil society. The aim would often be to prevent, stop and investigate crimes at the lowest financial cost, within an acceptable time frame and risk level. It would not be acceptable to seek prevention of a serious crime by means of a cheap measure if it implied high risk. In calm situations where most things are under control, assessment of risks and cost effectiveness could of course be carried out in highly rational ways. Given the great variety of situations which may occur in operational police work, it will however not be feasible to give a full rational analysis of alternative courses of action, and it must thus be assumed that some measures will be used (partly) because they are easily accessible.

The use of data from PT technology will often not be easily accessible to the police because legislation established to safeguard legal protection and privacy implies that the police will need a court decision or decision from a superior police body in order to legally collect such data. Thus, there will often be initial costs and need to invest resources in order to attain permission. In a first phase, collection of data from such technologies in ways which are directed towards individuals should in other words expectedly be rather expensive for the police (and the judiciary), because such measures will either need prior permission or succeeding approval.

Once permission from the court or from superior body of the police[36] is attained, concrete use of such methods (collection and analyses of personal location data) could, on the other hand, be quite cheap for the police.[37] In some cases, it is quite obvious that collection of personal location data is much cheaper than deploying other means of investigation: Having a detective inspector to tail a sus-

36 Typically in cases where it is critical to swiftly collect information in order to stop an evolving serious crime.

37 Dependent on interoperability, the model for division of expenditure between the police and the private party from whom the data is collected etc.

pect for many hours or for days will in most cases probably be much more expensive than collecting personal location data from the person's telephone company or ISP, alternatively to tag the person with a GPS device. On the other hand, a detective inspector may observe people and actions which will be missed out if personal location data alone are used, and thus it is not always obvious which police method would be the most effective (alone or in combination with other methods).

Here, we will not go into speculations about the police methods that are typically most cost-effective on various crime scenes. It may be that it is possible to work out standard cost models related to choice of police method, including collection of personal location data from various sources – but we doubt this will be a fruitful approach. In our view, it is however important to be aware of, and make visible, cost aspects related to collection and analyses of personal location data as measures of police work.

In section 5.3 and 5.4 (below) we refer to replies from Interpol offices in Europe and other parts of the world regarding the cost-effectiveness and usefulness of PT technology for police work. The investigation shows an almost unanimous view from the seven European respondents confirming that PT technology is a cost effective and an important means of investigation in their country. Figures for other parts of the world were somewhat lower, indicating that these answers are not given on "autopilot" but on the basis of differences in the relevant societies. Lower distribution of GSM, less use of GPS devices and RFID systems could for instance explain differences. Moreover, this part of our inquiry shows differences regarding assumed usefulness of the four groups of PT technologies we asked about (GSM, GPS, Wi-Fi/WLAN and RFID). An obvious implication is that this demonstrates different cost-benefit expectations to these technologies.

3.6 Overall classification of technology related to peoples' location

The analyses of this chapter have elucidated the fact that the technology comprised by RESPECT WP7, which we here have designated PT technologies, represents in fact one of several categories of technologies related to data on peoples' whereabouts. There are in particular two types of technological properties that should be highlighted: i) if the technology is wired (fixed) or wireless (mobile), and ii) if the technology is directed towards things or people:

	Directed towards	
	Things /artefacts	People
Wireless/mobile	techno metric GSM, Wi-Fi/WLAN, GPS, RFID etc.	biometric Fingerprint, facial, retinal and gait recognition etc.
Wired/fixed	techno metric Point of sale terminals, Automated Teller Machines etc.	biometric Fingerprint, facial, retinal and gait recognition etc.

Automatic number-plate readers are technometric and could either be wireless or wired. According to this classification, the technology especially highlighted in the project design of RESPECT WP7 is only one of four main categories of technologies which are directly relevant to questions of localization and tracking of people and related questions of efficiency of police work on the one hand and privacy and data protection on the other. In chapters 4 – 6 (below) we will maintain the initial defined boundaries of the project. In Part II of this report, containing privacy impact assessment and other legal political assessments; however, the main point will be personal location data and not the type of technology applied to capture such data.

4 Use of PT technology in civil society

4.1 Introduction

4.1.1 Approach

Task 7.1 of WP7 is to "Identify and classify RFID and geolocation devices already used or potentially deployable in crime detection, prevention and/or prosecution of crimes in participating member states and a number of non-member states where such systems are already deployed". Above, in chapter 3 we have examined the basic technologies which could be applied to locate and track individuals via objects they carry or in other ways are connected to. In this chapter, we will map and discuss the use of these technologies. Mapping implies a great challenge because the technology to be identified is not necessarily exposed and easy to detect.[38] More important is the fact that PT technology is "everywhere" and integrates parts of various services and devices. Thus, it is not fruitful to try to map these technologies completely. Furthermore, our subject of investigation is a moving target in the sense that technological development and development of use of existing technology is fast. The usefulness of snap-shooting current technology is thus limited. On this basis we have adjusted the mapping to what we believe is well-founded use of project resources.

Since every action and state of affairs has a place and a time, every use of electronic devices and electronically based services linked to actions and states creates a possibility to log and store location and time data. Because this type of information is very basic and of interest to both the providers and user of services it will, if available, be registered and stored for shorter or longer time. Storage of data showing place and time are increasingly possible, because PT technology is relatively cheap and easy to integrate in various devices. Thus, in the near future the relevant question will probably go beyond the referred research question in RESPECT WP7: To what extent will there be devices *without* geolocation functions? We believe the answer will be "hardly any", and find it to be a secure prediction to state that the great majority of devices and services will have the capability to generate data on time and place of actions etc. where an electronic device is in use. On this basis, we find it sufficient to make this statement probable by demonstrating how PT technologies are used within various and very different fields of society and for various purposes.

38 This does of course not imply that people are not aware of the technology that tools and services are based on.

Our assumption is, in other words, that we will be confronted with an ever increasing number of devices and services with PT technology as integral elements. A legal political discussion of if and how police should make use of such data should be supported and limited will probably not be very fruitful if every type of PT application is put into the same bag. Thus, the main challenges as we see it is the task of classifying this technology and their use, cf. the second element of the task description in WP7 ("map and classify"). In chapter 3 we have started this classification from a technological perspective, and in this chapter this classification will be developed further on basis of actual use and possible social effects (see in particular section 4.6).

4.1.2 Methodological considerations

Our mapping of PT technology is based on a combination of three methods. Firstly we have mapped knowledge in relevant national authorities.[39] In our inquiry, national telecommunication authorities were asked about their knowledge of relevant service providers. Moreover, these authorities and the national data protection authorities were asked about their knowledge regarding specific types of application of PT technologies. We knew beforehand that this will not give exhaustive answers, but we assumed it could be valuable in combination with other sources. Moreover, it is in itself interesting to have a picture of which types of PT technology applications these authorities know about.

The second method has been to detect use of PT technology through search in government documents and court decisions.[40] Results from documents studies have been available from six European countries.[41] However, the results of document studies have been very sparse; something which mirrors the fact that PT technology has not been a major issue in government and court cases.[42] Thirdly, a limited literature study has supplemented the first two methods.

It is important to emphasise that the technology we have tried to map is not limited to those developed and used for the purpose of locating and tracking people and objects. As indicated in chapter 3, location and tracking is not necessarily what the controllers and users of these technologies try to achieve. Often location and/or tracking are required in order to attain another (final) purpose. The only basic PT technology which has positioning as its main purpose is GPS, while GSM, Wi-Fi and WLAN first and foremost have various communication purposes (SMS, email, web services, social media etc.). RFID implies identification of objects, and may support a great number of purposes, including purposes

39 See section 4.2.

40 See section 4.3.

41 Austria, Bulgaria, Germany, the Netherlands, Norway and Slovenia.

42 Results have mainly been used as background information and will not be directly referred to.

connected to movements of these things. In addition to the direct purpose of locating and tracking, final purposes could be payment, providing insurance services, supporting effective control of employees etc.

In this chapter, it is obvious that the results we present give a limited picture of actual use of PT technology. Thus it should be stressed that data are mere examples which in our view are helpful as basis of legal political reasoning; it does however not tell the "full truth" about how PT technology is used in civil society.

Uncertainties exist of course even within the framework of questions posed in our inquiries. Use of vague wording, lack of context etc. may of course create the risk of respondents misunderstanding our questions. On points where we suspect misunderstandings appear in replies from respondents, we call attention to this fact.

Regarding sources and methodological questions of general nature (respondents, response rate etc.), we refer to section 2.2.

4.2 What is known by relevant authorities regarding providers of services based on PT technologies?

One of our initial assumptions was that use of PT technologies in the civil society by the police could make it desirable to have some sort of overview of services based on these technologies, i.e. who are the service providers? Due to telecom regulations we are aware of the fact that providers of services based on GSM are well identified, and we wanted to check to what extent similar knowledge existed regarding the three other types of PT technologies. Thus, one of the questions posed to the national telecom authorities was "To what extent does the national telecommunication authority know which companies established in the country that provides services based on the following technologies?" (PT technologies were indicated). Reply alternatives were "No knowledge", "Only uncertain estimates", "Rather certain estimates" and "Complete knowledge".43

Answers show that all eight telecom authorities claimed to have complete knowledge of providers of services based on GSM, three of nine authorities claimed to have full knowledge regarding Wi-Fi/WLAN, but only one regarding GPS and no one regarding RFID. Five of eight telecom authorities had no knowledge regarding RFID and three claimed to have only uncertain estimates. Five of the asked telecommunication authorities had no knowledge of RFID suppliers; four did not have knowledge of suppliers of GPS services, and two authorities had no knowledge of Wi-Fi/WLAN suppliers. The following ranking is according to

43 See telecom inquiry, question 1.

a simple assignment of values for each reply alternative, indicating the level of knowledge:[44]

Technology	Rank	Sum, value
GSM	1	34
Wi-Fi/WLAN	2	24
GPS	3	14
RFID	4	11

The table demonstrates a marked difference between knowledge regarding providers of services based on GSM and Wi-Fi/WLAN on the one hand and GPS and RFID on the other. This is hardly surprising, since telecom authorities tasks often do not cover GPS and RFID. On the other hand, telecom authorities are probably those in the best position to know anything about this issue. None of the national authorities refrained from answering this question.[45] The lack of overview regarding RFID and GPS is inter alia interesting because, according to other replies in this study, these technologies are used in a high number of services which involve location and tracking.

4.3 What are the purposes of services based on PT technology?

Both the data protection authorities and the telecom authorities were asked about their knowledge regarding type of service/purpose[46] based on the four basic PT technologies[47] in their country: **Are you aware of services in your country where the following types of technology are embedded?** Ten areas of application/purposes were listed with invitation to indicate services based on the four basic PT technologies. In order to capture additional types of services, respondents were also invited to add "others/comment", but in the replies no additional services were suggested. If we sum up all purposes in all countries for each type of PT technology,[48] use for marketing purposes is regarded as most common, while use on public events within sports, music etc. was least common. However most

44 With value 1 is assigned for "No knowledge" etc and value 4 for Complete knowledge.

45 The Norwegian authority stated that their knowledge relied to a large extent on whether or not a service is under the Norwegian Telecommunication Act, and that GPS and RFID normally would be outside the scope of this legislation. The Slovenian authority did not give reply regarding GPS and RFID.

46 Note, when we in this context use "purpose" as supplement to "service", the purpose does not necessarily corresponds to purpose pursuant to data protection legislation.

47 GSM, Wi-Fi/WLAN, GPS and RFID.

48 Information regarding the same purpose/technology from both the TCA and DPA of a country was only counted once.

purposes were familiar, i.e. they were known by at least one of the authorities that LP technology was in use in their country.[49]

The list presented to the respondents was limited, and more types of services/purposes could have been added. The fact that no respondent added other types of services based on PT technology, should not lead to the conclusion that the list gives a correct picture of the situation in the various countries. Even though a specific service/purpose is not known to one of the authorities asked, the use of PT technology to support a particular type of purpose could obviously still exist. Moreover, our results do not say anything about how frequent, neither how common use of PT technology for the listed purposes is within the area of each purpose. For instance, indication by a respondent of GSM use to locate/track children could refer to one or many examples in that country.

Purpose	**Score**
Marketing	15
Access control to rooms, buildings etc.	15
Tracking/localization of employees	14
Tracking/localization of children	14
Insurance services (of cars, vessels etc.)	14
Access control to information	10
Public transportation payment	10
Toll-road payment	08
Tracking/localization of students	07
Public events (music, sports, etc.)	06

Score marks the number of replies from the data protection and telecommunication authorities confirming that one of the four PT technologies is applied for each purpose.[50] It is worth noticing that several purposes where location and tracking is integrated and necessary to support the purpose, received high score (e.g. regarding employees and children). Tracking of employees is elaborated in section 4.5.2. Regarding several of the other purposes, location/tracking is more of a side effect (e.g. payment and access control to information).

For each of the purposes listed, the results from this question allows us also to say something about which PT technology is perceived as most and least important and to how many respondents.

49 In Italy and Germany, only telecom authorities responded to this question.

50 We have only counted one answer for each country; i.e. when both authorities of a country have confirmed use of e.g. RFID for marketing, this has been counted as one.

Purpose	PT most	PT least
Marketing	GSM (5)	GPS (2)
Tracking/localization of employees	GPS (5)	Wi-Fi (1)
Tracking/localization of children	GSM (5)	Wi-Fi (1)
Insurance services (of cars, vessels etc.)	GPS (5)	RFID (1)
Access control to rooms, buildings etc.	RFID (7)	Wi-Fi, GPS (1)
Access control to information	RFID (5)	GPS, GSM (1)
Public transportation payment	GSM (5)	Wi-Fi, GPS (0)
Toll-road payment	RFID (3)	Wi-Fi (0)
Public events (music, sports, etc.)	RFID (5)	GPS, GSM (0)

"PT most" indicates the PT technology which was indicated by most of the respondents. For instance "Marketing ... GSM (5)" indicates that GSM is in more frequent use than other PT technologies, and that five countries (of eight) apply this technology for that purpose. "GPS (2)" indicated that GPS is the least used PT technology for this purpose, and that respondents in only two countries confirmed use of GPS for marketing purposes.

The results indicate that for the listed purposes GPS and RFID seem to be the most important technologies. In other words, RFID of which five of eight telecom authorities had no knowledge and the remaining three only uncertain estimates is considered to be most important. Moreover, Wi-Fi seem to be least used. According to these results, highest use of Wi-Fi is within marketing and access to information.

Results regarding purposes related to marketing, toll-road payment and tracking/location of students are special in the sense that all/most types of PT technology seem to be in use and no technology seems to totally dominate. RFID seems to dominate regarding access control to rooms/buildings and is a strong number two regarding public transport payment. Where GPS or GSM is indicated as most used ("PT most"), the other of these two technologies seem to be a good number two. Thus, GPS and GSM dominate in the realisation of purposes regarding location/tracking of employees, children and cars, vessels etc. (cf. insurance services).

4.4 Dispersion of PT technology

The results to the question presented in section 4.3 were used to indicate something about possible differences in the distribution of such technologies in the countries represented in the inquiry and to indicate which PT technology is used in the highest number of services (cf. previous section). On this point, we have only incomplete results from four of the relevant authorities, and we have no basis for clear conclusions. However, if we count the number of different services based on PT technologies, it seems that the level of technology distribution in the countries

are on about the same level. The only country with a marked lower score than the others is Bulgaria.[51]

We have also used the replies to indicate something about which PT technology seems to be used in the highest number of different types of services.

Technology	Rank	Sum, value
RFID	1	30
GSM	2	28
GPS	3	22
Wi-Fi/WLAN	4	13

The answers indicate, based on the knowledge of the telecom and data protection authorities, that RFID is used in the highest number of different services, while Wi-Fi/WLAN seems to be far less applicable. It is also worth noticing that the applicability of three of four PT technologies is generally high.

4.5 Two examples of areas where PT technologies are applied

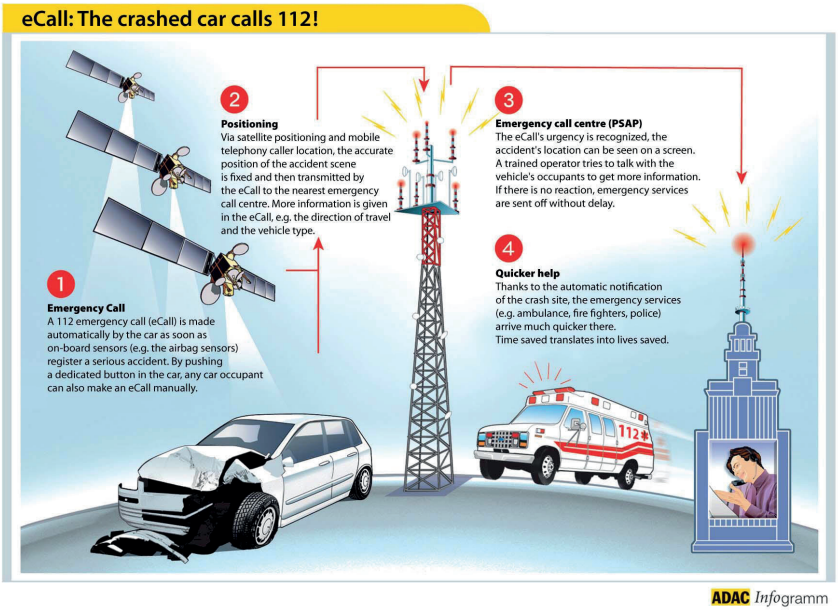
4.5.1 eCall

The pan-European initiative *eCall* is intended to bring rapid assistance to motorists involved in a collision anywhere in the EU and EEA territory. The illustration below is taken from the European Commission's [52] description of eCall and shows the intended use of the system.

The system uses a combination of two of the positioning technologies discussed in this report (GPS and GSM) to obtain personal location data, and GSM to communicate data to a central location.

51 Regarding Romania, we have no basis to conclude.

52 http://ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved



The eCall initiative mandates that all new vehicles are fitted with a tracking and communication device that will automatically dial the pan-European standard emergency number (112) in the event of a serious road accident or manual activation. When activated, the system will wirelessly transmit a "Minimum Set of Data" (MSD), which consists of:

1. Vehicle identification;
2. time of incident;
3. precise location including direction of driving, based upon both satellite positioning (GPS) and mobile telephony caller location (GSM);
4. eCall qualifier giving the severity of the incident (as a minimum, an indication if eCall has been manually or automatically triggered, but this qualifier may also contain details about airbag deployment and data from impact sensors);
5. information about a possible service provider.

The estimated cost per car for the device is about EURO 100.

As described by the European Commission (ibid.), the mandatory eCall system will be inactive when not explicitly activated (by a crash or manually), and that the system is "not traceable and when there is no emergency (its normal operational status) it is not subject to any constant tracking." However, the commission also expects that the eCall technology platform capabilities (i.e., positioning,

processing and wireless communication) to be used for other purposes, including "advanced insurances schemes, stolen vehicles tracking, eTolling". Most of these additional purposes will involve some form of continuous tracking of the vehicle.

As long as the sole application of eCall is to report automobile crashes and summon help, the technology is probably of little use for tracking purposes or for police work.

However, we have noticed that the tracking capabilities that exist as a *side-effect* of adoption of GSM (in all of the EU/EEA) and of Wi-Fi (in Denmark only) have led to the Data Retention Directive that requires the positioning data produced by these technologies to be retained for police purposes. This means that one cannot rule out a similar function creep in the case of eCall, where adoption of the system may lead to a legal requirement to collect and retain vehicle position data records in a register for police purposes.

4.5.2 Field technology

4.5.2.1 Introduction

One of the purposes of our inquiry referred to in section 4.3 (above) is "Tracking/localization of employees". Field technology is one very important group of technology for this purpose. Field technology may, for instance, make use of GPS-tracking, location-based applications, advanced geographical information systems and handheld devices (PDAs, smartphones, barcode- or RFID-scanners etc.). This technology is increasingly used by companies and organizations in the private and public sector. Field technologies, applications and devices facilitate real-time and remote monitoring or surveillance of the mobile work force, for instance truck, bus or taxi drivers, home care workers, electricians, salespeople, carpenters, plumbers, emergency or security personnel, etc. Managers can access data captured by the use of field technology over the Internet (these are hosted or cloud services – the data and software is stored on computers owned and operated by the product supplier or by sub-contractors around the world).

In addition, field technology products may communicate data stored in back-end systems to the mobile workers (for instance information about customers, service-level agreements or other contractual information, past service history or patient records). Also, the mobile worker may remotely enter crucial information into the back-end systems (like working hours, expenses, order parts required for service, etc.). By doing so, the suppliers of field technology products promise seamless integration between mobile systems or devices in the field and the informational resources held by back-end systems.

The main promise of field technology, however, is to make each member of the mobile work force visible from one central location (usually the head or

regional offices), so that their work-performance can be managed – evaluated, controlled and directed – remotely and in real-time. Surveillance and centralization, therefore, go hand-in-hand, and this is supposed to benefit the company or the organization, including the mobile workers themselves, in a number of ways: increased work-performance, higher profit margins, greater service quality and customer satisfaction, optimising travel routes, quicker response to service requests, enhance personnel security, reduce CO2-emissions, reduce the paper burden, and much more.

4.5.2.2 A Norwegian experience

Below we will briefly discuss the most significant experiences harvested by labour union representatives in 50 Norwegian private companies and public organizations concerning the use of field technologies.[53] These experiences show how field technologies, which should be regarded as subgroup of PT technologies, influence employees' autonomy and integrity.

A large variety of field technology applications and devices were in use by the 50 companies or organizations. Many of these applications and devices had only been used for three-four years or less (sometimes only for a couple of months). The two most commonly used field technology products were fleet management systems (location-control and GPS-tracking) and various handheld devices (PDAs, smartphones, etc.), often integrated with back-end systems (CRM, order management, accounting, parts management, etc.). Barcode- and RFID-scanners were also being used.

Field technology is largely introduced to promote efficient conduct of business. Control of employees could be one of several purposes, but control was not necessarily a predominant aim. Because control could be seen as an integrated element in many managerial tasks, it is on the other hand difficult to make a clear distinction between control and other effects and purposes. The more localization and tracking functions were integrated with back-end systems, the more difficult to regard the system as such a "surveillance system". When a manager for instance maps which company cars is closest to a location for a new assignment, he will obviously also inevitably notice if the car/employee is in a place where he should not be (in a car park, at the employees home address, etc.). Even if the intention is not control, it is therefore difficult to avoid that control could be an effect of such systems. To the extent that control was identified as purpose, a frequent argument was control needs of government agencies. An argument could be readiness in case of government control; fleet management systems could for

53 The discussions in this section are based on qualitative interviews with union representatives reported in Tranvik 2013. The interviews were conducted in 2011 and 2012.

instance produce evidence that company cars have not been used privately to a larger extent than what has been reported to tax authorities.

One important reason why fleet management systems (and similar location-control and GPS-tracking products) were viewed as particularly intrusive and problematic was that the systems were interpreted as "tools for managers", i.e. instruments for controlling workers by putting them on screens. This new way of managing the mobile work force often clashed with occupational cultures where values like individual autonomy and independence were held in high regard. Handheld devices, on the other hand, seemed, to a much greater extent than fleet management systems, to be viewed as "tools for workers" – hardware and software that assisted mobile workers in doing their jobs, but without real-time management intrusion that potentially threatened their autonomy and independence.

Another important reason why fleet management systems were seen as more intrusive than handheld devices, was frequent reports of what the union representatives described as "misuse of personal data". By misuse the union representatives meant function creep; the systems were used in new and not-agreed-upon ways. For instance, employers and employees had usually agreed (sometimes in writing) that data on work performance, for instance, routes travelled, engine not switched off during stops or locations visited during the day (including time of arrival and departure), could not be used by managers to discipline or punish the behaviour of mobile workers. Nevertheless, a majority of union representatives pointed to one or more instances where this had happened during the last 12-18 months. Employees had been called into meetings to account for their behaviour, particularly employees that were regarded as trouble-makers or did not enjoy the confidence of managers for other reasons. Some union representatives presented fleet management systems as union-busting devices – tools designed to scare union members into submission by collecting as much personal data on them as possible – but this was a view held by a minority of those interviewed. Similar examples of what was viewed as misuse of personal data were far fewer and further between when the conversation turned to handheld devices. Moreover, third parties, for instance important customers, were sometimes invited to log on to the fleet management systems. By doing so, they could keep track of trucks or lorries carrying the customers' goods. Generally, field technologies, also handheld devices, seemed to have facilitated greater third-party monitoring (and sometimes control) of the execution of mobile jobs.

In Norway the introduction and use of field technology in the work place is regulated by two pieces of legislation: The Working Environment Act and the Data Protection Act. The former regulates the process of implementation (provided that the field technology in question is regarded as control measures), while the latter regulates the subsequent processing of personal data. The union representatives seemed far more familiar with the relevant provisions of Working

Environment Act than with the provisions of the Data Protection Act. However, this does not imply that the 50 companies and organizations complied with the provisions of the Working Environment Act: most of them did not, or did so only to a limited extent. For instance, even if the Working Environment Act stipulates that the employer must discuss and plan the use of field technology (or control measures) with union representatives before implementation take place, this did not usually happen. More often than not the employees were told, often only a few days in advance, that the technology had been purchased. Then, they were instructed to use it as planned by the managers. Moreover, the subsequent processing of personal data was usually not regulated at all, at least not in accordance with the provisions of the Data Protection Act. A few companies and organizations had written agreements specifying a few rules concerning the processing of personal data. However, the agreements fell short of complying with the Data Protection Act, and the employees (and union representatives) could usually not monitor whether or not the managers honoured the rules of the agreements.

The majority of union representatives reported that privacy and data protection were the main concerns regarding the introduction and use of field technology: the feeling of being closely watched by managers. According to these representatives, diminished work-place privacy and data protection had other negative effects, for instance a transfer of power and influence from the mobile workers to the upper echelons of the company hierarchy. A number of union representatives also claimed that the introduction and use of field technology may have had other adverse effects, particularly on the working environment: greater levels of distrust between employers and employees; loss of autonomy and independence; more insecurity (fear of making mistakes) and more pressure to execute jobs or close service tickets quickly. However, it should be noted that some union representatives expressed little concern about these issues. Neither privacy or data protection nor the working environment had been adversely affected by the introduction of field technology, according to these voices. The representatives who expressed these views were mainly (but not only) found in occupations where handheld devices were the field technology of choice.

4.5.2.3 Reflections on basis of experiences with field technology

Privacy and data protection of employees is not a particular topic in RESPECT WP7, but the exemplification of how PT technology may be applied reminds us of some more general points regarding collection and use of personal location data by the police. Firstly, it is important to remember that vast differences may exist between free and mandatory use of PT technology. Use of field technology in work places is example of an application where the level of conflict regarding data and privacy protection may be high, regardless of police access and access by others

than the employer. Easy access to such data for the police may obviously increase the level of conflict, and the easier and more integrated links to the police are the higher probability of increased conflict level. Furthermore, such conflicts are to a large extent "locked" because employees' only way of escaping what they may see as privacy infringement is to quit the job. With high unemployment rates and many business areas moving towards the same technology, not much real choice is offered those employees wanting to avoid having their whereabouts mapped.

Access to personal location data by the police is obviously much more than a theoretical possibility: In cases of serious crimes (murder, rape etc.), police will routinely access recordings from CCTV systems and logs from mobile networks. In some cases they will even encourage people of affected areas to give DNA samples to the police in order to exclude them from the case. In other words, the need and hunger for information in cases of serious crimes is so big that it is probable that data from field technology will be accessed (for instance to map whereabouts of taxies, delivery trucks and others who may be involved or witness to the crime). In such situations, it is hardly true that those who have nothing to hide have nothing to fear: Even though you do not have something to hide, you may have something to explain; simply because you drove within the sphere of the scene of the crime. Altogether, access to personal location data by the employer and possibly by the police, may sum up to become a high level of conflict.

Use of many PT applications is highly optional and first and foremost connected to leisure and areas of life where most people probably will say they are in a rather free position. Use of GPS coordinates to upload images on social media, find a friend or as part of a training device are examples of applications to which there usually are not connected severe consequences for peoples welfare if they choose to stop using it in order to protect their privacy. In contrast, use of field technology directed towards employees may hardly be seen optional and for many people refusal of accepting these technologies may imply unemployment and loss of welfare. Most applications, however, are somewhere in-between these extremities: Most people are able to avoid certain payment methods, access control methods and marketing methods which involves generation of personal location data; however, only with a certain social and practical expense.

As technology where positioning functions are imbedded becomes more and more widespread in society, mentioned social expenses will increase and, at the end of the day, will make PT technology practically impossible to avoid. All in all, it may thus be claimed that regarding future widespread PT technology penetrating many actions in our daily lives, there will in many situations hardly be any real choice regarding use. It should at least be discussed if it is reasonable to establish legislation regarding access by the police of personal location data from civil society on the premise that people are able to avoid police access by refraining from using PT technologies. To the extent that no real liberty exists, this is

probably an argument for explicit legal regulation in order to clearly define access rights for the police, required routines etc. Probably, predictability should be regarded next best if real personal freedom is lacking.

4.6 Concluding observations and possible classification of technology

4.6.1 General

Our inquiries indicate that the four main categories of PT technology have been introduced in all countries and deployed for similar purposes in these countries. Bulgaria is the only country which seems to apply PT technology less than other countries.[54] A lot of services and purposes are based on RFID and GPS, technologies where national telecommunication authorities have no or only little knowledge of service providers. It may be that other authorities update lists of such service providers, but we cannot see that other civil authorities are in the position to carry out such mapping. Thus, we hold it as probable that it may be difficult for police authorities to know where PT technology is used in the civil sector, and for which purposes.

If this assumption is correct, RFID and GPS are in a very different situation than e.g. GSM, camera surveillance and toll road plants. For GSM, camera surveillance etc., requirements of permissions or notification lead to a large degree of overview in terms of where such technologies are installed and who is operating them. Certainly, when crimes are investigated on a specific crime scene, it will not be difficult for the police to do a concrete mapping of many RFID and GPS based systems adjacent to the places in question. However, if there is no concrete scene of crime, relevant uses of these technologies are probably relatively hard to identify.

4.6.2 Possible regulatory considerations

Our survey in combination with the referred recent research on field technology with location and tracking functions, may give basis for some regulatory considerations, first and foremost regarding possible fruitful classification of PT technologies in addition to the classifications made in chapter 2. Key words for the sets of classes we suggest to introduce are:

- Voluntariness and competence

54 At least compared to Slovenia, Slovakia and Norway from which we have replies from both authorities; but probably also compared to Germany and Italy for which we have replies from one of the authorities.

- Number and types of involved parties
- Purpose, potential and effect
- Type of power
- Transparency and accessibility

Voluntariness and competence

If we regard the extent of voluntariness and autonomy, the first and rather unproblematic category is that of individuals who are competent and actually free as to whether or not to use PT technology. Use of various GPS based apps on smartphones for purposes of entertainment is one example.

However, the investigation reminds us that PT-technology is not only used voluntary as a result of making use of various services. Employees in many branches are examples of groups where PT technology is mandatory; if not formally at least in a practical sense, because in the labour market of many economies, refusing such surveillance would imply that you would be excluded from jobs. This situation forms the background for the assumption that employees will often not be in the position to freely give their consent to process personal data about them. Working life is one of the areas of society where mandatory use of PT technology is most widespread and common. Other particularly exposed groups are children/youth and senile, i.e. people with limited rights of self-determination and often with a dependency to other people which reduce the value of any formal right to autonomy that they may have. We do not know how far the development has come regarding these other groups, if the potentials may be similar to what has been revealed in working life, and how fast such a development eventually will be. There are, however, particular reasons to follow the development for these groups because i) they lack self-determination and ii) location and tracking (thus) is formally or in practical terms mandatory.

By voluntariness we mean here that the use of PT technology is voluntary or not for the person (data subject) who has his location and movements registered. The first, simple and ideal category consists of people having competence to exercise autonomy and who are in a free situation to make independent choices.

As can be seen from the list of purposes/services in section 4.3 several of them are not mandatory in a formal sense, for instance you are not obliged to travel on a road with payment based on RFID, and you are not forced to travel abroad and thereby to use passport with RFID. However, the social effects of not travelling on that road or going to another country may easily make you experience that these actions are unavoidable. Similar situations occur for chauffeurs who are faced with the choice of accepting tracking of movements or not having a job and income. These people are formally competent to exercise autonomy, but social structures create social and economic costs that make choices very costly. We

may think of people in this second category as competent to exercise autonomy but not free to use it.

The third situation is where people are formally competent to exercise autonomy however not in a situation to exercise it, even though they are free to decide. This is the case for senile people who have not been placed under legal guardianship, plus certain other groups of hospitalized people who temporary are incapable of exercising their autonomy.

A fourth group does not have competence to exercise autonomy (and therefore no freedom to decide in this respect). They must, in other words, accept choices made by others regarding the use of PT technology. People under legal guardianship is one example, another is people in custody; for instance RFID used as part of home detention curfew arrangements.[55] Children under the age of 18 partly belong to this fourth group, dependent on age and maturity.

Competent and actually free	Competent but not actually free	Formally but not actually competent	Not competent and not free

Distinctions between the categories may of course create doubts, and "actually free" may in particular be source of discussion. From the viewpoint of privacy, the first category is rather unproblematic, while the other three categories comprise special and vulnerable groups which require special considerations.

Number and types of involved parties

It is quite possible that information on localization and tracking is result of personal actions where no one but the person in question is involved. This is for instance the case when a person uses GPS services, for instance by using devices in a car or handheld units in order to find the way, measure geographical distances etc. This is the simplest way of organising processing of data resulting in localization, and the user is in full control.

A more usual constellation of involved parties with PT technologies consists of two parties; the user (data subject) whose personal location data will be established and stored, and one service provider (controller). If so, we have a simple and classical relationship between one data subject and one or more controllers, as established in the Data Protection Directive. Use of RFID to get access to a hotel room could be example.

Several actors are quite often needed to produce a service where personal location data is involved. Several service providers are for instance needed, because

55 See for instance government information about the UK Home Detention Curfew (HDC) scheme (http://www.justice.gov.uk/offenders/before-after-release/home-detention-curfew).

the service is composed by resources from several data sources and because telecom services are needed to transmit signals between the user and the service providers. My GPS coordinates are for example transmitted to a data base with relevant geographical information, and this service collects more data from other providers (of pictures, weather forecast etc). The GPS position of the user will then be available to several service providers, and the number and business model could make such constellations quite complex. In terms of data protection legislation, there will in these cases be several controllers of personal location data.

On the supply side of the relationship between user and service provider(s), there will often also be engaged parties (data processor) who perform tasks pursuant to contract with controllers. This side of the relationship could in other words both have many controllers and these controllers may make use of data processors.

If we try to classify PT technology as a constellation of involved parties, one possibility is the following:

Data subject (user) alone	Data subject related to one controller (service provider)	Data subject related to one controller and subcontractors (data processors)	Data subject related to several controllers and subcontractors

This classification could of course have been made more detailed, but the numerous possibilities of combining these three main actors imply that clear simplification is in any case needed. One main point in the suggested classification is that, irrespective of these parties fit into definitions of controller or processor, multi-party constellations easily become complex for data subjects to deal with. Thus, various complex PT services offered today should probably be placed in the fourth category (to the right).

Purpose, potential and effect

Of course, sometimes PT technology is applied to locate and track peoples whereabouts; for instance to keep control over children and senile. However, as illustrated in section 4.3, such technology are probably even more important to produce various services to which localization is relevant but not always very important. RFID as part of payment and access control systems will for instance generate data about location, but the purpose is to receive payment, stop unauthorized people from entering into rooms and buildings etc. Thus, in our view, it is not sufficient to claim that the purposes of such use are positioning, but we suggest that potentials of location and actual effects are considered in addition.

Purpose refers to a declaration of what the controller would like to attain by processing a certain set of personal data. If the data set is comprehensive and/or

not particularly related to special aspects, it may thus not be expected that purpose specification will contain anything which clearly relates to localization and tracking of people. A payment system based on RFID will for instance have the purpose of carrying out payment for service x and collection of amount outstanding. The fact that information of location is important as part of documentation of payments made will in such cases hardly be visible to the data subject.

It could of course be possible to require that localization, under certain conditions, shows in the formulation of purpose, but this is probably not very practical and efficient. It is on the other hand easy to assess and state whether or not processing of data has the *potential* of establishing location and movements of people. Such a potential only describes a technological possibility, it does not say anything about the controller's purpose or the actual effect of the processing. On basis of the list of applications in section 4.3, we can conclude that only a few of them will have localization of people or objects as purpose,[56] but all applications have establishment of location and movements as potential.

Here, we anticipate that purposes and potentials are assessed prior to processing, and they should thus be seen as predictions rather than established facts. Purposes, and especially potentials, are not necessarily attained. Even if the controller state that he will pursue the purpose of tracking employees, it is not certain that this actually will happen, and technological potentials will obviously not be exploited. Thus in addition to prior establishment of purpose and potentials, a retrospective perspective is important. *Effect* could indicate actual consequences regarding localization etc. Here, effect would describe whether or not localization and tracking in fact has been carried out, i.e. described independently from declared purposes and potentials. Again, we suggest the following categorisation regarding this aspect of the processing:

Localization is a not a purpose or an effect	Localization is a purpose	Localization is a potential	Localization is an effect

In the table, we have also introduced a category where localization is a not a purpose or an effect. This indicates that there are no intentions or practises which show that the potentials of PT technology are used.[57] In a regulatory perspective it should be discussed whether or not the purpose specification principle is adequate in relation to PT technology, and if potentials and actual effects should be supplementing criteria.

56 Or, more precisely, it should be expected that these types of systems will be notified as having a purpose related to the whereabouts of people and objects.

57 Regarding PT technologies, potentials to locate may of course never be excluded.

Accessibility and transparency

Transparency is important to every aspect of privacy and legal protection, and evidently also regarding assessment of PT technologies. Many aspects could be addressed, for instance regarding contents and language. Here, we have chosen to highlight questions of accessibility, namely the extent to which users/data subjects need to invest time and background knowledge in order to attain the information about localization (and questions of if, why, how, when, consequences etc.). We presuppose that controllers are dispatchers of the information and that there are no economic costs for users.

We take it that best accessibility is achieved if information is given directly to users, for instance by means of SMS and email with link to a "My page" service, social media etc. Second best accessibility to information is probably created if made accessible on general web-pages, "My page" or social media (but without any notification for each change of information contents). Third best would be that users have a right to ask controllers to access the information, and the worst alternative will obviously be that access rights are disputed or non-existing.

Direct and active information to the user	Information is made available without request to the user	The user has a right to claim access right	Access rights are disputed or non-existent

***

The explained regulatory considerations in this section will be applied and further developed in Part II; in particularly in chapter 3 as part of a proposal for an individual rights impact assessment model.

5 Police use of PT technology

5.1 Introduction

Police may first and foremost use PT technology and personal data from the use of such technology within two spheres. Firstly, they may collect data from PT technology in the civil sector and secondly the police may collect personal location data directly by using their own PT technology. Below, we will highlight the first mentioned sphere.

This chapter contains first and foremost results from the three questionnaires performed by the national research teams, cf. the explanation and discussion of methods in section 2.2.2. Results are presented so that answers to related questions are referred in context, regardless of which part of questionnaires mentioned that was used as source.[58]

Others of the results presented below have the Interpol inquiry as source (cf. section 2.2.3). This part consists of 12 European countries and 25 countries from other parts of the world. We do not know which police office and country respondents represent.[59] The only thing we know is the region of the globe of each respondent.[60] Anonymity in the Interpol part of our inquiry represents a strong limitation and makes it impossible to match these results with the national European studies. Replies from European police offices, however, will be given special attention.

5.2 Legal regulation of deployment of PT technologies by the police

We have not mapped relevant substantive law of the 37 countries taking part in our inquiry. The aim was instead, on an overall level, to collect information of the methods of legal regulation and to obtain assessments of current legislation and opinions of needs for amendment.

58 The sequence of reported results may differ from the sequence in which questions were presented to the respondents in questionnaires.

59 See section 2.3.3.

60 We received answers from twelve Interpol offices in European countries and 25 offices from other regions of the world. Four replies came from Interpol offices in Central America and Caribbean, 2 from South America, 2 from North America, 3 from Asia, 2 from West Africa, 6 from East Africa and 6 from the Middle East and North Africa.

Firstly, we asked national Interpol offices "**What is the main Act or instrument on which the deployment and use of the following PT technologies is based?"**[61] Our reply alternatives were general law, specific regulation for a certain type of PT technology, guidelines, standard operating routines and "other" which we asked respondents to specify. No "other" way of regulation was suggested.

One of the twelve responses from European countries did not answer this question. Corresponding figure for counties outside Europe reply was eight.[62] The majority of these answers came from countries in Central America (3 of 3) and Middle East and North Africa (4 of 6). We cannot conclude that missing reply to this question implies that there is no relevant regulation in these countries, but because these technologies represent a rather new phenomenon, this is a probable assumption to make, cf. below.

In most European countries *general law* is main type of regulation of PT technologies. Deployment and use of GSM and GPS has general law as main type of regulation in 9 of 12 countries. In countries outside Europe, this figure is lower and only constitutes less than half.[63] WI-FI/WLAN has general law as main regulation in half of the European countries (6/12) and 8 of 25 countries outside Europe. Similarly, replies indicate that RFID has general law as main regulation in half of the European countries, while in other parts of the world RFID is only covered by general law in 4 of 25 countries.

Only a small minority of investigated European countries have *specific regulation* of PT technology as main type of regulation. Four European countries have specific regulation regarding GSM as main type of regulation, and corresponding figures for other technologies are similarly low. Figures for countries outside Europe are also on a very low level.

In our question we asked about *the main* Act or instrument on which use of PT technologies are based. In other words, we only asked for one alternative. Several countries indicated different types of regulation, something which creates problems for our interpretation of the answers.[64] These supplementary answers show however that several countries both regulate PT technologies in general law and specific regulations. Some even regulate on more than two levels.[65] However, we are unable to quantify this any further.

---

61 The PT technologies stated were GPS, GSM, RFID and WI-FI/WLAN.

62 Questionnaires from three of these countries were so incompletely filled in that it is uncertain if lack of information on this point could be understood as absence of regulation.

63 Respectively 13 (GSM) and 10 (GPS) of 25 countries.

64 Both general law and specific regulation may be regarded as "main" type of regulation. General law will often be lex superior and specific regulation may be lex specialis or at least contain so many specific rules that it is regarded as "main".

65 For instance, one European country regulate GSM and GPS on all four levels (general law, specific regulation, guidelines and standard operating procedures).

One European country answered that guidelines was main type of regulation for GPS. For other types of PT technologies, only general law and specific regulation was main type of regulation.

Answers regarding countries outside Europe show that, in a small number of countries, guidelines and standard operating procedures are main type of regulation.[66]

The overall picture is that deployment and use of GSM and GPS is better covered by legal instruments than WI-FI/WLAN and RFID.

Answers to this question only give a rough impression of state of affairs and we should therefore be careful regarding conclusions. Notwithstanding, the results indicate that general law is main type of regulation in a marked majority of countries. Probably, this implies that there is a lack of specific and concrete rules for police, courts and citizens to observe and follow. Thus, an important discussion is whether, and to what extent, it is necessary to pass specific regulations and/or guidelines in order to have a sufficiently clear legal basis for police deployment of PT technology. This is however not to say that more specific regulation should be directed towards the technology itself; cf. the discussion in Part II.

Four of twelve European respondents were positive to the statement

- PT technologies are not regulated in my country, but there is a need for a clear legal basis for the use of PT technologies.

The condition in the question that such technologies were not regulated seems to be ignored by some respondents, as three of them also answer that PT technology is either under general law or subject to regulation in guidelines and standards operating procedures. It is reasonable to interpret this collocation of replies as indication that regulations on lower levels than general law and specific regulation may be regarded insufficient.

Interpol offices in the same countries that answered positive to the previous statement gave negative responses to the statement that:

- From an operational point of view, legislation provides a clear framework for the use of PT technologies.

In three of twelve European countries, dissatisfaction of the current regulatory situation is in other words expressed, both with regard to need for clear legal basis and operational considerations. A fourth country with no relevant legal regulation may be added to this group.

We also wanted to highlight needs of amending existing legislation in order to make police work more effective:

66 GSM: 1/25, GPS: 3/25, WI-FI/WLAN: 1/25 and RFID: 3/25.

- There is a need to amend legislation in my country in order to ensure an effective use of the potentials of PT technologies.

Seven of twelve respondents were positive to this statement, of these two partly positive. This group consisted of those Interpol offices which generally indicated needs for amendment and the office indicating lack of legal regulation, implying that three additional Interpol offices gave positive feedback to this statement about needs for amendment.

We also asked Interpol offices to respond to a statement regarding need for clearer limits for use of PT technologies:

- Need exist to amend legislation in order to define clearer limits for the use of PT technologies by the police.

Four of twelve offices replied positively to this statement.[67] All of these were also positive to amendments to make technology use more effective. We understand this as an expression of a group of European Interpol offices with generally positive view on regulation of PT technology by means of legislation. This group only constitutes one third of the offices in our query.

Instructions and guidelines may give opportunities to adjust to operational needs of the police, and may thus be expected to be regarded by the police as the "right level" of regulation. We stated:

- There is a need to establish instructions/guidelines for the police in my country regarding PT technologies.

The number of positive responses to this statement were on the same level as the previous (five of twelve), and those positive to this statements were the same offices that were positive to the previous statements regarding amendment.

On an overall level more than half of our European police respondents were satisfied with the current legal regulation of PT technologies. Results indicate that among the twelve European Interpol offices in the query, there is a rather small group of "reform-friendly" offices. Willingness to amend current regulations increases if more efficient use of PT technologies by the police is the aim of reform.

As for other countries, the picture is different from European replies.[68] Twelve of 19 replies indicated that legislation in their country provides a clear framework for the use of PT technologies. However, a majority was positive to amend legislation to make more effective use of PT technology (12 positive, 7 negative[69]), and the same number of offices supported the statement of needs to amend legislation in order to define clearer limits for the use of PT technologies by the police.

67 One of these, partly positive.

68 The number of respondents who gave answers to relevant questions varied between 18 and 22.

69 Two had no experience regarding this question.

Interpol offices in countries outside Europe gave in other words much stronger support to statements regarding needs for regulatory reform than the European offices. Eleven of twelve offices outside Europe which supported amendments both supported legislation to make effective use of technology and to define clearer limits.

It is noteworthy that two of the countries reporting that they have comprehensive regulation of these technologies, gave replies indicating clear need of regulatory reform. The most likely explanation is that regulations exists but are seen as inadequate.

To sum up, within our selection of Interpol offices support for regulatory reform seems to be much stronger among offices in countries outside Europe compared to European offices. We do not have basis to explain this difference. One possibility is better developed legislation in European countries; another possibility is lesser support to the use of legislation in Europe than in other parts of the world. Offices in both geographical groups which support amendments seem to be in favour of legislation which prepares the ground for use of PT technology and to define limits to this technology, in an approximately equal degree.

5.3 Usefulness and cost-effectiveness of PT technologies

Five statements in our Interpol inquiry concerned use of PT technology by the police.[70] All European respondents replied that this technology is an important means of investigation in their country.[71] Responses from countries outside Europe were less unanimous; ten gave positive and six partly positive responses, while one was partly negative and three had no relevant experience.

Almost all European respondents agreed to the statement that PT technology is an effective tool for investigations of serious crime with unknown perpetrator (10/12), and for fighting terror and safeguarding national security (11/12). Corresponding figures for the group of other countries were 17/21 (regarding both statements).[72]

European respondents were in total agreement (12/12) of the cost-effectiveness of PT technology:

- PT technology is a cost-effective means of investigation.

70 Question 3, statements 1 - 5

71 Ten of eleven were positive to the statement "In my country PT technology is an important means of investigation", one was partly positive.

72 Two gave partly negative response to the statement regarding unknown perpetrators, and respectively one and two did not have experience regarding the issue in the two statements.

Respondents from non-European countries were also positive (11/21) or partly positive (4/21) to the statement expressing cost-effectiveness of PT technology. However, in this group answers deviated from the European countries in that 2 of 21 stated that they had no experience regarding the issue, 1 of 21 was negative and 2 of 21 were partly negative to the statement.[73] One probable explanation of these differences is lower dispersion of required infrastructures and use of PT technologies in some countries outside Europe.

Two of the statements in our police inquiry dealt with PT technology as evidence. We wanted to know how data from GSM, GPS, WI-FI/WLAN and RFID are used by the police, and asked respondents to consider the statements:

- Data from PT-technology is often submitted as evidence in criminal cases and
- Data from PT technology is often used as part of criminal investigations without being submitted as evidence.

The premise behind these referred statements is that data from PT technology could both be useful as part of circumstantiation directly before the court and as fact-finder used to collect *other* types of evidence which could be used in court. Replies seem to confirm this picture.

Only four of twelve replies concerning European countries expressed full agreement with the first referred statement (direct use of data as evidence), six replies were partly positive, while two replies were negative. Replies from countries in other parts of the world were similar, although slightly more towards the "fully positive" side (partly positive: 7/20, positive 8/20).[74] We interpret these answers as a confirmation that data from PT technology is not only valuable to the police because it may be used as evidence in criminal cases directly before the court, and that it is not unusual that such traces are treated as investigation materials only, without being subject to circumstantiation. Again, this may indicate that the question of openness should be addressed. Collection and processing of personal location data by the police which do not result in submission as evidence, easily implies that such data processing remains unknown to data subjects.

The above referred result corresponds with replies to the referred second statement (data used as part of criminal investigations without being submitted as evidence). Approximately half of the European respondents were positive to this statement and the other half partly positive. Only one answered negatively.[75] In the group of non-European respondents the answers to this statement were more

73 Four respondents did not consider this question.

74 Two of the replies in this group were negative, one was partly negative and three had no experience.

75 This probably should mean that this respondent only used such evidence directly before the court.

varied. Four had no relevant experience, six were more or less negative,[76] six were partly positive and only three were (fully) positive.

All together, on the basis of our data, it may seem that it is less usual in countries outside Europe to use data from PT technology without using it as evidence directly before the courts.

5.4 Police's assessment of the importance of different PT technologies

We asked the Interpol offices to assess the usefulness of PT technology at present and in the future. Responses were given in relation to each group of technology (GPS, GSM, RFID and WI-FI/WLAN).

In one question we asked which technology they would assess as having the most significance in the context of police investigation *today*? Answers were given by assigning values from 1 to 10 for each technology with 1 as best value.[77] The results clearly show a marked difference in the assessment by European respondents of GSM and GPS in contrast to RFID and WI-FI/WLAN. GPS was ranked almost as high as GSM by the European respondents. Respondents were in agreement regarding the importance of GSM,[78] while differences were more marked regarding GPS.[79]

Countries outside Europe assessed the technology in a similar way, with GSM receiving the best ranking and with GPS and WI-FI/WLAN ranked on approximately on the same level but lower than GSM.

Replies show rather marked differences between the four technologies which were highlighted in our inquiry – both with regard to current state of affairs and assumptions about the future (see below).

European responses indicate that police finds RFID and WI-FI/WLAN much less useful than GSM and GPS. Answers here were both marked by ranking of RFID and WI-FI/WLAN on approximately half the level of GSM and GPS. Moreover, there was a larger degree of variation in the assessment of Wi-Fi/WLAN and RFID compared to GSM and GPS. For instance, two respondent s gave RFID good/average ranking,[80] while three other gave very low ranking.[81]

76 Negative (3/21) and partly negative (3/21).

77 Some replies were given in ways which made them hard to interpret. Some did not reply to all alternatives, one marked "x" instead of indicating a value, and one seem to have misunderstood allowed values e.g. by indicating "0" (outside the valid scale). However, even with these irregular responses answers to the questions formed a quite clear general picture.

78 Receiving total score of 12, including six ranks = 1 (best).

79 Receiving total score of 18, including three ranks = 1 (best).

80 Value 3 and 5.

81 Values 8 and 9 (10 indicates lowest significance).

WI-FI/WLAN received marked lower ranking than GSM and GPS, but somewhat better than RFID. Assessed significance for police investigation of WI-FI/WLAN differed less than what was the case for RFID.

For illustration, the ranked list could be illustrated as follows:

European responses	**Other responses**
1 GSM	1 GSM
2 GPS	
	2 GPS,
3 WI-FI/WLAN	2 WI-FI/WLAN
4 RFID	4 RFID

In the table, marked difference of assessed significance for police investigation is illustrated by blank cells between the ranked technologies. It seems in other words that assessment of GSM and RFID in the two geographical groups of respondents are in line with each other, while GPS is assessed differently by the two groups of countries.

All respondents from Europe[82] and almost all of the respondents from other countries[83] fully agreed to the general statement that:

- There are reasons to believe that PT technology will be a more important means of police investigation in the next five years.

We also asked a more detailed question about the significance of PT technology for police investigation in future, and which of the four technologies the respondents would assess as having the most significance *in the next five years*. Answers to this question about future significance yield a similar picture to the present situation. In the table below, arrow up indicates increased expectations, arrow down indicates reduced expectations, while a dash indicates unchanged assessment. European respondents expressed even stronger belief in GSM and GPS, while respondents from other countries assess an almost unchanged significance for these technologies. A slight improved expectation to RFID could be registered in both geographical groups. WI-FI/WLAN was expected to have unchanged significance by European respondents. Countries outside Europe assess an improved significance for WI-FI/WLAN.

82 Except one that did not answer.

83 Except one which gave negative response and one which did not have relevant experience.

European responses	Other responses
1 GSM ↑	1 GSM –
2 GPS ↑	
	2 GPS –
3 WI-FI/WLAN –	2 WI-FI/WLAN ↑
4 RFID ↑	4 RFID ↑

Firstly, it should be noted that differences between the two groups of national Interpol offices regarding assessment of GPS seem to increase, with increasing European expectations and unchanged expectations in other countries.

It is also worth noticing that European replies regarding RFID may indicate a higher degree of uncertainty than for other technologies. The degree of disagreement between the respondents is somewhat higher than regarding other technologies. Moreover, compared to other technologies more respondents have refrained from answering questions concerning RFID.[84] It might be that police have less experience and less knowledge of RFID than other technologies like e.g. GSM and GPS.

The most surprising result is probably the comparably low future expectations to RFID technology regarding positioning and tracking of objects and (thereby) people. We would have expected that RFID and the related internet of things would be seen as something having great significance for police investigation – at least in the future.

5.5 ISPs experiences with police use of personal location data

Internet service providers (ISPs) are important potential sources of personal location data for the police. In order to get an impression about the relationship between these businesses and the police, we have carried out a simple inquiry among eighteen ISPs in the eight countries participating in the European part of RESPECT WP7 which was conducted by the national research teams.[85] Our aim has been both to capture national characteristics and differences as well as possible differences within countries represented with more than one ISP. Thus several

84 Three of twelve respondents, compared to one of twelve respondents regarding the other technologies.

85 ISPs in Austria, Bulgaria, Germany, Italy, Norway, Romania, Slovakia and Slovenia.

countries in our selection are represented by more than one ISP.[86] The inquiry was based on statements with reply alternatives yes, no and don't know.

First we wanted to have a picture of changes regarding police use of personal location data stored by ISPs:

- The police often ask for access to traffic data which may reveal individual's location.

The majority of ISPs answered yes to this statement (11/18), six replied no and one did not know. One interesting result was that ISPs from the same country responded differently to this statement. One of two Austrian, two of six Bulgarian, two of three Italian and three of four Slovenian ISPs answered yes. It is hard to explain these internal differences. One possibility is however that ISPs which answered no have a smaller volume of data and thus have a lower probability to be contacted by the police. Romania was the only country with no yes result.[87]

The next statement concerned movements (and not location as in the previous statement):

- The police often ask for access to traffic data which may reveal individuals' movements.

Eight ISPs gave affirmative answer to this statement and a majority of ten respondents replied no. Even here, answers from ISPs of the same country differed similar to answers regarding location. Romania was the only country with no yes result.[88] Answers regarding location and movements gave in other words more or less the same results.

We also wanted to have a picture of possible development regarding police access to personal location data:

- It happens more frequent today than two years ago that the police request access to traffic data which may reveal locations and movements of objects (and thus individuals).

Twelve of eighteen of the ISPs gave positive reply to this statement, while six answered no. Again, there were differences between ISPs of the same country, but every country had at least one ISP giving affirmative reply to this statement.

We wanted to know whether or not ISPs made independent judgements of police requests for access to traffic data:

86 Replies have been received from two ISPs in Austria, six in Bulgaria, three in Italy and three in Slovenia. We have tried to have answers from more than one ISP in all seven countries, but did not always succeed.

87 Romania was only represented by one ISP.

88 Romania was only represented by one ISP.

- Our company does not always act in accordance with police requests for access to traffic data that may reveal the location and movements of objects (and thus individuals).

Five of eighteen ISPs representing three of seven countries responded affirmatively to this statement, ten ISPs disagreed and three did not know. Here, the threshold for a positive reply was set very low ("not always"). Thus, it is natural to assume that negative replies either mean that no one of the requests from the police have contained legal flaws or serious uncertainties, or that the legal validity of such requests are not checked by the ISPs before they comply with police orders. We read this result as an indication of lack of independent judgement by the ISPs of police requests for traffic data.

We assume that a competent and well manned police force will do analyses of collected traffic data themselves. Nonetheless, considerations of time and costs may make it practical for the police to ask the ISP to carry out analyses. We asked the ISPs to consider the statement:

- Our employees often perform analyses of traffic data on behalf of the police.

Three ISPs (two Bulgarian and one Austrian) gave affirmative responses to this statement. Eleven gave negative responses, two did not know and two did not respond on this statement. We do not know the concrete background for the positive replies, but one general issue of discussion is of course the degree of independence or integration between police and ISPs. Seen on the background of the previous referred statement regarding compliance with police request, it may be claimed to be problematic if ISPs always act in accordance with police requests and often perform analyses on behalf of the police. Two of the Bulgarian ISPs seem to come in this category.

Discussions of the Data Retention Directive illustrate how traffic data are regarded highly sensitive by many people. Thus confidentiality obligations of the ISPs (pursuant to law or contract) should be seen as a possible problem for the ISPs when police request traffic data in order to locate and trace objects and people. With this general background in mind, it is hardly surprising that no one of the responding ISPs disagreed to the statement:

- It rarely creates problems with our confidentiality obligation if the police requests access to traffic data from our company.

Fourteen ISPs gave affirmative responses, three did not know and one did not give a response to this statement. We should, for the sake of good order, emphasi-

se that there is no basis for interpreting don't-know answers as a sort of disguised confession that such problems occur.[89]

To sum up this brief ISP inquiry, it is important to remember that results first and foremost say something about the situation in each country (Bulgaria, Germany, Italy, Norway, Romania, Slovakia and Slovenia), and that generalizations on this basis may create uncertain results. This being said, we believe that some general conclusions may cautiously be made as starting point for further examination and discussions:

- Police use of traffic data which may reveal peoples' location and movements stored by ISPs is probably increasing, and probably creates increased pressure on the ISPs as source for the police.
- There are reasons to further address the relationship between ISPs and police in order to map and discuss their relationship and independence.

Our inquiry comprised only internet service providers. Various other businesses provide services based on PT technology. It is probable that questions of pressure from the police and the issue of independence could be more challenging in these other businesses than for the ISPs.[90]

5.6 Telecommunication authorities' and data protection authorities' assumptions regarding police deployment of PT technologies

All national telecommunication authorities and data protection authorities in the selected European countries[91] were asked about their knowledge regarding police use of PT technology. Our aim was not primarily to say something about actual use of these technologies by the police, but to check the basis for possible involvement by these authorities. Most significant is probably the knowledge of data protection authorities, because most of these authorities control police use of PT technology. We asked:

- Are you aware if the police in your country apply means of investigation where the following technologies are included as an important element?92

89 The most probable cause for don't-know answers here (and to other statements), is that the persons giving response to our questionnaire did not have responsibilities which comprised the problem area in question.

90 We will return to this question in Deliverable 3.

91 Authorities in Austria, Bulgaria, Germany, Italy, Norway, Romania, Slovakia and Slovenia.

92 Reply alternatives were: no knowledge, assume it is in use, and know that the technology is in use. We listed the technologies: GSM, GPS, Wi-Fi/WLAN and RFID.

The inquiry gives clear indications that data protection authorities typically have more and more secure knowledge than the telecommunication authorities. The majority of answers from telecommunication authorities were either "No knowledge" or "Assume it is in use". The exception is knowledge about GSM where three knew it was in use and three assumed it was in use.

Generally, the knowledge of the data protection authorities was highest regarding GSM. Six of seven knew that this technology was in use.[93] Regarding GPS, four of seven knew that this technology was in use. Data protection authorities in the remaining countries assumed these technologies were in use.[94]

Two of six data protection authorities replied that they knew Wi-Fi/WLAN was in use by the police, while four assumed it was in use. Only one of six data protection authorities that answered this question knew that RFID was used by the police;[95] three assumed it was in use, while two had no knowledge.

Unless data protection authorities have concrete knowledge of police deployment of PT technologies, it is not probable that they carry out control or enter into constructive dialogue with the police regarding such use. This may indicate that for the great majority of data protection authorities of these countries, police deployment of RFID and Wi-Fi/WLAN has not been an independent issue of discussion. At least, compared to GSM and GPS the knowledge basis of the data protection authorities seems to be relatively weaker regarding Wi-Fi/WLAN and RFID compared to the two other technologies.

5.7 Use of PT technologies by criminals

Our questionnaire in the Interpol inquiry contained statements regarding possible use of PT technologies by criminals. The rationale for including this issue is the fact that GPS, GSM, Wi-Fi/WLAN and RFID is available to everyone and therefore constitutes a possible tool for everyone, including people with intentions of committing serious crime and avoiding criminal prosecution. As with many other open technologies, it may be that it both improves police's ability to investigate crimes *and* the criminals' ability to carry out crimes. One obvious criminal use may be to track people to reassure that they are away from scenes of a planned crimes, for instance in the case of burglaries. Tracking of police vehicles by means of GPS is another possible use by criminals, for instance as part of monitoring and counteracting police investigation.

93 The Bulgarian authority assumed GPS was in use.

94 No answer was received from the Romanian data protection authorities.

95 The Norwegian authority had such knowledge. The only telecommunication authority which answered that they had such knowledge was the Italian.

In the questionnaire we did not exemplify possible use of PT technologies by criminals but asked Interpol offices to respond to two general statements:

We have experienced that LT-technologies are used by criminals.

Nine of twelve European respondents gave either positive (3) or partly positive (6) responses to this statement. Three respondents had no experience regarding this issue and one gave negative response. The responses from non European countries gave a similar picture.[96] Although answers to this sole question do not tell us anything about extent and methods of criminal use, they probably form sufficient basis to conclude that technologies which position and track people and objects are used by criminals.

Our second statement regarding criminal use of PT technology was:

We have experienced that criminals use PT technologies against the police.

Five of twelve European respondents gave partly positive reply to this question,[97] one replied partly negative, but the majority either gave negative response (4) or had no experience regarding this issue (2). Answers from the non European group of respondents indicate that use of PT technology against the police may be a greater problem in other parts of the world: Eight of twenty-one respondents gave positive responses to the statement, partly positive: 2/21, negative: 6/21, partly negative: 1/21 and no experience: 4/21.

We read answers to this question as a confirmation that potentials of this technology have been directed against the police force itself both in Europe and in other regions of the world, and that this problem may be greater in countries outside Europe. Frequency and extent is however not indicated in our inquiry.

To what extent may use of PT technology by criminals be relevant to police use of this technology? It is possible that the referred answers only tell us the rather obvious: namely, that PT technology has potentials for everybody that uses it and that it is likely that both police and criminals have protecting need to protect themselves from use by the other. In this lies an elementary but rather important insight. Many PT technologies with basic ability to track and position people and objects are relatively cheap and available to everybody.

However, full benefit of these technologies requires access to service providers and stored traffic data etc. Provided the police is the only actor with access to data bases at network operators, service providers etc, their deployment of technology will be much more powerful than what most criminals may attain. Protection from access by criminals of stored traffic data of various service providers is thus probably a crucial requirement if PT technologies first and foremost shall facili-

96 Nine of twenty-one gave positive reply, partly positive: 5/21, negative: 2/21, partly negative: 2/21 and no experience: 3/21.

97 No one gave a (fully) positive reply.

tate work at law enforcement (and not criminal actors). Included in the discussion of future legal regulation, protection of localization data thus seems to be an important issue.

5.8 Concluding observations and regulatory considerations

Our inquiries regarding police use of PT technology do not give "hard data" on which we may draw firm and general conclusions. Answers first and foremost supplement, confirm or weaken our premises which were background of statements in the inquiry. Five topics seem to be of special relevance:

- Way of and degree of regulation
- Usefulness and cost-efficiency
- Independence of actors
- Vulnerability towards criminals
- Extent and type of police power

In conclusion of this chapter we will make some provisional reflections based on the responses to questions/statements referred above.

Way of and degree of regulation

The first question is of course whether or not the use of technology to localize and track people and objects should be regulated at all. Given the infringing potential of such methods, it could be assumed that at least some uses should be regulated by law, cf. ECHR art. 8 second paragraph. To the extent that we give affirmative answer to this first question, the next question is which type of legal regulation should be preferred.

Results of our inquiry show that general law constitutes the main regulatory approach to PT technology. We have not collected detailed information regarding regulatory design in each of the 37 countries and thus answers to general questions may hide important differences. Notwithstanding, we feel certain that in most countries general law is referring to technology neutral wording. Thus GSM, GPS, Wi-Fi/WLAN and RFID are probably not regulated directly. However, this does not exclude rather direct regulation of location and tracking, regardless of manual or technological method and – if technology is applied – regardless of specific technology. Thus, incidents of general law may include general regulation of tracking as well as other more general descriptions of police methods, actions of functions (e.g. police investigation).

Given a large degree of consensus regarding technology neutral legislation, it is hardly controversial to conclude that regulations should be about functions

rather than technology itself. If so, it is important to find the right level and technique to describe such functions.

The first question is on what level descriptions of functions should be. There are of course many possible ways of categorization, for instance:

Function on overall level	Locate	Locate, general method	Locate, specified method

The first alternative (far left) is to let localization be comprised by general phrasing such as "investigation" and "monitoring". Our initial assumption, however, is that this alone would not be sufficient related to ECHR art. 8 (2). A more concrete approach is to state the function of locating or tracking directly but without describing method (manual/technological based, "techno metric"/biometric[98]). Lastly, localization and tracking methods could be stated in concrete ways, for instance by indicating how close to the body a tracking remedy may be placed (on the person, in objects etc.), for how long, within which types of environments (e.g. in order to protect client relationships with physicians, lawyers, clergymen, family members etc.). The more specific, the better predictability for citizens. Thus data and privacy protection as well as legal protection in general will be argument to choose categorises on the right hand side of the table above. Interests in effective investigation may on the other hand represent a counter argument because specification of method may imply restriction of allowed method and thus a definition of "protected areas" for criminals. Thus the alternative far right may be particularly problematic from the viewpoint of the police.

Refusal of technology-specific legislation does not necessarily mean avoidance of technological specific guidelines and operating procedures. To make effective use of technological remedies and do the job on the ground, it is obviously necessary to "translate" what general wording of legislation actually may or should imply for concrete police work. Thus, a dualistic approach with relatively stable legislation based on statements of functions and relatively dynamic guidelines and operational procedures where technological issues are concretely described, may be a fruitful approach.

Extent and type of police power

Personal data on peoples' whereabouts are at least two-layered: Firstly, it is a question of privacy in relation to the primary controller of the data, e.g. the providers of services which generate such data. Secondly, privacy is a question related to secondary use by the police and other security agencies. It may in our view be

98 See section 3.6 (above).

reasonable to identify subgroups of people according to the degree and type of exposure to police interest and power.

The largest subgroup obviously comprises those people to which police have access to personal location data, but without any effect other than disclosure; i.e. the data is accessible but not used. A second subgroup could be said to consist of people who are subject to police surveillance and control, i.e. people whose personal location data are under police scrutiny, but without further exercise of police powers. The third subgroup we suggest consists of people who are subject to execution of direct police power, for instances because they are denied access to certain areas on basis of personal location data, are arrested on basis of such location data, are subject to home detention arrangements etc. A possible fourth subgroup is of another but related type, namely people who receives *protection* from police on basis of location data about themselves. This could for instance be children as well as senile and other mentally handicapped people. Even people working in dangerous professions which may create emergency situations when the police are needed on their location as soon as possible belongs to this subgroup. Needs of protection are arguments for access by the police to their personal location data. This is not to say that these groups should be under surveillance on a regular basis (by parents, relatives, hospital management etc.). Easy access to such location data for the police may on contrary be a measure to avoid surveillance on regular basis and only be accepted in exceptional situations.

In the table below, the four proposed categories are put in sequence with the less privacy intrusive group to the left.

Police protection and safeguard on basis of personal location data	Police access to data, without use	Police surveillance and control on basis of personal location data	Execution of direct police power on basis of personal location data

The large bulk of people will not be part of this classification, because in most cases police will only have access to data from a certain time period, geographical area, service provider etc. It is natural to assume that special guarantees should be offered to people in every of these four categories, and strongest measures could be substantiated for the two subgroups on the right hand side of the table.

Usefulness and cost-efficiency

Our inquiry shows the almost unanimous view among selected European Interpol offices that PT technology is a cost-effective means of investigation. We have not examined concrete costs and tried to do an independent assessment of costs. On the other hand, there are no reasons to doubt that in many cases and under certain circumstances, GSM, GPS, Wi-Fi/WLAN and RFID will be

a reasonable and cost-effective measure to use in smaller or larger part of police work, alone or in combination with other methods. Such technology both gives grounds for technology investments by the police and use of investments in the civil society by the police.

Promises of cost-effectiveness are not the least connected to the use of existing technology and data outside the police. This may give argument for improved access by the police, and for better survey of existing services which generates personal location data, and better technological interoperability and access to these data.

We assume that personal location data from sources outside the police will be still more important; both because such sources are many and comprehensive and because it may be relatively cheap to access and use by the police. This may create a development/pressure towards streamlining police access to such data. Questions of technological interoperability are probably not a major challenge if one wishes to go in this direction (cf. section 3.4 (above)). More important is probably mapping of various services and connected information which may secure as swift and easy access to these data as possible. To the extent that such a development is realised it may accentuate questions of the interdependence of such sources of data, see below.

Independence of actors

Replies from some of the ISPs indicate that i) some companies automatically comply with police requests to give access to traffic data including personal location data and ii) that some ISP carry out analyses for the police. This only represents a small minority of the ISPs in our inquiry and we have no basis to criticise these concrete practises. However, the results make topical a general discussion of independence and interdependencies between the police and actors in the civil society with whom they interact.

Here, we will not go into possible grounds for close and closer collaboration between the police and private parties, but issues regarding efficiency are certainly among the important incentives. Arguments against close collaboration are first and foremost of a legal nature and linked to legal protection of citizens. Here, we mention only two basic considerations with special relevance for data from PT technology.

The first consideration is linked to the fact that police, when the conditions in law are met, has the monopoly of exercising lawful violence against citizens, including infringement of citizens' privacy. In such a situation, it could be claimed to be urgently important that there are strict boundaries between the police as "infringer" and other parties with whom the police choose to interact. If these lines of demarcation are blurred, it may be a danger that an *infringement by proxy*

will develop, i.e. that power to lawfully infringe peoples' privacy may seep into the business of private collaborators. Without very clear boundaries it may even be problematic to clearly establish responsibility in case powers are exceeded. Thus, in this perspective it is important that the police and the ISPs and others who are sources of information for the police have a strictly formal and defined relationship, and *interact* rather than collaborate.

This first consideration could be seen as "passive" in the sense that legal protection of citizens are safeguarded by restraint from mixing exercise of public authority with private business. The second consideration is more of an active nature. Clear distinctions between the police and involved private parties; make it possible that private parties make their own independent assessment of the legality of police requests for personal location data etc. Our inquiry was directed towards ISPs which often are quite big businesses with rather easy access to necessary legal expertise. PT technologies involve many service providers which sit on data bases with personal location data that may be of great interest to the police. On a general level in European countries, citizens may as a rule expect that the police acts within their legitimate powers and for instance refrain from unlawful collection of personal location data. On the other hand, there are several possible situations where this presumption may fail (lack of competence in the police, overly enthusiastic police detectives etc.), and where legal protection of citizens also should rest on the attentive attitudes of interacting businesses. Because PT technologies make personal location data available for the police from many service providers which could not be expected to have knowledge of the legal rules determining lawful police access to these data, it should be asked whether or not measures should be made to increase service providers competences on this point. A possible objective could be that as many service providers as possible are capable of demonstrating an equal degree of independence as the great majority of ISPs in our inquiry showed.[99]

Vulnerability to criminals

Our inquiry indicates that a part of the problem with PT technologies is that it is deployed by criminals and even directed towards the police. This situation may call for measures that may reduce this threat. Certainly, there are very limited possibilities to reduce general access to technology that generates personal location data etc. GPS devices will for instance always be available even for people with dishonest intentions. However, these limitations should not hinder us from considering if stored personal location data could be protected in a better way in order to prevent unlawful access and consequent legal actions. Personal loca-

99 Other questions of independence and competence are discussed in Deliverable 3.

tion data are elements of what should be retained pursuant to the Data Retention Directive, cf. Art. 5, 1.(f)(2). The technological development and widespread use of PT technologies remind us that this data are increasingly stored in data bases connected to a large number of service providers. On this background it should be discussed if information security requirements and actual compliance with these requirements are satisfactory.

6 Data protection authorities' views on PT technology

6.1 Introduction

Two questions in the data protection authority inquiry contained rather comprehensive sets of statements concerning the authorities' evaluation of data protection effects of PT technology. [100] One set of statements concerned police use of PT technology and effects for data protection.[101] The other set of statements concerned evaluation of data protection effects in general. [102]

The first question contained eight statements with reply alternatives yes, no and don't know. The German DPA only responded to half of the statements and the authorities of Austria, Bulgaria, Norway, Slovakia and Slovenia gave full response.

6.2 Police use of PT technology and effects for data protection

Questions regarding effects of police use of PT technology for privacy and data protection were part of Q4 of our inquiry. Even Q1 contained three statements regarding this issue. All relevant statements will be referred in this section.

Five data protection authorities gave their view on the legal basis for processing personal data related to PT technology:

- PT-technology challenges the requirement of clear legal basis for processing of personal data.

Legal basis refers to consent and necessary grounds as stated in DPD art. 7. In addition, a clear statutory basis could make the processing lawful. Here, replies demonstrate a marked difference between the countries. Two countries (Bulgaria and Slovenia) totally disagreed to the statement, while the three other authorities (Austria, Norway and Slovakia) totally agreed. Since rules regarding consent and

100 Six of eight authorities responded to the questionnaire, while two authorities (the Italian and the Romanian) only gave brief overall statements. Two of the questions in the questionnaire concerned knowledge of services based on PT technology as well as their knowledge of police deployment of such technology. Results from these two questions are already referred, see section 5.6.

101 Question 1.

102 Question 4.

necessary grounds are similar in all countries, it is likely that these differences refer to differences of existing statutory basis. Similar to replies from Interpol offices regarding the need for a clear legal basis for the use of PT technologies (cf. section 5.2), replies do not indicate a unanimous claim for legal amendments. Such needs may of course exist but that there are probably clear differences regarding the regulatory situation in each country.

The autonomy of data subjects is considered to be an important aim for privacy protection, and may also be seen as a basic precondition for acceptable privacy regimes.[103] We asked the respondents to indicate their view on the statement:

- PT-technology weakens the autonomy of data subjects.

All five responding authorities agreed. Three totally agreed (Austria, Norway, Slovenia) and two partly agreed to the statement (Bulgaria, Slovakia).

In Q4 we gave a related statement:

- Data subjects are offered co-determination regarding development and use of PT-technology.

Four of five respondents disagreed with this statement. Three totally disagreed (Norway, Slovakia and Slovenia), while the Austrian authority partly disagreed. The Bulgarian authority did not know.

It seems that replies to these two referred statements confirm that autonomy and co-determination may be a challenge when PT technology is deployed by the police.

As explained in section 3.3, PT technology may imply a more or less close connection between the object (smart phone, care, RFID tag) that is positioned and one or several persons who are related to the object. We asked the respondents in the national data protection authorities about their opinion of the statement:

- PT-technology implies secure identification of data subjects.

The Norwegian authority totally disagreed, while the others partly agreed (Austria, Slovenia, and Slovakia) or totally agreed (Bulgaria). Concretely assessed, responses to this statement should to a large extent rely on which subgroup of technology and type of situation the respondents consider. However, replies could be seen as express of these authorities' basic expectations and attitudes to the question.

One important privacy and data protection principle is about minimality. On this background the data protection authorities were asked to consider the statement:

- PT-technology challenges the requirement that processing of personal data shall not be excessive in relation to the purpose of the processing.

103 Although even a patriarchal approach may be claimed to be acceptable.

Four of five respondents agreed with this statement. One partly agreed (Bulgaria) and three totally agreed (Austria, Norway and Slovakia). The reply from Slovenia partly disagreed.

Another major privacy concern is of course confidentiality. The relevant statement was worded:

- PT-technology weakens the confidentiality of personal data.

The result was similar to the previous statement: All five responding authorities agreed. Three totally agreed (Bulgaria, Norway, and Slovenia) and two partly agreed with the statement (Austria, Slovakia).

The three first statements in Q1 concerned possible side effects of police deployment of PT technology. One of these statements was formulated on basis of the fact that the location of people may reveal private life and relations, combined with the obvious fact that it is almost impossible to avoid that the police locate and track people who later will be checked out of the case as innocent:

- Police use of PT-technology has negative effects for innocent people.

Only the Slovenian DPA answered agreed with this statement, while two authorities disagreed and two did not know.[104] It is hard to interpret these results. Probably respondents have answered on basis of different presumptions. To the authors of this report it is hard to make other presumptions than i) it is sometimes uncertain whether or not targeted people are involved in crimes; and ii) in case they are not involved there will always be a possibility that information about them will continue to exist in police files.

The next two statements did not presuppose that tracked persons are innocent, but referred to the right to enjoy a protected relation to a person's lawyer or physician and the fact that information regarding location could reveal this relationship.

- Police use of PT-technology has negative effects for the relation between the data subject and his/her lawyer.
- Police use of PT-technology has negative effects for the relation between the data subject and his/her physician

None of the DPA agreed with these statements, two disagreed and three did not know.[105] The responses are quite surprising. It is obvious that ability to track people may show that they call on a physician and thereby reveal medical conditions which are expected to be confidential information. It may be that answers would

104 The German DPA did not reply to this statement.

105 The German DPA did not reply to these two statements.

have been different if "has negative effects" was replaced by "may have negative effects".

In Q4 we included one statement concerning sensitivity of data, with reply alternatives yes, no and don't know:

- PT-technology implies processing of sensitive personal data.

The replies we received were – not unexpectedly – highly scattered. Two answered yes, two answered no and one did not know. Data from PT technology could be regarded sensitive, but may just as often be thought of as rather trivial. No one of the respondents commented on this problem. Location which e.g. indicates places connected to special categories of personal data, such as religious beliefs (place of worship) or political opinion (place of political protest march) would in many situations be regarded sensitive.[106]

Duration of data storage and thereby the accessibility of personal data regarding peoples' whereabouts is obviously an important indication of level of privacy and data protection. We asked opinions on the statement:

- Personal data from PT-technology are stored for a limited amount of time.

Two respondents totally disagreed (Norway and Slovakia), one partly agreed (Slovenia), one totally agreed (Bulgaria) and one did not know (Austria).

We also asked about the opinion of data quality:

- PT-technology implies high quality of personal data.

Three partly agreed to this statement (Austria, Slovenia and Slovakia), Bulgaria totally agreed, while Norwegian reply totally disagreed.

Responses to a statement on information security gave very scattered results:

- Information security linked to PT-technology is challenging.

Two totally agreed (Austria and Norway), one totally disagreed (Bulgaria) and the two others partly disagreed (Slovenia) and partly agreed (Slovakia).

Another important point of privacy and data protection is access rights and transparency. In Q4 we presented the statement:

- Access rights and transparency are fully respected when PT-technology is used.

Three of five respondents disagreed. One totally disagreed (Norway) and two partly disagreed (Austria and Slovakia). Two partly agreed (Bulgaria and Slovenia). It seems in other words to be a certain level of agreement that there is a potential for improved access and transparency related to PT technology.

106 Cf. DPD art. 8 (1).

We should of course be very cautious when drawing general conclusions on basis of this small inquiry. PT technology is not one homogenous topic and a reasonable (but not existing) reply alternative to some of the statements we asked for responses to could have been "it depends". Other responses must probably be understood on the background of national differences regarding legislation and practices. This said, although we are unable to explain underlying reasons for agreements, it seems to be possible to indicate some conclusions on an overall level. At least, there is a large degree of agreement among the data protection authorities responding to our inquiry that:

- PT-technology weakens the confidentiality of personal data.
- PT-technology weakens the autonomy of data subjects.
- PT-technology challenges the requirement that processing of personal data shall not be excessive in relation to the purpose of the processing.

At least four of five data protection authorities agreed with these three statements, and no one totally disagreed.

Another result seems to be that the responding data protection authorities have a many-facetted approach to what here is denoted PT technology. Their responses to the query do not contribute to a uniform picture of this technology.

6.3 Effects for data protection authorities of police use of PT technology

Four statements in Q3 were about the data protection authorities and their competences and activities regarding police use of PT technology. Reply alternatives were yes, no and don't know.

- The data protection authority has power to control the police's use of PT-technology.

Five DPA confirmed that they had such powers,[107] while the authority in Norway expressed that they did not have the power to control police use of PT technology.

- During the last two years, the data protection authority has carried out control of police use of PT-technology one or several times.

107 The Bulgarian authority explained that they do not have the power to control the specific choice of PT technology, but can control the data processing itself by such technologies.

Three DPA had carried out such controls during the last two years.[108] Two of the authorities with the power to control, had not carried out such controls.[109]

- Control of police use of PT-technology has been basis of criticism from the data protection authority against the police.

Two of the authorities which had carried out control with the police, answered that these controls have been basis of criticism from the data protection authority against the police.

- The data protection authority often receives complaints from individuals who are subject to police use of PT-technology.

None of the DPAs often receives such complaints. Note that the statement uses the word "often", and less frequent complaints are not covered by that statement.

The last statement in question 1 concerned the DPAs evaluation of legislation:

- Current legislation provides sufficient data protection in connection with police use of PT-technology.

The DPAs of Norway, Slovakia and Bulgaria gave affirmative feedback to this statement. Only the authority of Slovenia disagreed. The Austrian authority did not know and the German authority did not answer.

Results from Q3 should be considered on the background of Q4 of our inquiry. Here, the two last statements concerned the work situation of the Data protection authorities, with the reply alternatives yes, no and don't know:

- PT-technology creates much work for the national data protection authority.

Five of six of the authorities agreed with this statement, one disagreed (Slovakia).

- The national data protection authority is in constructive dialogue with the police regarding PT-technologies.

Five of six authorities agreed with this statement. The Norwegian authority disagreed.

A cautious interpretation of these replies may indicate that most data protection authorities of the six countries both have a dialogue and control police use of PT technology, but dialogue seems to be more important than control. For the great majority of these authorities, positioning and tracking technology creates much work, but this seems not to be generated by complaints from individuals.

If we consider all referred questions country-wise, the data protection authorities of two authorities should receive special attention. The Slovenian autho-

108 The Norwegian authority is without power in this area had had naturally not carried out any controls either.

109 The authorities in Slovakia and Austria.

rity seems to be the most critical of the six authorities who gave responses: They have power to control PT technology used by the police; carry out controls and direct criticism against the police; agree that PT technology has negative effects on innocent people and disagree that current legislation provides sufficient data protection in connection with police use of PT technology. Answers from the Norwegian authority are very different from those of the Slovenians: It states that it has no power to control PT technology used by the police and has consequently not carried out controls or directed criticism against the police; it disagrees that PT technology has negative effects on innocent people and the relations between data subject and lawyer/physician; and agrees with the statement saying that current legislation provides sufficient data protection in connection with police use of PT technology.

6.4 Concluding observations

There are methodologically weak points in the parts of our inquiry referred in this chapter; particular regarding some of the results reported in section 6.2. The reasons are first and foremost that PT technology is a heterogeneous category and that each type of technology is and may be used by the police in various situations. We should thus be careful to draw conclusions other than on overall general level.

Many of the statements we presented to the data protection authorities gave plenty of room for interpretation and thus the possibility to only look at the down-side of PT technology. However, we evaluate the replies as being rather multi-facetted and far from drawing a scare picture. Of course, if inquiry had been connected to special and controversial application of technology to determine peoples' position etc., answers could have been different.

WP7 could be said to rest on a misconceived emphasis placed on certain technologies; cf. "To assess the use of RFID and geolocation devices in the detection, prevention and/or prosecution of crimes across Europe ..."[110] Research is a learning process, and reconsidering the research objective and project design of this WP, it may have been a better approach to only concentrate on *what technologies may do*, namely locate and track, instead of focusing on the specific technologies which have made geolocation such a hot topic.

The principle of technology neutral legislation could be said to make such an approach obvious. However policy documents issued by the Commission and Article 29 Working Party have also a technology perspective: Special attention is for instance given to privacy protection connected to RFID and apps on smart

110 Quote of the first part of the objective for WP7.

phones, i.e. on technologies. Such documents encounter the same types of challenges as part of our inquiry; answers depend to a large extent on concrete applications and situations.

7 Main findings and concluding points

One major result from the work in the first part of WP7 is an extended technological model which describes what we claim is a fruitful technological understanding as basis of discussions of personal location data and privacy protection. While the upper left cell in the table below was point of departure of WP7, our discussions have developed a much more complete description of all relevant technologies, including classification and concepts to describe main elements (cf. all four cells in the Table).

	Directed towards	
	Things /artefacts	**People**
Wireless/mobile	*techno metric* GSM, Wi-Fi/WLAN, GPS, RFID etc.	*biometric* Fingerprint, facial, retinal and gait recognition etc.
Wired/fixed	*techno metric* Point of sale terminals, Automated Teller Machines etc.	*biometric* Fingerprint, facial, retinal and gait recognition etc.

Many of these technologies are pervasive and penetrate a large number of activities, functions and relations of the civil society, and their concrete existence and application are in our view too many and manifold to exhaustively map as part of this work. Thus, we have only discussed selected areas of application comprising: Marketing access control to rooms; buildings etc.; tracking/localization of employees; tracking/localization of children; insurance services (of cars, vessels etc.); access control to information; public transportation payment; toll-road payment; tracking/localization of students, and public events (music, sports, etc.).

With a large variety of basic technologies which may generate data about peoples' whereabouts plus a variety of possible uses of such data (included use by the police), the importance of privacy protection related to this technology will probably be increasing in the years to come.

Our inquiries indicate that:

Regarding knowledge of PT technology

- The PT technologies GSM, WLAN/Wi-Fi, GPS and RFID have been introduced in all investigated countries and deployed for similar purposes in all these countries.
- Providers of services based on RFID and GPS seems to be much less known to European telecommunication authorities, compared to providers of other PT technologies (GSM, Wi-Fi/WLAN).

- A lot of services are based on RFID and GPS, but national telecommunication authorities have no or only little knowledge of the relevant service providers. It may be that other authorities update lists of such service providers, but we cannot see that other civil authorities are in the position to carry out such mapping. Thus, we hold it as probable that it may be difficult for police authorities to know where PT technology is used in the civil sector, and for which purposes.
- It seems that data protection authorities typically have more knowledge and more secure knowledge than the telecommunication authorities regarding police application of PT technology as means of investigation.
- Regarding PT technologies, data protection authorities seem to have the most knowledge of GSM and least knowledge of RFID.

Regarding use of PT technology by the police

- There is an almost unanimous view among the seven European police respondents that PT technology is a cost effective and important means of investigation in their country. Police from other parts of the world seem to assess that these technologies are comparatively less important.
- Data from PT technology are also valuable to the police as investigation materials, without data being disclosed in court.
- Answers from 18 European ISPs in countries of our inquiry, indicate that the majority of ISPs experience that police often ask for traffic data which may reveal peoples' location and movements, and the majority of companies also experience an increased interest on the part of the police in such data.
- Our investigation indicates that RFID is most used in the different groups of services studied.[111] Still, of the examined PT technologies, the police assess that RFID is/will be least important to police investigation, both today and in five years.
- In the opinion of European Interpol respondents, GSM and GPS are marked more important for police investigation than other PT technologies, and it is expected that their significance will increase in the five years to come. Police in other parts of the world hold GSM as the most important technology for them, both now and in the next five years.
- A clear majority of Interpol responses from Europe and other parts of the world indicate that PT technology is used by criminals. According to Interpol responses, it seems to be far less frequent that PT technology is directed

111 Cf. marketing access control to rooms; buildings etc; tracking/localization of employees; tracking/localization of children; insurance services (of cars, vessels etc.); access control to information; public transportation payment; toll-road payment; tracking/localization of students, and public events (music, sports, etc.)

against the police, but according to almost half of the European responses this threat seems to be relevant.

- Ten of eighteen ISPs disagreed to the statement that their company "does not always act in accordance with police requests for access to traffic data that may reveal the location and movements of objects (and thus individuals)". Three ISPs representing two countries confirmed that their "employees often perform analyses of traffic data on behalf of the police". These answers may indicate a need to discuss the degree of and importance of independence of ISPs vis-a-vis police authorities.

Regarding costs

- There is a big and growing sector outside the police domain where PT technology is in use and which may serve as a reservoir of data in case of legitimate police needs. Thus, the coming into existence of this data is basically without costs for the police.
- The great majority of investments in PT technology happen in civil society. Thus, even though police need to make their own investments to access and make use of personal location data collected by others, such use is of course much cheaper compared to methods based on direct positioning and tracking of individuals by the police.
- Once permission from the court or from superior body of the police[112] is attained, concrete use of such methods (collection and analyses of personal location data) could be relatively cheap for the police.[113]
- The threshold effect of costs for the police related to attainment of permission from the courts to collect personal location data (prior permission or succeeding approval) should probably not be underestimated. Thus legislation limiting access to such location data by requiring review by courts of law and permission, both constitute a formal obstacle and (probably) an economical threshold due to procedural costs etc.

Regarding data protection authorities experiences and views on PT technology

- There is a large consensus among the responding data protection authorities that PT technology i) weakens the confidentiality of personal data; ii) weakens the autonomy of data subjects and challenges the requirement that

112 Typically in cases where it is critical to swiftly collect information in order to stop an evolving serious crime.

113 Dependent on interoperability, the model for division of expenditure between the police and the private party from whom the data is collected etc.

processing of personal data shall not be excessive in relation to the purpose of the processing.
- Replies from data protection authorities indicate that most of these authorities both have a dialogue with the police regarding PT technology and control police use of it. Dialogue seems to be more important than control.
- For the great majority of data protection authorities taking part in our inquiry, positioning and tracking technology creates much work, but this seems not to be generated by complaints from individuals.

Regarding legal regulation of PT technology
- In most European countries investigated general law is main type of regulation of PT technologies.
- Only a small minority of investigated European countries have specific regulation of PT technology as main type of regulation.
- The overall picture is that deployment and use of GSM and GPS is better covered by legal instruments than WI-FI/WLAN and RFID.
- More than half the European police respondents seem to be satisfied with the current legal regulation of PT technologies. Results indicate that among the twelve European Interpol offices taking part in the query, there is a rather small group of "reform-friendly" offices.
- Willingness by Interpol offices to amend current regulations increases if more efficient use of PT technologies by the police is the aim of reform.
- Within our selection of Interpol offices, support for regulatory reform seems to be much stronger among offices in countries outside Europe compared to European offices.

Regarding regulatory considerations
The technological understanding developed in chapter 2 combined with our basic legal training and experience, resulted in a list of possible regulatory consideration which were tentatively discussed in section 4.6.2. This comprises:
- Voluntariness and competence of data subjects
- Number and types of parties involved in the processing of location data
- Purposes, potentials and effects of processing location data
- Type of power executed as part of processing location data
- Transparency and accessibility of location data processing

The brief analyses made of each issues of the bullet point list have significance on its own, but are especially designed to fit into the assessment analyses, see Part II, chapter 3.

PART II

Assessing impacts on individual rights of positioning and tracking people

1 Introduction

Inquiries reported in Part I of this report were based on the concept "position and tracking technologies", abbreviated "PT technologies." PT-technologies are characterized by:

I. Application of infrastructure/electronic communication (e.g. GPS,[114] GSM,[115] RFID,[116] WLAN,[117] WiFi,[118] Bluetooth,[119] ultrasound);
II. with the objective to locate and trace objects (e.g. vehicles, equipment, vessels, containers, small items (cloths, bags, people, animals);
III. which have a unique identity (e.g. RFID-tags, SIM-cards, license plates, QR-codes[120])

Our analyses concluded that positioning and tracking technologies as defined here as starting point of our research, represents one of several categories of technologies related to data on peoples' whereabouts. Thus, in Part I, section 3.6 we suggested an overall model which captures all technologies with ability to determine position of people and their movements.

Particularly two types of technological properties should be highlighted: Wired (fixed) and wireless (mobile) technology, and ii) technology directly directed towards things/artefacts and technology directly directed towards people:

	Directed towards	
	Things /objects	**People**
Wireless/mobile	***technometric*** **GSM, Wi-Fi/WLAN, GPS, RFID etc.**	*biometric* Fingerprint, facial, retinal and gait recognition etc.
Wired/fixed	*technometric* Point of sale terminals, Automated Teller Machines etc.	*biometric* Fingerprint, facial, retinal and gait recognition etc.

Table 1 Main classification of location-enabling technology

The shadowed cell (above) contains the type of technology as the point of departure of inquiries reported in Part I. According to well established use of concepts, technology which directly "reads the body" is *biometric*. In Part I focus was on technology which reads/measures digital devices which people carry or is close

114 Global Positioning System.
115 Global System for Mobile Communications.
116 Radio-frequency identification.
117 Wireless local area network.
118 Wireless exchange of data using radio waves over a computer network.
119 Wireless exchange of data over short distances using short-wavelength radio transmissions.
120 Quick Response Code, a type of matrix barcode.

to. Thus, technology is not biometric but reads/measures objects which are close to or even attached to a human body. As a corresponding term to biometric we thus introduced the term "*technometric* technology".

In Part I we used the term "position and tracking technology" ("PT technology") to denote mobile/wireless technology capable of positioning and tracking people by targeting objects in the proximity of a person. The insights demonstrated in Table 1 create needs for a new concept which embraces every technology in the table, regardless if it is wireless/wired and technometric/biometric. Thus in Part II of this report, the concept "*location-enabling technology*" will be used to denote all four subcategories of technologies in Table 1. In this work, each of the four subcategories indicated in the table are not important; all discussions below will have all location-enabling technologies as subject. Further, the designation indicates the fact that many of these technologies do not have location as objective, but nonetheless have qualities which makes it possible to locate and track people.

In our view, the overall importance in a privacy impact assessment is *function* rather than technology itself. Even though we will argue that privacy assessments may be different for technometric and biometric technology, the similarities are more important than differences. Thus, in the following impact assessment, we include all technology which may perform the function of deciding the position and movements of people, i.e. both technometric and biometric technology. This implies that all four categories of technologies in Table 1 will be included in the following impact assessment. Our research attention in the first part of this report has been on what was called "positioning and tracking technology" (first cell). Discussions will thus to a large extent be about examples within this category.

When location-enabling technology is used for positioning and tracking purposes, we assume that some common features may be identified as illustrated below.

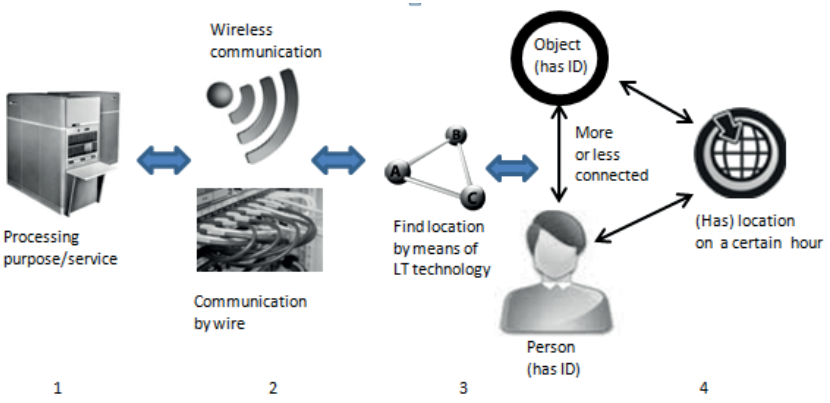


Figure 1: Basic chart of positioning and tracking technology use

For detailed explanation of Figure 1 we refer to Part I, section 3.3. Identification of objects connected to a person or of a person directly, is carried out in step 3, followed by positioning or series of positioning (tracking) in step 4. Impact on privacy is of course produced by the entire process, i.e. all four steps.

2 Relevant EU regulations and guidelines

2.1 Introduction and brief overview of regulation on EU level

This chapter contains an overview of applicable EU legislation especially relevant for location and tracking of people. The discussion is limited to selected aspects, and the selection will subsequently be explained and substantiated. We also assume that the main lines of the general legal framework are known to the reader; mainly regarding the Data Protection Directive.

As a point of departure, we take it that location and tracking of people by means of technology implies processing of personal data. Thus as starting point, Data Protection Directive (95/46/EC) applies provided the processing falls under the substantive and geographical scope of the directive.[121]

The scope of the Data Protection Directive but with exemptions regarding "processing operations concerning public security, defence, State security [...] and the activities of the State in areas of criminal law", and processing of personal data "by a natural person in the course of a purely personal or household activity", cf. article 3 (2). A limited part of the exemption first mentioned is covered by Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Roughly put, scope of the framework decision is linked to transmission of personal data between Member states and between certain competent authorities and information systems linked to the European Union, for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.122 It is clearly stated in the decision that it is "without prejudice to essential national security interests and specific intelligence activities in the field of national security".123 Each country may chose to have higher standards than imposed by the decision.124 Since the framework decision is limited to transfer/exchange of personal data on international level, the significance of it for questions of positioning and tracking is limited. We will only return to specific points of this set of rules if relevant.[125]

121 Scope of the Directive is discussed in section 2.3.2 (below).

122 Cf. article 1(2).

123 Cf. article 1(4).

124 Cf. article 1(5).

125 A much more comprehensive set of rules is put forward in Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Brussels, 25.1.2012 COM(2012) 10 final). To date (October 2013) this proposal is still negotiated and we will thus not go into detail.

The second applicable directive that is Directive 2002/58/EC, the "e-Privacy Directive",[126] which particularises and complements Directive 95/46/EC regarding processing of personal data in the electronic communication sector. Since important positioning and tracking activities are linked to electronic communication, this Directive is relevant to parts of our discussion. The e-Privacy Directive does not apply to *information society services*, i.e. "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." Even services providing access to or transfer of information over an electronic communications network or providing web hosting of the recipient's data are covered by this exception. The understanding of "information society services" is far from clear, and here we do not have sufficient grounds to discuss the interpretation. In our context it is sufficient to note that localization functions may be part of such services and therefore not regulated by the e-Privacy Directive. Which types of technology use/services that will be covered must be decided on a concrete level.

A third Directive of interest is Directive 2006/24/EC, the Data Retention Directive. It encompasses "traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user." Duty to retain traffic data etc. applies, inter alia, to mobile telephony and internet communication. Communication generated through use of these communication platforms shall in other words be subject to data retention, regardless of contents of the communication. Thus a request to find a friend, measure travel time from A to B, carry out payment etc. may result in retention of these data.

Data retention pursuant to the Directive applies to "publicly available electronic communications services or of public communications networks" and therefore does not cover communication between components outside such services and networks, for instance between a private GPS unit and satellites or between RFID readers and tags. However, if data from such communication is transferred through public networks/services, data will be subject to the retention obligation. Much, but not all, personal location data generated will in other words be available for police on the conditions established in national legislation of each country pursuant to the Data Retention Directive.

Summing up, in order to give a rough survey of EU legislation concerning personal location data:

- The majority of personal location data *in civil society* is protected by EU data protection instruments (exceptions being data processed "by a natural person in the course of a purely personal or household activity" and "data processing operations concerning public security, defence, State security [...] and the activities of the State in areas of criminal law");

126 As revised by Directive 2009/136/EC.

- Most personal location data collected and further processed *by the police* only enjoys a very limited protection by EU data protection instruments; at the same time,
- a large fraction of personal location data are under EU obligation to be retained for police purposes; but
- some personal location data are not under obligation to be retained because they are not part of publicly available electronic communications services or public communications networks.

In particular within the field of police work, EU law leaves a rather wide room of manoeuvre for national legislators. Moreover, there are variations between countries regarding implementation of the directives. Thus, current EU law may give clear indications of privacy protection in national legislation in civil society, but only limited input to the understanding of privacy protection in the policing sector.

EU legislation regarding privacy protection is under revision and a proposal for a Data Protection Regulation[127] is forwarded to replace the Data Protection Directive. Similarly, a Directive is proposed to replace the Council Framework Decision on personal data processed in the framework of police and judicial cooperation in criminal matters, and to greatly expand the legal regulation within this sector.[128] At this stage of the legislative process (November 2013), there is still considerable uncertainty regarding contents of the final legislation. Thus, we will not make systematic use of available drafts. Certain innovative elements of the proposed Regulation will however be integrated in some of our discussions in chapter 3 (below).

2.2 Other relevant EU documents

2.2.1 Introduction

Above we have introduced legal instruments which all partly regulate questions of localization. Below, we will make a brief presentation of other important documents from EU authorities with special relevance location-enabling technology.

127 Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD))
Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

128 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data {SEC(2012) 72 final} {SEC(2012) 73 final}.

2.2.2 Commission Recommendation regarding RFID and Privacy and Data Protection Impact Assessment Framework for RFID Application.

In 12 May 2009 the European Commission issued a recommendation of on the implementation of privacy and data protection principles in applications supported by radio-frequency identification ("RFID recommendation"). Potentials of applying RFID technology to *monitor* individuals through their possession of one or more items that contain an RFID item are stated as one of the motivations for giving the Recommendation.[129] The possibility to localize tags and possible privacy implications thereof is imbedded in the definition of monitoring: 'monitoring' means any activity carried out for the purpose of detecting, observing, copying or recording the *location*, *movement*, activities or state of an individual" (italics added).[130] Thus the perspective of the Recommendation is wider than questions of peoples' whereabouts in that it also takes into consideration questions of activities and state of individuals.

Regarding monitoring, emphasis is placed on assessing implications for the protection of personal data and privacy. Assessments should direct special attention to whether or not an application could be used to monitor an individual.[131] In article 4 it is stated that Member States should ensure that industry and other relevant civil society stakeholders, develop a framework for such impact assessments, and submit it for endorsement to the Article 29 Data Protection Working Party (cf. below). It is also recommended that Member States ensure that "operators develop and publish a concise, accurate and easy to understand information policy for each of their applications." Certain minimum requirements are defined for such information. Whether the location of tags will be monitored is one of these information requirements.[132]

On basis of the Recommendation, an industry-prepared framework for personal data and privacy impact assessments of RFID applications was adopted 12 January 2011. It contains definition of key concepts as well as a rather detailed description of recommended procedures. The process is organised in two phases; initial and risk assessment phase, and both full scale and small scale assessment procedures are described. In annexes to the document, it is suggested how RFID applications should be described as basis of a privacy impact assessment, and nine relevant privacy targets and fifteen privacy risks are specified.

129 See, the preamble, section 5.

130 See, Recommendation, art. 3(g).

131 See, Recommendation, art. 5(a).

132 The others are information on the identity and address of the operators; the purpose of the application; what data are to be processed by the application and in particular if personal data will be processed.

Here we will not go into detail regarding privacy targets and risks. We limit ourselves to noting that most privacy targets are closely linked to questions of compliance with applicable regulation, in particular the Data Protection Directive. This is of course a relevant line of action. However, in our view it is also of interest to questions if other privacy targets may be relevant, i.e. targets based on *legal political* considerations not (properly) addressed in existing regulations, in addition to issues affiliated with the law as it is.

The Recommendation and the Privacy Impact Assessment Framework for RFID Applications is of course relevant for the discussion below. However, they only relate to one of many relevant technologies (cf. section 1.2, above) and have a wider perspective than location. An important observation is that these documents are technology specific. In our view legal privacy impact assessments and political considerations should address localization, i.e. the function of various technologies rather than each technology itself. In chapter 3 we will return to questions of choice of perspective for assessment of location-enabling technologies.

2.2.3 Opinion 13/2011 of the article 29 Data Protection Working Party on geolocation services on smart mobile devices

In 2011 the Article 29 Working Party adopted an opinion on geolocation services on smart mobile devices.[133] The opinion evaluates location services and not the underlying technology itself; however GPS, GSM and Wi-Fi are presented as technologies on which these services are based, and in the opinion the technological and organizational description of technology is an important premise for the legal discussion of the services. Several other technologies could be applied to produce services and functions based on personal location data (WLAN, RFID, ultrasound, Bluetooth, ANPR), but such other technologies are not mentioned, and the Working Party does not explicitly apply a general approach, neither to technology nor to location services.

Examples of services mentioned in the opinion are: maps and navigation, geo-personalised services (including nearby points of interests), augmented reality, geo-tagging of content on the Internet, tracking the whereabouts of friends, child control and location based advertising. In many of these services location may be seen as the main objective, and the Working Party does not discuss other services and functions where other objectives dominate; for instance payment and access control. Furthermore, the opinion does not discuss the relation between civil/pri-

133 ARTICLE 29 Data Protection Working Party, opinion 13/2011 on Geolocation services on smart mobile devices.

vate use of geolocation services and the possibility that police and other security authorities access the data generated by these services.

Despite the fact that the opinion has a more narrow approach than this project, the clarification of legal regulation and the assessment of privacy risks is informative and useful for discussions regarding location-enabling technology. However, as we see it, the opinion contains mostly a concretisation and information regarding legal questions which do not add much to the general understanding of the Data Protection Directive, and here we will therefore not explain the contents of the document.

2.2.4 Opinion 02/2013 on apps on smart devices

The objective of this opinion is to clarify the legal framework applicable to the processing of personal data in the distribution and usage of apps on smart devices. The opinion also considers processing which might take place outside of the app, for instance using collected data to build profiles and target users. The fact that apps often comprise localization services is stated as one important motivation for the opinion.

Among the basic observations of developments creating privacy risks is the fact that development of apps may be carried out by small businesses without knowledge of privacy and data protection requirements which could attain a world audience. The discussion in the Opinion of the applicable European legal regulation should thus first and foremost be regarded as having an educational aim. The addressees of the opinion are primarily the group of actors that may be included in the development and use of apps, including: developers; owners; app stores; manufacturers of operating systems and device manufacturers. Also in the target group are third parties that are involved in the collection and processing of personal data from smart devices, such as analytics and advertising providers.

Towards the end of the Opinion, the Article 29 Working party sums up their discussions by lists of recommendations; both what relevant actors "must" do and what the Working Party recommend that these actors do. Only one of these points could be said to directly concern location-enabling technology.

Firstly, according to the Working Party, app developers must "Ask for granular consent for each type of data the app will access; at least for the categories Location, Contacts, Unique Device Identifier, Identity of the data subject, Identity of the phone, Credit card and payment data, Telephony and SMS, Browsing history, Email, Social networks credentials and Biometrics;". Here personal location data is one of the types of data which should be separately mentioned and evident as part of a consent procedure.

We will not go into detail regarding discussions and recommendations on apps on smart devices, but will only underline the fact that much of this opinion

is relevant for location-enabling technology. However, although they represent an important part of the problem area, privacy questions relevant to location range much wider than apps on smartphones etc. It is also worth noticing that while Opinion 13/2001 takes geolocation *services* as starting point, Opinion 02/2013 has a *technology* perspective (apps and devices). One major difference between the Opinions is that the latter is much clearer regarding relevant actors and their obligations and ought-to-dos.

2.2.5 Concluding reflections

The documents discussed in section 2.2 all provide valuable support for correct application of the law and for legal considerations in line with the principles on which current legislation is based. The documents do not problematise the transfer of personal location data from applications used in civil society to use by the police and other law enforcement authorities. A privacy assessment along the same line of thought as could be found in framework for personal data and privacy impact assessments of RFID applications will first and foremost produce repetitions and will thus be of limited benefit. In our view, given the extensive use of personal location data that may be foreseen in future, and given the probable great importance of such data for law enforcement authorities, there is a need to try to do analyses "outside the box" or at least without too tight bonds to well established perspectives. This is partly done by discussing issues actualised in Part I, and partly by assessing aspects outside what customarily is reckoned as privacy protection. Thus, in chapter 3 we will try and assess privacy risks and other effects for individuals of the processing of personal location data from a slightly different perspective than in the referred documents.

2.3 Selected basic considerations viewed on basis of the Data Protection Directive

2.3.1 Introduction

In this section we will briefly discuss selected questions related to the Data Protection Directive. Our main motivation is to highlight points regarding personal location data which we think should be given special attention, inter alia, in the context of succeeding police use. The relevant provisions of the Directive are implemented in national legislation in ways which probably creates variation between the national legal systems, and it is of course these national laws which in fact have legal effect. Thus, discussion of the Directive does not give basis for firm conclusions of the actual legal situation in each country, but rather produce some

expectations of the state of affairs. Our discussion is carried out on the precondition that readers know basic structures and contents of the Directive.

2.3.2 Scope

Scope of the Data Protection Directive is wide and generally comprises processing of personal data. Several exceptions are made, of which we will mention two. Both exceptions narrow the privacy protection of personal location data pursuant to the Directive. Exception is made regarding "processing operations concerning public security, defence, State security [...] and the activities of the State in areas of criminal law" (art. 3 (2)). Further processing by the police in the course of prevention and investigation of crimes does in other words fall outside the scope of the Directive. Each country may decide that the Directive, wholly or partly, shall apply even to processing by the police, and regardless of area of application it should be expected that European national regulation of personal data processing – by and large – is in accordance with basic data protection principles – even within the police sector. Notwithstanding this, there is a rather marked regulatory boundary between regulation of personal data processing within the civil sector and processing within the field of police and public security. Briefly put, collection of personal data by the police originating from location-enabling technology in the civil sector implies transfer from a detailed regulated legal regime based on EU law to applicable national legal regimes, first and foremost criminal procedural legislation. On EU level it is in other words not possible to make general detailed analyses of the legal consequences regarding police acquisition of personal data from such systems.[134]

The second exception from the Directive which is of great importance to location-enabling technology regards processing of such data "by a natural person in the course of a purely personal or household activity", cf. article 3 (2). Location-enabling technologies may often be used for such activities. For instance, GPS is much used as integrated part of physical exercise (jogging) where the purpose is to track and measure the route (distance, speed etc.). In addition the GPS component may be combined with sensors to the person's body, measuring pulse frequency, caloric consumption etc. Similar devices could be used within a family/household to keep track of small children and people suffering from dementia. The Data Protection Directive does not apply as long as these activities are under

134 Passing of the proposed Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data {SEC(2012) 72 final} {SEC(2012) 73 final}, will change this situation but here we will not anticipate such amended legislation.

complete private control.[135] However, it is not trivial to decide the circumstances under which private control is sufficient to except the processing from the scope of the Directive. However, we take it that private use of GPS does not make satellite owners "controller" pursuant to the Directive and that private use of such devices are outside the scope of the Directive.

The documents we referred to under section 2.2 do not discuss the possibility that data subjects are controllers, i.e. determine "the purposes and means of the processing of personal data" (article 2(d)). The question is in other words to what extent it is possible that the roles of data subject and controller merge, so that service providers could be seen as processors on behalf of the data subject (instead of the controller)? Given the objective of autonomous data subjects, this possibility would be of special interest to investigate and define. For data subjects also to be controller, it would, probably presuppose full data portability, for instance that personal historical location data may be transferred from one service provider to another (cf. means of processing). Full portability may also prepare the ground for use of location data for new purposes (cf. the criteria of Data Protection Directive article 2(d)). Position as controller would probably also presuppose that data subjects have full competence to e.g. erase and correct data. In our view it would benefit privacy protection if these possibilities were discussed or decided on authoritative level, and these questions are particularly important to groups of location-enabling which is applied in the private marked within personal spheres.

Similarly, communication between members of the same family or household will be among the exempted categories of processing, at least if no one else outside the family has access to the data. The same presumption could be maintained regarding communication between a private person and things which he or she owns (P2T), and regarding communication between such privately owned things in a household (T2T). Data generated by positioning functions in the car[136] communicating with the access/lock system of the driver's home could for instance be considered as concerning purely personal or household activity. However, conclusions may only be drawn on basis of concrete assessment of each case.

Also, tracking data from a person's jogs during the last year which e.g. is transmitted through the GSM network and stored "in the cloud", will probably fall outside the scope of the Data protection directive because it is "part of this strictly personal or household activity". The condition is that the data subject determines

135 See, for instance the Lindqvist case. Specialized national legislation may regulate the activity, but this is a possibility that will not be considered in this discussion. If such devices are used by health and nursing services, kindergartens, schools etc, they are obviously within the scope of the Directive.

136 Together with geographical information, traffic information and personalised inputs.

objectives and means of processing.[137] In the Lindqvist case (ECJ, C-101/01) the court stated that "processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people" is clearly not activities which are carried out in the course of private or family life of individuals (47). Thus, it may be held that information made accessible within a limited number of people, and particular within a family, is comprised by this exception. A similar situation will appear in case of T2T mentioned above.

Notwithstanding the conclusions above, to the extent that data are transmitted by means of a public communication infrastructure (GSM, Wi-Fi/WLAN, Internet), the transmission may be subject to data retention pursuant to the Data Retention Directive and thus traffic data may be available to the police. However, in such a case the GPS based personal location data will probably be contents data (not traffic data).[138]

2.3.3 Personal data

The Data Protection Directive article 2(a) defines personal data as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". Here we will not go into the many questions of interpretation this definition embed, but will limit ourselves to comment on the element "relating to", i.e. the relation between a piece of information and the data subject.

When the location of a person is determined, information of his whereabouts clearly related to him. For instance data on sites, movements, time and speed could clearly be seen as personal data, at least provided the identity may be sufficiently established. However, each such location may be linked to lots of other data of that site, something which potentially may greatly increase the volume of personal data. The condition is that location data may be said to *relate to* a data subject.

For instance: GPS data may reveal that I am driving on E6 in Oslo, Norway, southwards at a speed of 90 km/hour, and location data may in addition show that the speed limit is 80, temperature is minus 10 degrees Celsius, the site is 234 metres above sea level, number of serious traffic accidents last year was 11, a tourist site is situated 543 metres on the left hand side of the road, etc. Moreover, almost every piece of this information mentioned could be expanded, at least by

137 In such a case the telecom provider and other service providers will be processors of parts of the processing.

138 But location data showing from where and to where GPS data were sent, will be part of retained traffic data.

adding historical and statistical data, plus possible events connected to the site or area where the site is. One of the important characteristics of personal location data is that they could easily be linked to general location data and thus to a very comprehensive body of relevant information. The fact that the basic personal location data is linked to general location data would imply that parts of the general data should be seen as personal (e.g. driving at 90 in a zone with speed limit at 80). However, all general data may hardly be seen as transformed to be personal: Historical data about the tourist site will for instance not be personal data pursuant to the Data Protection Directive. How do we draw the boundary line between personal and general location data?

The Article 29 Working Party has issued an opinion where this question is addressed; see Opinion 4/2007 on the concept of personal data. In the opinion the Working Party applies three guiding criteria for the establishing of this distinction:

> *In view of the cases mentioned above, and along the same lines, it could be pointed out that, in order to consider that the data "relate" to an individual, a «**content**» element OR a «**purpose**» element OR a «**result**» element should be present.* (page 10)

As demonstrated in the quote, the Working Party regards these conditions to be alternative. The content criterion constitutes the main type of relation and comprises information which describes a person or is "about" him. Where a person is, how fast he is moving, at what time etc., is clearly describing the person and these data are within the definition of "personal data".

The next criterion, purpose, is more problematic. Decisive here, according to the Working Party is whether or not "data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual." If general location data is used to assess if my driving is attentive, these data should in other words be considered as personal data. Thus, data showing weather conditions where I drive my car could be seen as data relating to me.

The criterion «result» may according to the Working Party be relevant if it is *likely* that data "have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case." They see it as sufficient that the individual may be treated differently from other persons as a result of the processing of such data. If we understand this correctly, general location data may be seen as personal data if for instance I drive in an area with high crime rates because this increase the probability that I will have special attention from the police.

These three guiding criteria imply a need to consider each concrete individual case; or as the Working Party states: "the question of whether data relate to a cer-

tain person is something that has to be answered for each specific data item on its own merits." Needs to carry out individual considerations are in one sense very sympathetic, but on the other hand extremely impractical. The answer to the questions of what should be regarded personal data is decisive for the establishment of obligations of the controller and rights of the data subject. These obligations and rights are linked to a certain type of processing thus, in many cases, a certain information system or other software and software-driven service. It would in our view produce inacceptable legal uncertainty if classification of data as personal should rely on individual assessments. Legal uncertainty regarding scope of privacy protection could in our view be regarded a privacy threat in itself.

We have no miracle solutions to these problems, but would argue that, as a starting point, primarily data *about* persons should be regarded personal data. We accept that this criterion is insufficient and is in need of supplementary criteria. These criteria should however relate to the *information system level* (rather to an individual level). One possibility is to include in the definition of personal data, every data which according to the design of the system, concrete arrangements are made in order to link data to identified individuals. Such a criterion would imply that it is up to the system designer for every information system to decide which data should be considered personal. A prerequisite would thus be that controllers have obligation to declare and make public the types of personal data which the system is designed to process. Since it is almost impossible to overview consequences of introducing such a general criterion, it is slightly more practical to introduce the "systems design criterion" as part of regulation of personal location data.

2.3.4 Identification

The Data Protection Directive regulates electronic processing of personal data. There is no doubt that personal location data processed with location-enabling technology as described in section 1.2 are processed electronically. It is however not obvious that all data are personal, i.e. "... relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly" (article 2(a)). With technometric technology, data is first and foremost linked to devices and objects, for instance smart phones, PCs, RFID tags etc. These devices are typically, but not necessarily, more or less linked to specific individuals. Smart phones will often be seen as very personal and will often contain private information regarding the owner of the phone and people close to him. Other technology use is much less personal; for instance, RFID tags to unlock *city cycles* which people can collect from a rack, could not be seen as linked to a person in the same way. Such tags do not hold sensitive information and people will not find it risky to lend the cycle to someone else (without RFID

registration on a new person). Even though it may be probable that it was the subscriber who unlocked the cycle from the rack, it is not at all certain that it was the same person who returned the cycle to another rack a day later. Thus, it is very uncertain if it was the subscriber who started at point A and moved to point B.

These two small examples should suffice to demonstrate that due to uncertainty regarding identification, for each use of technometric location-enabling technology, it must be considered whether or not processing of data represents "processing of personal data" and thus is within the scope of the directive.

The question of identification and the boundary between personal data and other data must as a rule be considered *on the level of information systems*, cf. "set of operations which is performed upon personal data" in the definition of "processing" in art. 2 (b). Thus, even though location data are regarded as personal data in concrete cases, the processing of data on information system level may be considered to fall outside this category. In the case of city cycles for instance, the overall picture may be that identification of users of cycles is too uncertain to be "personal data". However, this does not exclude the fact that in a number of concrete cases, it is rather certain who used the bike.[139]

The point here is that "personal data" requires a degree of certainty of identification. When the processing/system typically produce data below this limit (cf. the city cycle example), the system/data may fall outside the scope of the directive because identification is too unsure. This does however not imply that such uncertain data will be without interest to the police in cases of crime investigation and surveillance. On the contrary, normal situation for police work is processing of uncertain information which must be checked and used against other more or less uncertain information. If we compare the Data Protection Directive and normal methods of the police, there is in other words a difference of identity requirements: According to the Directive, there is a lower limit; according to police methods there are no absolute lower limit. The result is that data which falls short of living up to identification requirements of the Directive may still be sufficiently linked up to individuals to be of interest to the police. If data is not considered personal data pursuant to the Directive, this does not imply that no serious privacy concern exist when the police use this data. The mere possibility that a set of data relates to a certain identified person may cast suspicion on him and thus be experienced as a burden.

Situations where it is uncertain which person is linked to a set of data (cf. above) should not be mixed up with cases where a link exists but is protected and thus unavailable. The typical example might be situations where data are encrypted or made pseudonymous. It could even be that data are unavailable because of

139 Other sources of information, for instance data from a GSM system, combined with information from the RFID readers of the city cycle facility may establish the identity of the user of the bike.

technological obstacles of other kinds, for instance due to lack of competences, unavailability of technological formats and equipment to access data etc. In the civil sphere (outside police, defence etc.), such obstacles may be relevant for the definition of the lower limit of personal data. To the police, this will probably not have significance other that in exceptional cases. In the preamble of the Directive it is stated that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; "(26). If we suppose that data is accessed by the police from technometric location-enabling technology in the course of detection and prevention of serious crimes, it is likely that all existing means will be used to break protection of information on identity. Thus, in the hands of the police, such data will be personal even if they are protected by means of encryption, require of special equipment or competences or other obstacles.

With biometric location-enabling technology it should always be considered that identification of physical person will be possible and that the police always will have access to required means of such identification. With technometric techniques it will not always be possible to determine which person who have been connected to the object/device (cf. the city cycle example). It could for instance be unclear who of five possible people carried an object with an RFID tag. If such a situation is normal for the information system, the uncertainty regarding link between a specific person and the tag, could imply that the information in the tag is not considered "personal data". However we could normally suppose that the police will be able to establish identification of all possible individuals.

As we understand the Data Protection Directive, there are situations where it is doubtful whether location-enabling technology produces personal data. Moreover, the situation could probably exist that location data could not be classified as "personal data" when processed by service providers as controllers, because there are too uncertain links between data and person(s); while the same data may be reckoned as personal when processed by the police, because they have stronger means to establish these links.

With the great number of different systems and services which use and produce location data, it should in our view be discussed if the area of uncertainty regarding which personal location data falls under the definition of the Directive could be reduced. The aim should be to make it simpler to decide and thereby increase predictability both for data subjects and controllers.

2.3.5 Identification of controllers

In cases when the Data Protection Directive applies to processing of personal location data, there will be one or more controllers, i.e. organizations or persons responsible for the processing. Unless purpose and means of the processing is

established in national or Community law, controllers shall determine "the purposes and means of the processing of personal data" (Data Protection Directive article 2 (d)). If the processing is carried out in a chain of services where several actors take part, there will often be a controller for every service / part of the processing.

In opinion 13/2011 the Article 29 Data Protection Working Party discuss geolocation services on smart mobile devices on basis of a chain of processing involving up to three types of controllers:

I. provider of the geolocation infrastructure,
II. provider of applications and services and
III. provider (developer) of the operating system.[140]

Here, we will not go into detail regarding why and how these types of controller functions may appear, but some further explanations will follow from the examples below. The main point we want to make is that there will often be more than one type of controller in each chain of processing of data, and thus more than three controllers involved in the use of each application where personal location data is included. Starting with the infrastructure, we may use the example of a car equipped with RFID tag to register that a suitcase with drugs is removed from the car. This data together with data on time, place and temperature is transmitted via the GSM network for further processing. Since the location shows that the car is on the home address of Ms Illness, these are personal data about her.[141] These personal data are sent to and processed in a medicine prescription system together with data on weather forecast, pollen forecast, medical information on Ms. Illness, and the result is sent back to the nurse for execution. To make the example complete, the provider of the operating system of one of these system modules could contain an advertising application offering holidays in "pollen-free" destinations. The point here is to illustrate how end-services may rely on several providers of services (regarding weather, pollen, medicine).[142] Each provider will expectably be controller of personal data processing in their part of the service chain, and each controller will process personal location data.

Services where location is an element may be highly integrated and automatically controlled. Thus it will be difficult for users to understand who the controllers are and what role each of them play. It will most likely be a problem to identify how responsibilities are shared, which personal data are processed and how data may be accessed; or as the Article 29 Data Protection Working Party puts it in opinion 13/2011 regarding data on geolocation on smartphones: "One of the great risks is that the owners are unaware they transmit their location, and

140 See page 12 – 13.

141 In addition, it is also personal data about the home nursing service officer who drives the car.

142 The extent to which various service providers need personal data relies on the design and function of the system and the extent to which it is based on a privacy-by-design approach.

to whom" (page 19). In criminal cases, it follows that it may be difficult to identify relevant controllers for services used by people who suspect they have been near a crime scene and who therefore want to access their data and map exact time of their whereabouts. It may, even to the police be difficult to overview which systems could contain relevant information. Note in particular the point made by the Article 29 Data Protection Working Party in Opinion 02/2013 that there are many players in the app development landscape and that they operate globally (page 5). Apps often process personal location data. Such service providers may be among the most valuable sources to the police, because data on location/time and other derived information (route, speed) may be combined with other data.

Regarding the challenge for the police to acquire an overview of relevant location-enabling technology/service, at least three situations should be addressed:

1. Situations when information about relevant controllers could be found because they are registered by public authorities. Telecom authorities will for instance have full information of providers of GSM services in a certain area.
2. Situations when personal location data from a service are stored in the data base of several service providers (controllers), but information about relevant services and controllers is not comprised by a registration arrangement. Location data from such services must in case be mapped as part of e.g. police investigation.
3. In a third type of situation, personal location data are only stored on personal devices (and not on databases of service providers). If so, police may wish to access each personal device, but will probably not have information enabling them to identify people that might have data of interest on their device.

The first situation will probably be satisfactory to the police.[143] In the second situation, our data presented in Part I indicate that there will be no central overview of services based on for instance Wi-Fi, RFID and GPS, and thus service providers/controllers may be hard to identify. It is of course possible to make such surveys, but establishment and maintenance of this information will probably imply high cost. Registration arrangements will of course be even less realistic in situation 3 (with personal location data only on personal devices).

With the aim to balance privacy protection against police needs of collecting information in the course of crime investigation, an obvious possibility is to recruit as many people as possible with location-enabling technology which for instance have been nearby the scene of a crime. This could for instance be realized by urging people with location-enabling devices in the right area and time to contact the police. Peoples' knowledge of relevant services and devices may possibly

143 If this is thecase, they need authorization from the court or from a high police official in order to access data from relevant GSM providers.

be supported by means of a "location management app".[144] One central function in such an app could be identification of controllers with contract information.

2.3.6 Legal basis of processing and information to the data subject

Article 7 of the Data Protection Directive qualifies certain legal bases of processing. Consent is one alternative and other alternatives are linked to what is regarded necessary for purposes and situations mentioned in the provision. It is up to each controller to consider which legal basis is necessary for the processing to which he is responsible, but the supervisory authority may control and review this decision. Here, we will not go into the various alternatives of art. 7, but only establish that consent and consent-like alternatives often will be legal bases in cases of location-enabling technology.

By "consent-like" we refer to alternative (b) and cases when 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". Similar to situations where consent is only given to process personal data, these contractual situations implies that the data subject accepts terms of the contract, included necessary handling of information to implement it (or entering into it). However, in these situations the Directive does not specify any requirement regarding how acceptance should be given. There are requirements regarding information from controllers to data subjects when personal data are collected from the data subject (art. 10) and when data is collected from other sources (art. 11). Information should comprise the identity of the controller, purpose(s) of the processing and "any further information ... in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject."

The possibility that personal data is transferred to the police may have significance for such fair processing, and we may ask if further information should comprise information regarding rules of the relevant criminal procedure legislation. In such a case, this may educate and create awareness among users of location-enabling technologies. On the other side, this information will not be directly relevant to the great majority of data subjects, and it may thus be rather annoying to receive this information every time data are collected. Communication of general information to the public may therefore be a better idea.

Obligation to inform the data subject is formulated in a highly discretionary manner and requires concrete considerations: "having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject". The mere possibility that personal location data is

144 See section 2.3.10 (below).

turned over to the police does not create any obligation to inform. However, if police make use of personal location data rather frequently, this will probably imply such an obligation. For instance, the Swedish secret police SÄPO, is negotiating with Swedish telecom companies to allow automatic collection by the police of retained traffic data, including personal location data.[145] The precondition is (as now) that police access data on basis of a court decision, and superficially viewed the reform is about a faster collection of data than with today's more manual routines. Here we will not discuss possible effects of such a direct access. However, if collection of personal data to the police is embedded in an automatic routine as described, this will most likely trigger an obligation to inform data subjects.

The legal basis of police's collection and further processing of personal data must be clearly stated in legislation or other clear expression of the law, cf. ECHR art. 8 (2) and "in accordance with the law". Most people do not read laws and a formal legal basis does thus not necessarily imply that data subjects are informed. Information to data subjects by means of consent and by requiring that information should be given by controllers to data subjects implies far better ways of creating clarity. Compared to situations when personal data are exchanged within the civil sector, it may be asked why it is justifiable to give less general information to data subjects about the possibility that the police collect personal data from controllers in the civil sector. Obviously, in order avoid revealing strategies and methods, the police have an interest in keeping concrete collection of personal data secret. Likewise, the police have probably legitimate grounds not to reveal details of how they analyse data. However, plain information that police may have court permission to collect and analyse personal location data from e.g. telecom service providers should obviously be openly available.

One possibility to create sufficient transparency is to develop a small legal information tool available through use of location-enabling technologies. The tool could for instance be an app providing general information regarding the legal framework for collection and interception by the police of personal location data, see section 2.3.10.

2.3.7 Purposes of processing

Personal data processed by means of location-enabling technology must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes" (Article 6 (b)). There are no limits regarding numbers of purposes linked to each type of processing, and as our brief discussion regarding controller illustrates, there may be several controllers in-

145 See Svenska Dagbladet, Wednesday 19 November 2013 (http://www.svd.se/nyheter/inrikes/sapo-vill-komma-at-data-direkt_8740078.svd).

volved to produce desired results. Thus, altogether, there may be many purposes connected to the production of each end-service. Purposes must be specified for each type of processing, i.e. on the level of the relevant information system. Controllers must notify the supervisory authority before carrying out automatic processing operations intended to serve such purposes, and purpose is among the types of information in the notification to the data protection authority.[146] It follows that purposes must be established *before* processing of location data starts.

Regarding processing of data from location-enabling technology, purpose of processing is of special interest in at least two situations:

- Before a data subject begins to use a location-enabling technology (prior to installation of software, before entering into service agreements etc.), and
- Before the police collects location data from software and services mentioned in the first bullet point.

Regarding the first bullet point, even if personal location data are incorporated in the data processing, localization and tracking is often not a purpose of the processing. When RFID is used as part of a payment procedure, or when biometric access control to a building is performed, the purpose is obviously respectively payment and access control. Thus explicit statement of the purpose will in these cases not necessarily reveal the fact that personal location data are processed to produce services, or that software functions which supports the declared purpose make use of such data. However, in our view, even when localization is not the purpose (but a function) it should always be seen as important and something which concerned data subjects should be expected to have an interest in. Data Subjects may of course inform themselves of localization functions by applying their access rights, but the necessity of requiring access should be seen as representing an unnecessary threshold. Alternatively, data subjects could be informed that location is established and processed as part of the production of a service.[147]

Use of location-enabling technology in civil society will often be based on consent and contract, and all purposes of the processing must be part of the information given as part of the procedure of acceptance. Even though we may not exclude the possibility that it may be legitimate for the controller to specify a purpose related to crime prevention and reporting of suspicious personal data to the police, this will probably be a very rare situation. Most purposes will be linked to the main result produced by the location-enabling technology, for instance access control, payment, navigation, tracking of things and persons etc. – and not

146 See Data protection directive art. 18 (1) and art. 19 (1) (b).

147 Cf. Commission Recommendation regarding RFID and Privacy and Data Protection Impact Assessment Framework for RFID where it is stated that "operators develop and publish a concise, accurate and easy to understand information policy for each of their applications," and where information if the location of tags will be monitored, is one of these information requirements.

to policing. Therefore, the normal situation will be that personal data may not be transferred to the police with reference to a specified purpose which the data subject has accepted.

Instead of referring to purposes of processing, the police will need a special legal basis. Such legal basis for collection of personal data as part of investigation will be found in the criminal procedure legislation of each national legal system. The notified purposes of personal data processing linked to location-enabling technology will in other words normally not have any significance for police access to these data, and possible access by the police will not be visible for the data subjects through consent procedures.

2.3.8 Data quality

Data Protection Directive article 6 (1) (d) stipulates that personal data should be "accurate and, where necessary, kept up to date". To attain this "every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified". These quality requirements shall be established "having regard to the purposes for which [the personal data] were collected or for which they are further processed". For every application and service using location-enabling technology where personal location data are prior and critical, this provision implies that accuracy and updating of data should be optimal. If you equip an employee carrying out dangerous work alone with positioning and tracking technology in order to find and rescue him if an accident strikes, it is obviously hard to argue that location data should be approximate. If the aim is to have attention where a person suffering from dementia is, it would in contrast often be sufficient to assure that the person is within a certain area.

Accuracy and updating frequency of location data will often depend on the technological system. Accuracy of localization by means of GSM networks will for instance first and foremost be the result of GSM network coverage, capacity etc. There are reasons to believe that coverage and capacity of location-enabling technology will increase and thus produce more and more precise and updated data. It is hardly imaginable that legislation will limit the degree of preciseness and update frequency of such systems, based on arguments to protect personal data. The most realistic presumption to make as basis of privacy impact assessments and legal political considerations is probably that future location-enabling technology as a rule will produce personal location data with high quality, without interruptions due to "GPS shadows" etc.

2.3.9 Access rights

The Data Protection Directive creates openness by giving access rights to data subjects (article 12(a)) and by establishing duties for controllers to inform data subjects (article 10 and 11). Basis of both these regulatory techniques is that data are under the control of controllers, and thus both types of openness presuppose that the controller takes active part in order to make information available. If the aim is to create openness, this is of course not the only possible way of organizing data. One alternative is that data subjects are given *direct* access to data about themselves, without the direct mediation from the controller.

If we apply direct access in the area of location-enabling technology, there are at least three types of situations which should be considered, of which the first two involve technometric technology, cf. section 1.2. First, we have the situation where personal location data are produced by, stored in or connected to a device which is at the disposal of the data subject, and which have a display or other means to expose information. Important examples are smartphones, PDAs, personal GPS-based devices (for training, path finding etc.). Here, the expectation in the great majority of situations will be that there is no reason why location data should not be directly accessible (without request) for each data subject.

The second type of situation is where location data are produced by, stored in or connected to a device which is at the disposal of the data subject, and where the device *does not* have a display or other means to expose information on the device. Examples are RFID tags (tickets, keys, passports etc.). In these situations, direct access to location data could be arranged by making available readers which each data subject may use freely and on their own initiative. Readers could e.g. be installed on places of service, for instance toll stations, premises of the key system, customs control areas etc.). Parallel type of systems is common in e.g. bookstores where bar code readers are made available to make price information available to customers.

The third type of situation is when data subjects do not use any type of object they carry, but are recognized and located by means of biometric techniques. In these cases processing of data will often have other legal bases than consent; typically because the aim of the system is to secretly monitor and locate specific individuals. Thus, in this third group it will normally not be feasible and desirable to let data subjects have direct access to location data about themselves, and in many such cases right to request access and to receive information from controllers are limited or non-existent.

Direct access for data subjects in the two first situations mentioned above may very well fit with a privacy-by-design approach. Ultimately, it is quite possible to imagining legal requirement of direct access function as part of technologies as mentioned in situation one and two. Regarding the first situation (smartphones, PDAs etc.), direct access functions will in many cases be easy to realize and is first

and foremost a question of programming and setup of the software. The least powerful way of applying privacy by design is to call on (or even oblige) developers of location-enabling services to include direct access features in their product.

2.3.10 Conclusion

Below, in section 3.2.2, we conclude that personal location data is a category that should have stronger protection than "ordinary" personal data. Given this apprehension and considering the emphasis by regulators on privacy by design,[148] we would argue that it should be considered to introduce "location management apps", or in other words small computer based services which manage location-enabling technologies and give users critical information to help safeguard privacy. Such apps should as a minimum inform the user of the services on each device which have localization functions; the purposes which these functions support; the legal basis of processing; and statistics regarding acquisition of location data from the service the government authorities, for instance the police, customs, tax authorities and others. It should in addition be made available coordinated information regarding collaborating controllers and processors, and whether or not the controllers reckon the processing to fall under the Data Protection Directive.

Here, we will not go in further detail regarding what such apps could contain and how they may be designed. In the last element regarding information of controllers, processing of personal data etc., lays the important point that such information should refer to obligations for controllers to clarify and inform of certain (assumedly) hard legal problems: In sections 2.3.2 to 2.3.7 we have discussed selected legal problems related to personal location data. Our simple point is that controllers should have obligation to decide about these questions and inform the users by means of the location management app in a standardized way. For instance, when controllers and processors operate in a chain to produce a service, these relations should be established in explicit ways (e.g. agreement) and users should be informed, for instance included one piece of contact information to which every communication to collaborating controller and processor could be directed. Information could also concern applicable law and relevant control authority etc., and could when appropriate partly be based on symbols and visu-

148 See Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data {SEC(2012) 72 final} {SEC(2012) 73 final}, article 23.

als similar to what has been suggested as part of the proposed Data Protection Proposal, article 13a about standardised information policies.[149]

Another important point is that location management apps should be designed and described in standardised ways, something which will allow automatic identification and analyses, both by data protection authorities and the police. One effect could be easier controls and review of controllers' legal interpretations as expressed in the apps; another effect is easier overview for the police of location-enabling services and systems which could be of use for police work and accessed pursuant to court order.

149 See proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)).

3 Proposal for an individual rights impact assessment model

3.1 Reflections regarding PIA as method in this work

As starting point this chapter will be based on the definition of Privacy Impact Assessment (PIA) in Raab and Wright 2012:

> *A privacy impact assessment is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts.*

The following assessment could not be said to concern *project, policy, programme, service, product or other initiative,* as mentioned in the citation above. Still, we see the enumeration of subjects to assessments as incomplete. Thus, the definition could be extended by for instance adding a type of technology. Below we will be "*assessing the impacts on privacy of location-enabling technologies which involves the processing of personal information*", *cf. Raab's and Wright's definition.*

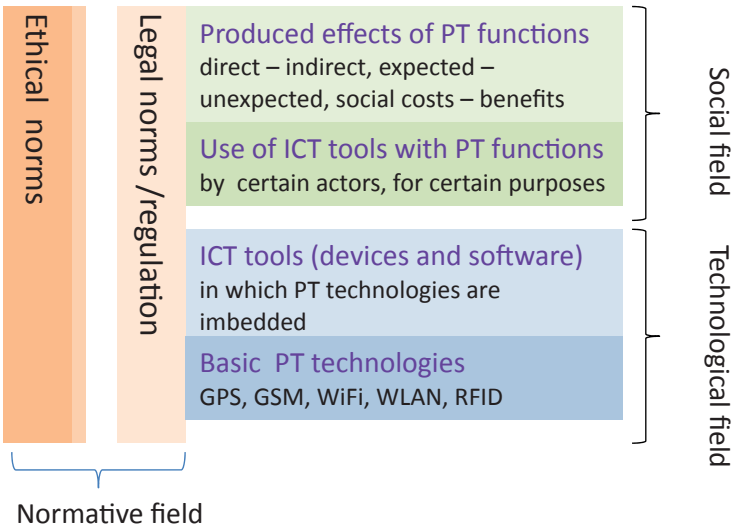


Figure 2 Overall model of technological, social and normative aspects of location-enabling technology

In D1 we made distinctions between four layers in order to describe the domain of RESPECT WP7. The two first layers contain mere technology. PIA of technology alone will in our view not be meaningful, because impact assessment would require some sort of application in a social context. Thus, the following impact assessment will have its point of departure on the third layer; cf. "Use of ICT tools with positioning and tracking functions" in Figure 2. Our approach is broad and thus all actors and purposes as included in this layer could realistically not be determined. In civil society there is a variety of actors using technologies with localization functions and which are generating personal location data that police may have an interest to collect and process further as part of police work. Although localization is integral parts of the processing of these other actors, their purposes may for instance be payment and access control (and *not* localization as such). Without restricting the scope of the following discussion, it is thus not possible to fix deliberations to specific actors with specific purposes in civil society. The situations on which we base our discussions are therefore less specific than what ordinarily should be expected in an impact assessment.

Impact assessment of location-enabling technology should also give room for considering effects of future emerging technologies. There is no need to speculate regarding detailed future technological solutions; what is important in our context is what the technology basically does (regardless of specific type of basic technology). Our simple assumption is that there are great needs both in civil society and within the police to link personal location data to processes, conditions, actions, events etc., and that several technologies may produce such data. Today, many technologies may help generate personal location data (in particular GPS, RFID, Wi-Fi, WLAN, GSM, Bluetooth, ultrasound, ANPR, CCTV etc.). Without doubt, we will be having technological shifts where some of these existing technologies will be developed further, others will disappear and new technologies will be introduced. However, in the perspective of privacy concerns and of legal protection in general, the technology itself is hardly important, but the potential functions of applications are crucial. Given pronounced needs of positioning and tracking functions chances are high that it will be imbedded in future services and devices. We hold it to be most probable that such functions will be even more effective and widespread than today, and provided sufficient legitimate grounds exist, these functions will be allowed and will produce an even greater supply of personal location data than today.

Our discussion of impacts and remedies on a general level will concentrate on what we see as "ideal" trade-offs between privacy and legal protection concerns on the one hand and concerns regarding fighting serious crime on the other. "Minimise negative impacts" in the above referred definition seem to presuppose that privacy is something that gives arguments for modification of a given proces-

sing of personal data designed without regard to privacy. Understood in this way, PIA does not embody privacy by design, or privacy by design becomes something which "repairs" an unsatisfactory design. In contrast, we will seek to support the invert approach by setting privacy concerns in front and then discuss whether or not it is necessary to modify in order to make police work more efficient. This does not imply that privacy is given priority, but represents only an approach where we try to introduce privacy concerns in a way that increases the possibility that they will have effect.

A privacy impact assessment will in many cases have a precautionary and predictive appliance and this ought to be the main perspective when processing of personal data is considered. The aim is in other words to become aware of undesirable effects on such an early point of time that such effects could be avoided or mitigated. The same assessment elements would in most cases also be relevant and useful in retrospective, for instance as part of evaluation of processing that have been carried out over a period of time. Even this perspective is included in our approach.

Privacy impact assessment is obviously about privacy, and privacy is a rather broad problem field. In the RESPECT project privacy concerns is partly analysed within the context of law enforcement, i.e. within an area where privacy infringements may be required in order to collect evidence as basis of e.g. prosecution and sentencing. Personal location data is possible evidence and may be basis of imprisonment. Because our basic assumption should be that we first and foremost should presuppose serious crimes, the perspective should be that collection of personal data as evidence could lead to long sentences. This should in our view also lead to attention regarding *legal protection in more general terms*.

Privacy protection is of particular importance for fractions of the population which are affected by police work without being guilty in any criminal act. Because collection of information of suspected persons easily also will imply collection of personal data of family members, friends, colleagues, neighbours and others with which the suspect has social relations, special attention should be given to people with close relations to individuals under suspect.

During police work prior to trial, due to the presumption of innocence, one cannot set aside the privacy of *any* individual. Our point is that we need to take legal protection under consideration at an early stage of collection and processing of personal location data and in principle to the date of final and enforceable judgment. Even though only a small fraction of personal location data will be accessed by the police, it is in our view required that such data are always processed *as if they will be used in a criminal procedure*. Application of the adversarial principle and protection against self-incrimination may e.g. probably be best realised if unreliable data with insufficient quality is avoided.

It follows from the observations mentioned above that assessments should not only relate to privacy principles, but take other fundamental rights and legal principles under consideration as well. However, there are hardly any need to make strict distinctions between privacy theory and other relevant theory regarding protection of individuals. We will not assess impacts on the basis of a full list of privacy principles and principles within criminal law and criminal procedure law etc. Instead we will limit discussions to a selection of principles that we find sufficiently relevant. Moreover, assessments should not only be based on established principles and reflect established legal categories and views, but in addition allow new and less developed considerations to be made: Developments of technology and use of technology require renewed legal reflections (although parts of this may imply trial and failure).

WP7 of the RESPECT project is about application of personal location data by the police and thus it may be expected that assessments should be limited to processing of location data by the police. Collection of personal location data from the many and increasing number of sources of such data in civil society makes this a too limited approach. We regard it necessary to assess the whole chain from processing of location data by private and public parties as part of everyday doings to processing of such data by the police. This is not to say that we should expect large scale collection of such data by the police picturing everyday life of citizens. On contrary, the typical expectation in democratic societies under rule of law should be that police collect and process location data from civil society systems only when this is necessary in a democratic society for police work with serious crime, and only to the extent that it is proportionate in view of conflicting rights and freedoms.

We have chosen to carry out the assessment in two parts: First, we assess elements which we believe are of general importance, both from the perspective of privacy protection and legal protection in general[150] (section 3.2), while in section 3.3 our assessment deals with elements which may be seen as particular to processing of personal location data by the police. We refer to this broadened assessment as *individual rights impact assessment* (IRIA).[151] Suggestions of typical weight will be included in the conclusions regarding each element. Our approach implies that processing of personal location data in civil society should be assessed on basis of the elements in section 3.2, while processing by the police should *in addition* be assessed in the light of elements in this and next section.

The ambition of the individual rights impact assessment below is to express possible and typical impacts by means of subcategories, each for which we assign a value. By designing an assessment scheme our objective is to prepare the ground

150 Cf. first and foremost criminal law and criminal procedure law.

151 In other words, what we designate individual rights impact assessment comprises both assessments in section 3.2 and 3.3.

for future impact assessments of concrete services and devices. This scheme both suggests particularly relevant characteristics of location-enabling technology and their expected weight, seen from the perspective of protection of individual rights. Sum of values indicates the seriousness of possible impacts for such rights.

The scheme we suggest has, of course, several limitations. First, we are not claiming that our list and description of impacts is in anyway complete. Thus if required it may/should be extended. Because the scheme is result of both results from D1 and D2 of RESPECT WP7 and of relevant policy documents and regulations, we do, however, believe that in many cases our selection of impacts represents elements of particular importance. We therefore believe that in many cases the suggested scheme would be sufficient and that supplementary assessments first and foremost are required if assessment according to our scheme gives indistinct results.

3.2 Assessment elements with general relevance

3.2.1 Introduction

The following discussions of impact elements concern first and foremost questions which could be classified as privacy and data protection. We mainly relate deliberations to existing legal principles and regulations on European Union level, but add other legal-political considerations. Conclusions are not about what is needed to comply with existing legal requirements, but indicate what should be recommended when protection of individuals is considered.

3.2.2 Sensitivity and privacy exposure

Personal location data is not among the special categories of data regarded as generally sensitive as identified in the Data Protection Directive art. 8(1); i.e. personal data that is revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Thus, the basic conclusion is that personal location data is not generally sensitive.

However, sensitive data may be "constructed" by combining several non-sensitive data, for instance if a location-enabling service links to other pieces of information found in co-functioning systems. In GPS based maps, *coordinates* showing where a person is may for instance reveal sensitive information because they are linked to addresses of for instance a hospital, medical office, church and similar sites. On the other hand, only a tiny number of coordinates are linked to sites which could be associated to the types of personal data which are regarded to be sensitive. In a legal sense, the mere possibility that there is concurrence

between a position and e.g. a hospital does not make location data sensitive. However, if location-enabling technologies are *designed to particularly target sites which are linked to sensitive data*, the conclusion may easily be different. For instance, an emergency app designed to locate and rescue people who have fallen ill or are injured, may be seen as processing sensitive data even if sensitivity is only revealed by a combination of non-sensitive data (e.g. the information that person P has been staying for two days on an address where there is a hospital).

Location could be seen as possible entrance to almost every kind of other information, and location increases the usability and importance of these other types of data. Thus, there is a clear difference between use of location-enabling technologies which is restricted to presenting basic position data and technologies which adds or facilitates to add information about activities, forthcoming and historical events, property information, social information etc. to the locations.

In concrete services/functions based on location-enabling technology, coordinates and other information about sites will not necessarily be directly exposed as part of application, or this information may be very limited. However, personal location data is always combined with time stamps, and may almost always be connected to a very large spectrum of other data; both personal data and general data connected to the location. All together, this may create a complex information context to the limited information on coordinates etc. Coordinates and addresses are excellent means of linking information, both because these data are used to identify other types of information on locations, and because almost all locations may be linked to names of individuals, national identification numbers and other means of personal identification.[152]

Given the nature of current technology and development of technology, there is no reason to place emphasis on the fact that systems/services/functions are formally distinct from each other. A realistic approach for the future is that services will often allow great amounts of information on each location to be connected. Returning to the example where a certain position shows presence at hospital H1; given the identity of the business, there may be a lot of other information available about this hospital, of which some will add to the picture drawn of the data subject, and others giving context information: The hospital is a private abortion clinic, the clinic is owned by P which also owns hospital H2 where the data subject was present on date D1 and D2 for a certain amount of time, and H2 has been under police investigation, *etc*.

Equally important; if we consider possibilities of linking other data to a certain position, we should not limit ourselves to examples where a location directly reveals sensitive data (e.g. because it is the site of a hospital). It may just as well be that an "innocent" location, when combined with other information, identifies a

152 At least owners and usufructuaries.

place which reveals sensitive data. Several sources of data may for instance reveal that a certain site (an apartment) has been scene of a serious crime, where the convicted criminal lives after expiation together with identified family members.

On basis of these descriptions, a reasonable conclusion could be that location-enabling technology and personal location data represents great possibilities to reveal sensitive data, both directly and indirectly, and in particular if combined with the many types of other information that could be linked to locations. The probability and extent for this to happen is basically uncertain, but the potentials are in many situations considerable. Given this insight, in a legal-political view, there may be reasons to reconsider what could be seen as grounds for assessing data as sensitive.

The general regulatory approach of the Data Protection Directive and other relevant legislation is to a large extent based on the assumption that processing of data is carried out within the framework of information systems which have specific controllers, used for specific purposes etc. Of course, it is recognised that systems interact; that controllers collaborate etc.[153] Our point is however that systems may interact with other systems in a seamless and automatic way, turning it into an *information infrastructure* rather than being separate information systems. If sensitivity of personal location data is considered with the infrastructure perspective, the subject-matter we assess will be hard to describe with sufficient certainty and credibility because we are in the open environment of infrastructures where actual information patterns may be hard to predict.

Personal location data may have indirect effects on other fundamental rights such as the right to free movement,[154] freedom of thought, conscience and religion[155] and freedom of assembly and association.[156] The primary reason is the possible chilling effects from the fact that location data may reveal political, religious and philosophical opinions and actions. Possible indirect effects on other human rights may support the idea of location data as sensitive.

Even though personal location data may not be linked to information of traditionally sensitive character, aggregation of "innocent" location data may be regarded sensitive in a popular sense of the word, because it may give a very detailed picture of the daily life of each person, documenting whereabouts and hours, and thus indicating actions, habits, preferences, relations etc.;[157] a sort of *constant*

153 Cf. proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), article 4(5) which defines "controller" as a role carried out "alone or jointly with others".

154 Cf. TFEU art. 21 (1).

155 Cf. ECHR art. 9.

156 Cf. ECHR art. 11.

157 See ARTICLE 29 Data Protection Working Party, opinion 13/2011 on Geolocation services on smart mobile devices.

profiling. A person is always somewhere at a certain hour, and seen in this way, location-enabling technology ultimately have the potential of indicating every aspect of life during a lifetime. The current number of applications using such data and the fact that future potentials of location data are great makes it probable that the insensitivity of registration and further use of personal location data will continue to grow, and that use of several, parallel sources of information on people's whereabouts will be rather common.[158] Moreover, to the extent that we sum up all location information related to all/many individuals within a defined area, personal, social, economical, and consumer patterns etc. will be revealed, making it possible to analyse each individual in a societal context.

So far, we have discussed whether personal location data is *generally* regarded to be sensitive, cf. Data Protection Directive art. 8(1). Concrete opinions among citizens of needs for protection could of course deviate from this general classification, and personal views of data subjects could be that data on their financial circumstances, their whereabouts or other types of data are equally sensitive as those identified in the Data Protection Directive. In addition, in concrete cases almost any type of data may be regarded sensitive when it is matched with other data. Location is very often one important ingredient of such concrete assessments of sensitivity (someone has been on the wrong place on the wrong time). Such individual and situational assessments of sensitivity may of course not be basis for classification of what should be regarded sensitive in legislation, but may still be relevant when the sensitivity of personal location data is assessed on general level.

If we consider the sensitivity of personal location data as the basis for conducting an individual rights impact assessment, we really have two basic choices. Either we stick to the information system perspective and carefully examine each application of location-enabling technology in order to consider whether or not a certain type of device/service yields data which may reveal circumstances as indicated in Data Protection Directive art. 8(1). This will leave us in a situation with basic uncertainty because possibilities of linking to other data are many and hard to assess; and we will be in constant doubt regarding where boundaries should be drawn. Thus, even small developments of existing services could be grounds to reclassify. The other approach would be to change to an information infrastructure perspective and presuppose that geographical information will almost always be possible to link up to a variety of other information, making it almost impossible to say something in advance about the sensitivity of these combinations.

We have argued that given the infrastructure perspective, assessments of sensitivity of personal location data "dissolves" into over-complexity and uncertainty:

158 For instance four sources of personal location data linked to cars: GPS anti-theft device, GPS-based maps and traffic information device, RFID toll road payment device and GSM telephone service activated.

Location data will sometimes be directly sensitive, sometimes indirectly sensitive (because of general available possibilities to combine data), and sometimes because location data is assessed as sensitive in concrete cases. It may be claimed that altogether this supports the idea that location data should be regarded as sensitive.

The sum of possibilities mentioned above could be argument for supplementing the traditional sensitivity assessment (regarding revelations of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life). Alternative to assessing if concrete processing of location data may reveal such information, it may be claimed that the probability that it does may be so high that, in a general sense, personal location data should often be regarded sensitive by its own.

Possible consequences of classifying location data as sensitive

Even if we conclude that personal location data should be regarded sensitive, this would not necessarily lead to the conclusion that such location data should be subject to prohibition of processing unless certain conditions are met, similar to Data Protection Directive art. 8(1) cf. (2). In the future it should be expected that location data will be part of a great number of processing, and we strongly doubt that requirement for data subjects' consent and identification of "necessary" purposes and grounds in all these everyday situations would add much positive to the protection of individuals concerned. Instead, other safeguards should be considered.

In the last available version of proposal for Data Protection Regulation,[159] three provisions exemplify that *location data* together with data on children and employees are added to special categories of personal data as referred to in Article 9(1).[160] Within the following three areas, we understand this as giving location data an *equal status* as general sensitive data in art. 9(1):

- Representatives of controllers not established in the Union (art. 25 (2)(b))
- Risk analyses (art. 32a (2)(b))
- Designation of data protection officer (art. 35 (1)(d))

The fixed wording of these provisions is: "... processing special categories of personal data as referred to in Article 9(1), **location data** or data on children or employees in large-scale filing systems …" (bold added).[161] Similar regulatory strategies could of course be pursued with respect to other aspects of privacy protection, and classification of location data as sensitive could instead of regulations

159 As agreed 21 October 2013.

160 Similar to Data Protection Directive art. 6 (1).

161 This phrasing is used in different contexts, both positively put and with prior negation. However all three examples clearly strengthens the protection of data subjects.

like in Data Protection Directive art. 8(1) cf. (2) lead to other safeguards similar to those exemplified above.

Possible subcategories of sensitivity and their weight

In the discussion above we concluded that personal location data should be regarded as generally sensitive by its own. This does however not imply that sensitivity should be assessed in the same way regardless of how these data are used. We will suggest the following subcategories:

1. Location-enabling services have functions which link location to data which directly reveal (traditionally) sensitive data as specified in Data Protection Directive art. 8(1) cf. (2). Suggested weight: 4.
2. Location-enabling services have functions which facilitate linking of personal location data to other personal data. Suggested weight: 3.
3. Location-enabling services have functions which facilitate linking of personal location data to other geographical data. Suggested weight: 2.
4. Location-enabling services do not have functions which facilitate linking of location to other types of data. Suggested weight: 1.

The four subcategories reflect a traditional approach to sensitivity in the sense that most weight (4) is assigned positioning and tracking functions which yields information directly revealing the special categories of data as established in Data Protection Directive art. 8(1) cf. (2). Examples are applications directly revealing that a certain position is a church, hospital, site of demonstration, etc. (e.g. various types of map services). What seems to be the dilemma here is that such functions probably will be even more common and have obvious applications which will be desired by a great number of people. It must, however, be remembered that classification of data as sensitive does not presuppose any prohibition against use, and is only one element of a total individual rights impact assessment. The final assessment would thus rely on a combination of several assessments. Thus, at the end of the day, personal use of positioning and tracking functions assigned top sensitivity (cf. above) will all in all receive much lower rating than use of the same function by others against the data subjects' own will.

The categorization above is based on the general assumption that combination of personal location data and other personal data about the same person typically will generate more sensitive results than combination with geographical data. By geographical data in category 3 is meant everything from topography and speed limits to information of addresses, descriptions of businesses and functions etc. on addresses and other geographical sites etc. We consider that functions are facilitated for a certain type of data, as mentioned in the subcategories, if it is described how to carry out necessary operations.

3.2.3 Autonomy of data subjects

In D1 of WP7 we classified four types of situations to capture the degree of autonomy and voluntariness for data subjects who use location-enabling technology. The following groups were suggested:

- People having competence to exercise autonomy and who are in a free situation to make independent choices.
- People having formal competence to exercise autonomy, but do not find them in a position to make (totally) free choices due to social and economical effects.[162]
- People having formal competence to exercise autonomy but are not in a situation to exercise it (cognitively and otherwise).[163]
- People not having competence to exercise autonomy and therefore have in this respect no freedom to decide.[164]

In the following we will build on and rephrase the main elements of this categorization.

Autonomy of data subjects may be seen as a fundamental privacy principle. There are of course both legal and factual limitations to this principle, for instance concerning personal location data. One central example of legal limitation is the Data Retention Directive art. 5(1)(f) which establish an obligation to retain personal location data without regard to the opinion of data subjects. As we understand today's situation, requirements to retain personal location data is dependent on the type of technology which generate these data. Unless linked to publicly available telecommunication services/networks, RFID-based systems will for instance not be under the obligations of this Directive.[165]

It goes without saying that possible extended obligations to retain personal location data will have negative effects on privacy, and we will not go into discussions of possible remedial actions if that should happen. Even if formal limitations of data subjects' autonomy (like in the case of data retention) is crucial for an individual rights impact assessment, limitations of data subjects' self-determination due to factual and societal circumstances (not only legal) are probably just as important and will be emphasized in the discussions below.

162 Employees may typically find themselves in this situation.

163 Senile people who have not been placed under legal guardianship, plus certain other groups of hospitalized people who temporary are incapable of exercising their autonomy.

164 People under legal guardianship is one example, another is people in custody etc. Children under the age of 18 partly belong to this group, dependent on age and maturity.

165 Cf. article 1. It is of course quite possible that retention obligations may be introduced in other fields of society, and given the grounds for existing data retention obligations, it may in principle seem inconsequent if some types of location data are not included in such an obligation.

In D1 we have underlined that technometric location-enabling technology is used as integral part of many services, i.e. the position of various devices and objects which are closely linked to data subjects may be traced. In addition, biometric technology may be used to directly determine positions of individuals. Given the fact that everything has a time and a place, and that information of location in theory may be linked to every processes, conditions, actions, events etc., and that several technologies may produce this data, we believe it is probable that in the future, location functions will be available in a variety of devices and situations. Thus, we see the possibility that individuals will live in surroundings where, in order to avoid having their location registered at all times, they will have to turn off and opt out of such functions. Similar to "consent exhaustion"[166] this would probably lead to a situation where people may dislike the fact that these data are filed, but refrain from turning off/opting out because it is not sufficiently important compared to the toil they will have to endure order to decide for themselves.[167]

Moreover, and more important, is the fact that where personal location data is generated as result of functions necessary to make payment, stay at an hotel, attend a sports event, go shopping etc, access to these services will be much more important to individuals than the fact that information of where they have been is stored somewhere in the system. In case, this could be seen as a reflection of autonomy because, people probably assess access to services to have greater weight than the – often – theoretical privacy concern that their location data will be misused or applied by the police as part of a wrongful process. Thus, all in all we believe it is unlikely that autonomy of data subjects will have great influence on the protection of individuals connected to processing of personal location data integrated in socially attractive services. People will probably:

- be too exhausted to opt out/turn off location function, and
- accept location functions in order to have access to necessary services and functions, and
- actively acquire location services for their own private purposes.

The third bullet point does not, of course, create any problem with self-determination. The two first points, however, are results of a more narrow scope of free choices of citizens and thus, in principle, represent a problem for autonomy. It is in our view important to recognize that in the years to come a shrinking room of self-determination concerning personal location data will probably be a fact. We are in great doubt as to whether a possible answer to such a development should be stronger self-determination mechanisms, for instance a greater emphasis on

166 See for instance Bygrave and Schartum 2009.

167 However, in the proposed Data Protection Regulation article 23, a privacy by default obligation is introduced as an information system design requirement.

individual consent and opt-out rights. If it is considered that limits should be put on the lawful access to process location data, we believe collective arrangements through legislation, collective agreements, business standards etc. may be more effective than individual autonomy and choice.

Possible subcategories of autonomy and their weight

Although we foresee that self-determination regarding use of personal location data will decrease, autonomy has of course a positive value for privacy protection. Furthermore, there will be differences between location-enabling services with regard to autonomy. We suggest four subcategories to describe this aspect as part of an individual rights impact assessment:

1. Location-enabling services are mandatory and actually unavoidable, e.g. pursuant to legal regulation. Suggested weight: 4.
2. Location-enabling services are actually unavoidable, because in order to live what is considered to be a normal life such services must be used. Suggested weight: 3.
3. Location-enabling services are avoidable provided that data subjects take active actions and accept drawbacks. Suggested weight: 2.
4. Location-enabling services are avoidable and could be regarded as a question of free choice. Suggested weight: 1.

The first category comprises location-enabling services which are mandatory and actually impossible to avoid. Examples under the first subcategory comprise persons subjected to home detention wearing an ankle bracelet locked to their body; hospitalized people wearing a wrist bracelet with ultrasound sender; and RFID tags inserted under the skin of a person. Formally binding legal rules regarding mandatory use of location-enabling technology which are not enforced (and thus possible to avoid) should not be considered to be in the subcategory 1 (and least favourable for privacy and legal protection). Mere formal obligation should probably be considered under category 2 (weight: 3). There are of course only gradual differences between these four subcategories, and assessment will thus be rather discretionary. Also, the wordings of the criteria are intended to give room for assessments relative to qualities of the societies in question. Use of location-enabling services will of course be much easier to avoid in societies where relevant technology have limited distribution, compared to societies which are pervaded.

3.2.4 Purpose of processing and function

Purpose of personal data processing refers to the controller's decision about the ultimate objectives of the processing as it was considered on a certain point of time, typically when the system was developed, procured or revised.[168] The purpose limitation principle of privacy law implies that personal data may only be processed to the extent this is required to achieve such defined purpose(s). As mentioned earlier, even though localization and tracking is carried out, this is not necessarily the purpose of processing. Localization may e.g. just as well be part of the realization of *other* purposes: For instance the purpose of carrying out payment and controlling entrance to sport events.

From a data protection perspective, localization as purpose is of course relevant and important. It is impossible, however, to prevent personal location data from being used for purposes other than those formally specified (cf. "function creep"). An example may illustrate this point: Fleet management systems are typically employed in order to make efficient use of the workforce of a business, and often control is not among specified purposes. Nevertheless, the information about employees' whereabouts are easily accessible to the employer and he will thus at every point of time be able to know the position of specific employees. The actual use employers make of such information is of course impossible to control (or even have any knowledge of). Such use outside specified purposes may be difficult to reveal, because knowledge of location may only be a stepping stone in order to relate to the employee in other ways. The purpose of data processing may for instance be to direct service cars in an effective way. In a given situation with curtailment of the business, the same data may be used to determine which of the chauffeurs that should be dismissed (because aggregated location data on each employee tells who is carrying out work in the most efficient way). Given the purpose of processing as presupposed in the example, this use will be unlawful but hard to track. Thus the purpose limitation may not be regarded effective. We believe this illustrates a limited usefulness of the purpose limitation principle as measure to regulate use of location-enabling technologies/services; in particular when personal location data is accessible and clearly exposed in the system interface.

Our general view is that purpose limitation is important when personal location data is processed. It should however be expected that in many situations purpose specification is not an effective limitation. Therefore impact assessments should have actual *possibilities* of processing personal location data as main criteria and presuppose that purpose specification will not always prevent other use of these data.

168 Cf. article 6(1)(b) of the Data Protection Directive.

Possible subcategories of purpose and their weight

Assessment according to purpose and function is of course not meaningful unless there is some type of function available allowing localization of individuals. Thus, the following subcategories are to a large extent constructed on the basis of how available these functions are:

1. Location-enabling services have localization as purpose. Suggested weight: 4.
2. Location-enabling services have localization as open and available function. Suggested weight: 3.
3. Location-enabling services have localization as possible function provided that users of the system take active actions. Suggested weight: 2.
4. Location-enabling services have localization as possible function provided users overcome technological obstacles. Suggested weight: 1.

The fact that positioning and tracking functions exist as possibility is imbedded in the designation "location-enabling services" and mentioning of these functions are included to qualify their availability. Again, there are only gradual differences between the four subcategories, and assessment will thus basically be discretionary.

3.2.5 Minimality

The principle of minimality is another basic principle within privacy protection law and implies that processing of data should not exceed what is necessary to attain the purposes of processing. Minimality is also related to other privacy aspects and may for instance substantiate the requirement that data should not be revealed to others than those with a need to access data for the fulfilment of specified purposes (cf. confidentiality, "need to know"). The principle of minimality could also state the reason for the requirement that personal location data should not be more detailed than necessary to attain purposes of processing.

Minimality is normally evaluated within the framework of each processing and refers first and foremost to the number of different types of personal data. Regarding personal location data it is however the number of occurrences of data on location and hour that should be seen as the main challenge. In such situations, principle of minimality would imply limitations of how frequent location is established, in other words how detailed patterns of movement that should be allowed.

The principle of minimality may also give rise to identifying different access levels of personal location data. It may be necessary to process rather detailed and comprehensive data. This does however not imply that the controllers always have access to all these data. More than that, seen on the background of purposes of processing, it may not be necessary for the controller to have access to all personal location data. If for instance a fleet management system is established to facilitate

effective directing of service cars to places of assignment, it may not be necessary (or serviceable) to reveal the position of each car to the controller (even if these data exist deep down in the system). Instead the system could be set up to calculate probable travelling time for each car, on basis of general location data (road quality, speed limits, distance, rush hour delays etc.). What the operator needs is just information showing which car has the least probable travelling time to the place of assignment. Basically no personal data is needed to support the purpose of effective management of service cars. Obviously, in order to make it possible for the employer representative to decide who to send, information on which car/driver that has less travelling time is much less sensitive and more serviceable than information of the position of every car/driver at each moment of time.

An additional particularity with relevance to the principle of minimality is the fact that amount of personal location data should not only be assessed for each system/service but in addition to *the sum* of such information from overlapping systems and services working independently and in parallel. When I drive my car with digital GPS-based travel log, pay toll road fee with a RFID based system, find my way to a parking place near my hotel by means of a electronic map, park and pay the parking fee with my GMS smartphone; walk through the streets towards the hotel while using my phone (GSM), and finally enter my hotel room by means of my RFID key, and finally access the Internet through Wi-Fi, I have made use of at least seven services all of which have logged information about my movements. Thus, even if each service were set up to collect as little personal location data as possible, the sum of such data would give a quite comprehensive picture of my movements.

Possible subcategories of minimality and their weight

We suggest that the main criteria in the construction of subcategories below should be the question of inter-linking with other services (creating access to more personal location data), and the availability of these data to the controller. Of course, the situation could be that systems with very limited processing of personal location data is linked, and still the system may be classified as more serious for data protection than a system which register much more location data but is not integrated with other services. It must be remembered, however, that this is one of several classifications and that the final assessment would rely on a combination sub-criteria.

1. Location-enabling services are inter-linked with other such services and there are no limitations regarding the amount of personal location data filed. Suggested weight: 4.

2. Location-enabling service is not inter-linked with other such services and there are no limitations regarding the amount of personal location data filed. Suggested weight: 3.
3. Location-enabling services have limitations regarding the amount of personal location data filed which the controller may circumvent alone. Suggested weight: 2.
4. Location-enabling services have limitations regarding the amount of personal location data filed which the controller may not circumvent alone. Suggested weight: 1.

Inter-linked services should probably mean that they are integrated in ways which make it trivial or at least not difficult to operate them together. Differences between criteria 3 and 4 should probably be that the controller needs authorisation by another person in order to access personal location data contained in and protected by the system. Such authorisation could for instance be carried out government authorities, but it could also be an actor external to the controller for instance a data processor.

3.2.6 Complexity

In D1 of WP7 we classified four types of situations in order to capture the degree of complex relationship between data subjects using location-enabling technology and other actors (controllers, processors and subcontractors). The following groups were suggested:

1. Data subjects (user) alone.[169]
2. Data subjects related to one controller (service provider).[170]
3. Data subjects related to one controller and subcontractors (processors).
4. Data subjects related to several controllers and subcontractors.

The more complex relationship between data subjects and involved parties, the more likely it is that data subjects will have problems understanding the actual role and influence of each actor and the interplay between them. Thus, we assume that there typically will be more difficult in complex situations than in simple situations for data subjects to use the autonomy pursuant to the law. We do however not regard it realistic to prohibit or in other ways restrict over-complex co-operation patterns, and thus we assume that the best way to deal with complexity is to require that it is described and made account for in an eligible way.

169 This is for instance the case when a person uses GPS-based road map device in his car or a handheld units in order to find the way, measure geographical distances etc.

170 This represents a simple and classical. Use of RFID to get access to a hotel room is one of many examples.

Group 3 and especially group 4 (above) represent situations where it should be considered to introduce measures to create as much clarity as possible between collaborating/co-functioning parties. An appropriate point of departure may be the existing requirement of agreements between controllers and processors, cf. Data Protection Directive art. 17(3). The proposed Data Protection Regulation art. 26 define more detailed provisions regarding the relation between controllers and processors. However, it gives controllers and the processors freedom to determine their respective roles and tasks with respect to the requirements of the proposed regulation. Such free options may lead to situations where production of similar location based services and functions are organised with several different divisions of tasks between controllers and processors. This again may make it more difficult for data subjects to understand how these collaborations are composed. Documentation requirements in art. 26(3) may ease such negative effects, but in our view standard requirements regarding contractual relationships between controllers and processors taking part in the production of personal location data should be considered.

Complexity also relates to technological matters and the ability to understand how location data are generated, possible uncertainties regarding correctness, preciseness etc. is important to be able to scrutinize and contradict concrete data. Thus, the more complex technological set-up and functioning of positioning and tracking services, the greater need to describe and clarify technological aspects of processing. In section 3.2.7, we will come back to related questions of transparency and accessibility.

Possible subcategories of complexity and their weight

Our proposal of categorisation of aspects of complexity builds on the referred division in D1:

1. Location-enabling services where data subjects relate to several controllers and several subcontractors. Suggested weight: 4.
2. Location-enabling services where data subjects relate to one controller and several subcontractors (processors). Suggested weight: 3.
3. Location-enabling services where data subjects relate to one controller and (eventually) one processor. Suggested weight: 2.
4. Location-enabling services where data subjects operate alone ("self-controller"). Suggested weight: 1.

The categorisation is simply based on the number of collaborating actors on the service provider side of the relationship and represents a strong simplification. It is possible to imagine several actors even on the data subject side of the relationship, for instance in cases where the object being located is linked to a group of people

(family, colleagues). It is however not practical to embed every possible combinations of relationships. In return for these strong simplifications we gain applicability. Furthermore, possible interplay between categories of other impacts makes it possible to – in total – capture more than what one type of impact may express. In relation to complexity, transparency is particularly important, cf. next section.

3.2.7 Transparency and accessibility

In section 3.2.3 we concluded that the autonomy of data subjects substantiates direct access to his or her personal location data. In our opinion, transparency is of outmost importance as basis of protection of any type of individual right, both regarding privacy protection and legal protection in general.

Current legislation is to a large extent based on access requests from data subjects.[171] In addition, controllers have certain obligations to inform the data subject in predefined situations.[172] Notwithstanding, most important is probably access rights enabling data subjects to attain insight on basis of their own inquisitiveness and with as low formal and practical thresholds as possible. Thus, *direct access* to personal location data for data subjects (without request) could in our view be important measure to strengthen the protection of individuals.[173]

Direct access requires that information is available at all times and – ideally – that it is constantly updated. Thus, even for systems not having location as purpose, they should be designed to automatically log location data in ways which are accessible to data subjects. Such logging functions should, in our view, be a privacy-by-design requirement. Among data with particular interest for each data subject, is of course personal location data, whether or not these data have been made available to others, as well as legal basis for disclosure.

In the proposed Data Protection Regulation Article 15 about the right to access and to obtain data for the data subject, access rights are still based on request from the data subject. In our view, protection of individuals regarding personal location data gives grounds to consider going one step ahead and giving access without request by means of sufficiently secure log-on procedures. This is in line

171 See, the Data Protection Directive, article 11.

172 See, the Data Protection Directive, article 10.

173 Open information regarding disclosure could not be expected if data are made available to the police. In cases where personal location data is accessed in the course of investigation of particularly serious crimes and access rights are limited, it should however be considered to introduce compensating measures. One aim could be to safeguard data quality and avoid that police base their actions on what could be incorrect or insufficient personal location data. Such safeguards are of critical importance for the legal protection of suspects. A possible measure could be to authorize access to publicly appointed secret representatives (lawyer) of suspects. The representative's task could be to control that the quality of personal location data and other critical information of the case are sufficient.

with the proposed provision in article 12 of the PDR concerning procedures and mechanisms for exercising the rights of data subjects:

"2. […] The information shall be given in writing and, where possible, the data controller may *provide remote access to a secure system which would provide the data subject with direct access to their personal data*."(Italics added)

Placed together with the referred art. 15 this probably implies that, on the condition of secure systems, direct access to personal location data would be allowed, but will not be an obligation for the controllers. In our view, regarding personal location data, it should considered as a main rule to make direct access a right when these data could be made available on-line through existing systems.

Possible subcategories of transparency and their weight

Questions of transparency are of basic importance to every other issue of protection of the individual: Without relevant knowledge, data subjects have no basis to control legality and claim their rights. Transparency is also a very comprehensive issue and comprises transparency on the level both of information systems and of concrete personal location data connected to each individual. The multifactor nature of transparency questions makes it desirable to introduce more than one set of criteria, and below we suggest one set regarding the level of information *systems* and another set of criteria for the level of concrete *personal location data*.

System level:

1. Documentation of systems producing location-enabling services does not exist and information must be provided on a case-by-case basis. Suggested weight: 4.
2. Documentation of systems producing location-enabling services exists and is available on request on basis of payment or other accessibility hindrances. Suggested weight: 3.
3. Documentation of systems producing location-enabling services exists and is available without accessibility hindrances. Suggested weight: 2.
4. Documentation of systems producing location-enabling services exists and is publicly available/published. Suggested weight: 1.

Contents of documentation of systems producing location-enabling services should first and foremost be of technological and organizational nature; it should in other words e.g. describe how positioning and tracking functions works and specify types of actors involved and their role and relations, cf. section 3.2.6

(above).[174] Other accessibility hindrances (cf. point 2 and 3) than payment may for instance be format requirements and requirements for authentication measures which many people will have problems to satisfy.

Level of personal location data:

1. Documentation of personal data which are processed and produced in the course of location-enabling services does not exist and information must be provided on a case-by-case basis. Suggested weight: 4.
2. Documentation of personal data which are processed and produced in the course of location-enabling services exists and is available on request on basis of payment or other accessibility hindrances. Suggested weight: 3.
3. Documentation of personal data which are processed and produced in the course of location-enabling services exists and is available without accessibility hindrances. Suggested weight: 2.
4. Documentation of personal data which are processed and produced in the course of location-enabling services exists and is directly available for the employee in question. Suggested weight: 1.

The structure of this second set of criteria is built similar to the structure as for the systems level. Difference concern first and foremost subject of documentation.

3.2.8 Summarising possible subcategories and their weight

Our idea is that location-enabling technologies basically may be assessed on the basis of the seven sets of criteria specified in section 3.2.

Value of impact / **Type**	1	2	3	4
Sensitivity				
Autonomy				
Purpose				
Minimality				
Complexity				
Transparency, systems				
Transparency, personal data				

Table 2 Suggestion of elements and weights in a basic impact assessment of location-enabling technology.

174 In general information similar to what is specified in Data Protection Directive art. 21 (3), cf. article 19 (1) (a) to (e).

In order to demonstrate how individual rights impact assessment could be carried out by means of the individual rights impact assessment model represented in the table above we will here describe aspects of a fleet management system and categorise pursuant to the criteria in section 3.2.2 – 3.2.7 (above). Conclusions regarding each aspect will be a value 1 – 4 where 4 indicates the most severe privacy challenges.

The fleet management system we will use as an example keeps track of company cars by means of a GPS-based system connected to the car. Rosters show which chauffeur that (most probably) is driving, and thus movements of the car would in most cases even show whereabouts of a specific employee. Our fleet management system is online and integrated with other personal management systems, including the wage payment system. Below, we continue the description of the system as we go through the seven types of impact with connected criteria.

- Sensitivity. In our system data from the GPS function is linked to data from a RFID based system which registers every time a suitcase containing medicine is removed from and put back into the car. The two systems are integrated and automatically produce reports where both types of data show. This description implies that assigned sensitivity value is 3.[175]
- Autonomy. Use of GPS and RFID functions is mandatory for employees, and assigned value regarding this aspect is consequently 4.[176]
- Purpose. The purpose of the fleet management system is not to locate employees, but to perform effective management of the company. In order to achieve this purpose, location and tracking is necessary. Assigned value regarding this aspect is 3.[177]
- Minimality. The fleet management system is set up to carry out constant logging of GPS data, but reports from the system only contain a selection of data. In order to have full reports, the employer has to ask for assistance from a processor with technical expertise who is running the system. Assigned value regarding this aspect is 1.[178]
- Complexity. In the fleet management system we consider, there are only one controller (the employer) who is assisted by one processor. Assigned value regarding this aspect is 2. [179]

175 "PT-based services have functions which facilitate linking of personal location data to other personal data."

176 "PT-based services are mandatory and actually unavoidable, e.g. pursuant to legal regulation."

177 "PT-based services have localization as open and available function."

178 "PT-based services have limitations regarding the amount of personal location data filed which the controller may not circumvent alone."

179 "PT-based services where data subjects relate to one controller and (eventually) one processor."

- Transparency, system. In our system, no system documentation is available but information is given in each case on basis of request. Assigned value regarding this aspect is 4.[180]
- Transparency, personal data. Last, but not least, files containing personal data on each employee are directly available from a personal PDA which every employee have at his or her disposal.[181] Assigned value regarding this aspect is 1.

Total picture. Results of this type of assessment range from 7 (easy concern) to 28 (grave concern) and may function as a signal to decision-makers. Procedural rules may be attached to certain values; values between 7 and 13 may for instance follow normal procedure, while values between 14 and 28 follow a special procedure with e.g. special requirements regarding participation and competences on the preparatory stage, decision-making level etc.

The fleet management system we imagined (above) has been assigned a total score of 18 (cf. the bullet points above). In other words, viewed from a privacy perspective; the system is assessed as representing more than averagely problematic use of location-enabling technology.

Categorization and scores may of course be used to improve systems on basis of assessed impact. It may also be used to pursue a bundle of other purposes:

1. Categorise systems as basis of legal regulation; for instance by introducing stronger protection for systems with score above certain values.
2. Self-evaluation for controllers as part of the process of developing, adjusting or purchasing a location-enabling system.
3. Tool for policymakers which assist the process of mapping problem areas which should receive special attention.
4. Guidance to developers of commercial location-enabling systems and suppliers of positioning and tracking based services for their choice of system/service design.
5. Specify qualities of location-enabling systems as basis for information to data subjects, for instance in cases of his or her consent to process personal location data.
6. Classification of systems by the police in order to give assistance for the selection and assessment of possible sources of evidence and other information in course of police work.
7. Classification of systems applied by the courts as basis of decisions regarding permission to the police to collect personal location data from specific positioning and tracking systems.

180 "Documentation of systems producing PT-based services does not exist and information must be provided on a case-by-case basis."

181 "Documentation of personal data which are processed and produced in the course of PT-based services exists and is directly available for the employee in question."

The applications mentioned above as well as other uses may be relevant and fruitful. In section 3.3 we will return to application 7 on the list.

Of course the assessment model may be extended, both in terms of numbers of aspects and the number of criteria related to each aspect. It is however important that such models balance between needs of accurate description of problems on the one side and practicality on the other. A much extended model may lead to little use, and a too limited model reduces the fruitfulness and effectiveness of the tool.

3.3 Elements of assessments of particular relevance to processing by the police

3.3.1 Introduction

The impacts which were discussed in section 3.2 are of basic nature and designed to be applied on all location-enabling systems and services regardless of sector and situation. Emphasis was put on privacy protection aspects. In this section we will add certain impacts which we have identified as particularly important for police processing of personal location data as part of investigation and other police work which represents exercise of public authority over citizens or which has direct influence on such authority. Intelligence and other preventive work are important examples of work which may imply direct influence on exercise of authority; even when open sources are used.

We have only selected three elements with particular relevance to processing by the police. The relevance of the first element, lawfulness, is of course not limited to the police and is for instance one of the basic principles of privacy. Thus we could have chosen to discuss it in section 3.2 or both in 3.2 and this section. General questions of lawfulness of the processing of personal location data are in our view rather obvious and comparatively simpler than when processing is carried out in the police. Thus, we have chosen to limit the discussion to the last mentioned situations. The element contradiction (see section 3.3.4) is also relevant to privacy protection, but is not formulated as independent data protection principle. Ability to contradict may however be seen as the objective of central elements of privacy and data protection legislation in particular transparency and access rights. (The third element, regarding extent and type of police power (section3.3.3), is not closely related to any privacy principle.)

3.3.2 Lawfulness

Fairly and lawfully processing of personal data is a basic requirement in both the Data Protection Directive and the European Convention on Data Protection.[182] More importantly, article 8 of the ECHR on "Right to respect for private and family life", state in paragraph 2 that "[t]here shall be no interference by a public authority with the exercise of [the right to respect for private and family life*]* except such as is *in accordance with the law* and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." (Italics added)

Here we will limit discussions to questions of lawfulness and refrain from going into discussions of criteria like "interference" and "necessary in a democratic society". In the context of location-enabling technology and processing of personal location data, our simple point is that the police always need to consider i) if access to such data represents an infringement of the right guaranteed by ECHR article 8 (1) and ii) if this is the case, if the police have sufficient legal basis to collect these data and further process them.

An individual rights impact assessment as described in section 3.1 (above) should investigate if individual rights could be endangered because there are doubts regarding lawfulness of police access to such data. An impact assessment model should assist police and courts in their evaluation of lawfulness. Like in section 3.2, the criteria of the model do not lead directly to conclusions; it rather indicates level of attention and helps to distinguish between (relatively) expectably easy and hard cases.

We will suggest that lawfulness of police access to and processing of personal location data should be assessed according to two aspects:

1. Existence of legal basis and the authority of these sources, and
2. communicative qualities of legal sources and appurtenant legal information.

These criteria are close to criteria developed in case-law of the ECtHR,[183] but we underline that our approach represent a much more simple line of action only designed to lead up to in-depth evaluation of legal questions affined to ECHR article 8. The criteria could also be seen as an extension of transparency aspects discussed in section 3.2.7 (above).

Regarding the first aspect, we will suggest the following set of criteria:

1. Police access to and processing of personal location data is not regulated by any legal source. Suggested weight: 10.

182 Cf. art 6(1)(a) respectively art. 5(a).

183 Van der Hilst 2013 discusses ECtHR case law regarding geolocation, see page 173 – 279.

2. Police access to and processing of personal location data is only regulated by internal guidelines and standard operating police routines. Suggested weight: 6.
3. Police access to and processing of personal location data is only regulated by general law. Suggested weight: 3.
4. Police access to and processing of personal location data is regulated by specialised law which directly addresses questions of personal location data. Suggested weight: 1.

In order to better identify assumed easy and grave cases, our suggested weights are defined over a broader scale compared to those in section 3.2. Thus, here the range is between 1 and 10, while in section 3.2 the range was between 1 and 4. With "regulate" we both refer to legislation and case-law where a clear opinion is expressed regarding applicable law.

The second aspect regarding communicative qualities of legal sources and appurtenant legal information, seem to presuppose the existence of a legal basis, and thus logically situation 1 above will not be applicable. However, if these situations are not part of assessment of quality of sources, they will receive a misleading low total score. We have therefore included a criteria suited to comprise even these situations.

1. Police access to and processing of personal location data is not regulated by any legal source (and no information of lawfulness exists) Suggested weight: 10.
2. Legal sources are the only source of information regarding police access to personal location data and further processing of such data. Suggested weight: 6.
3. Legal information regarding police access to personal location data and further processing of such data exists and is available on request. Suggested weight: 3.
4. Legal information regarding police access to personal location data and further processing of such data exists and is publically available (without request). Suggested weight: 1.

The criteria above are built on a distinction between legal sources and legal information. By "legal sources" we mean the authentic texts and "legal information"; the term refers to information based on legal sources in order to identify and explain legal rules derived from these sources.

Suggested weights of each criterion produce marked differences between them. The effect will be that cases of collection and further processing of personal location data without basis in legal sources or only regulated in police' internal guidelines, and with no available legal information regarding this issue, will receive score between 12 and 20. High scores will be a signal of needs of very careful legal considerations by the police, courts, privacy advocates and others.

3.3.3 Extent and type of police power

In D1 and D2 report, section 5.8 we raised questions concerning the extent and type of police power and suggested four subcategories which we will apply here. It may in our view be reasonable to identify subgroups of people according to the degree and type of exposure to police interest and power. The large bulk of people will not be exposed, because in most cases police will only have access to data from a limited time period, geographical area, service provider etc.

Here, we will suggest the following four criteria:

1. Police access to personal location data and further processing of such data is carried out in the course of execution of direct police power (investigation, arrest etc.). Suggested weight: 10.
2. Police access to personal location data and further processing of such data is carried out in the course of surveillance and control (police intelligence work etc.). Suggested weight: 6.
3. Police has access to personal location data, but without using it. Suggested weight: 3.
4. Police access to personal location data and further processing of such data is limited to the aim of protecting and safeguarding these people.[184] Suggested weight: 1.

It is natural to assume that special guarantees should be offered to people in every of these four categories. Needs of protection are however very different in situation 1 and 2 compared to situation 3 and in particular situation 4. In the latter situations, the main requirement is that police respect the strong limitations connected to their processing; while in the two first situations processing could be extensive and possibly with very direct and severe consequences for individuals.

We assume it may be very practical that police process personal location data both in the course of e.g. surveillance and investigation, cf. categories 2 and 1. In such cases assessments should be made on basis of the *sum* of each criteria, i.e. total weight = 16.

3.3.4 Contradiction

The adversarial principle is fundamental in criminal procedure and should thus be emphasised when access to and further processing of personal location data by the police is considered (by the police, courts, privacy advocates etc.). This principle may be entrance to many sub-problems but here we will limit ourselves to questions of finding alternative sources which could shed light on the same facts which personal location data is applied to prove/document. The more police may

184 For instance to protect children, senile and other mentally handicapped people.

be said to be in the position of a "information monopoly", the more careful and critical the police and courts should be regarding police procedures, assessment of possible sources of error, data quality etc.

The more difficult it is to understand the technological aspects of processing, the stronger considerations should be of possible dangers of deficient possibilities to contradict. Such considerations are especially well-founded in situations where *technometric* techniques are applied, i.e. in situations where assumptions of a certain individual's movements are based on location of objects connected to this person.[185]

We suggest the following criteria as basis to access the contradiction aspect:

1. There is only one known and available technologically based source of data that could shed light on locations of individuals in the case at hand. Suggested weight: 10.
2. There are several known and available technologically based sources of data that could shed light on locations of individuals in the case at hand, but these takes special expertise to access and interpret. Suggested weight: 6.
3. There are several known and available technologically based sources of data that could shed light on locations of individuals in the case at hand which expectedly could be accessed and interpreted without special expertise. Suggested weight: 3.
4. There are several known and available sources (technological and other) of data that could shed light on locations of individuals in the case at hand which expectedly could be accessed and interpreted without special expertise. Suggested weight: 1.

By "individuals" we refer to data subjects receiving special attention by the police as suspect, witness or in similar roles which actualise needs of legal protection. A source may be considered available if there are no insuperable formal or practical/technical obstacles.

The first alternative will easily be apprehended by the data subject as a "black box experience", i.e. a situation where input and output may be observed and understood but with no possibility to understand the encapsulated technological processes without help from experts. In such situations it should be expected that it will be hard for the data subject to contradict, i.e. produce an alternative understanding of location data produced by a technical system. The possibility to for data subjects to contradict is better in situations 2 to 4 (above), because here there are several alternative sources of location data which may be compared. The difference between situations 2 to 4 relates first and foremost to the level of expertise required and the type of data source.[186]

185 See D1, section 3.3. Even establishment of location based on *biometric* technology have uncertainties that should be taken very seriously.

186 "Other" source of data may for instance refer to a witness, a finger print etc.

3.4 Summarising subcategories in section 3.3 and total picture

In this chapter, we have suggested aspects and conditions in an individual rights impact assessment performed in two stages; one basic/general stage and one stage linked to processing by the police and the judiciary. This assessment model does not lead directly to conclusions but is meant to represent a systematic approach which both safeguard that main aspects are considered and that indications are given regarding the degree of controversy and difficulty, as seen from the perspective of privacy and other individual protection.

The approach we suggest is a system where results from the general assessments of positioning and tracking technology and personal location data are summed up and classified in one of four categories with connected weights:

1. General assessment of positioning and tracking technology and personal location data are summed up to be 23 – 28. Suggested weight: 10.
2. General assessment of positioning and tracking technology and personal location data are summed up to be 18 – 23. Suggested weight: 6.
3. General assessment of positioning and tracking technology and personal location data are summed up to be 12 – 17. Suggested weight: 3.
4. General assessment of positioning and tracking technology and personal location data are summed up to be 7 – 11. Suggested weight: 1.

Our idea is that location-enabling technologies may be evaluated on basis of the seven sets of general criteria specified in section 3.2 summed up in one weight, plus the weights from assessments in this section (3.3). Application of this approach on the imagined fleet management system presented in section 3.2.8 is illustrated in Table 3 (below):

Value of impact / **Type**	1	3	6	10
General assessment			6	
Lawfulness, legal basis	1			
Lawfulness, information			6	
Police power				10
Contradiction		3		
Sum				

Table 3 Suggestion of elements and weights in a total impact assessment of location-enabling technology.

The score of the imagined fleet management system was 18, something which implies that value 6 is assigned in the first row in the table above.[187] The three next aspects refer to possible police use of personal location data from this fleet management system: If we assume that the lawfulness of police access to data in the fleet management system (and thus considered by the legislator), this will pursuant to the criteria in section 3.3.2 (above) result in weight = 1. Lack of information regarding contents of relevant legislation would however result in the weight = 6. When processing is conducted as part of police investigation, this yields weight = 10 (police power), and since there are other easily available sources (e.g. private mobile phone of the employee), the score regarding contradiction is 3. Regarding our example, this gives a total score of 26 which is above average possible score (highest score: 40, lowest: 4).

Again, results of this type of assessment (here ranging from a minimum of 6 to a maximum of 60) may function as a signal to decision-makers, and procedural rules may be attached to certain values. Values between 6 and 18 may for instance follow normal procedure, while values between 19 and 100 may follow a special procedure with e.g. special requirements regarding participation and competences on the preparatory stage, decision-making level etc.

Ratings as suggested may also be linked to the sentencing framework, for instance implying that application by the police of a certain location-enabling technology could not have a higher score than 10 if the maximum penalty of investigated crimes is less than a certain number of years (e.g. 3 years of imprisonment). It follows that location-based investigation measures giving high scores (e.g. more than 19) could be reserved for particularly serious crimes. In Table 4 (below) we have exemplified how links between individual rights impact assessment (IRIA) score and sentencing framework could be.

IRIA score	**Sentencing framework**
37 – 100	More than 10 years imprisonment
19 – 36	Minimum 10 years imprisonment
6 – 18	Maximum 3 years imprisonment

Table 4 Example of guiding links between assumed infringed use by the police of location-enabling technology and sentencing framework.

Here, for purposes of illustration, we have chosen to set limits for police investigation by means of location-enabling means according to three categories. For the group of less serious crimes, investigation by means of location-enabling technology could for instance not exceed a score of 18; for more serious crimes the limit could be set higher (36 in our example), and for the most serious crimes there

187 Cf. the shaded frame above point 2, where values 18 – 23 are assigned the weight 6.

could be no limit (pursuant to the scoring system 100 is maximum). The scores give a picture of degree of infringement of privacy of people being subject to such investigation methods, and the thought behind this approach is that it should be proportionality between such infringements and the sentencing framework for the crimes investigated. Important grounds for such a proportionality requirement is i) that it is in principle always a chance that persons investigated are innocent (cf. presumption of innocence), and ii) there are always a chance that the privacy of people outside suspicion will be infringed when location-enabling technology is used (family, friends, colleagues etc.).

It is neither desirable nor realistic to strictly follow an approach based on a formal system of scores and categories of crimes etc. Our intention is that e.g. police and courts may use such approaches as guideline, rather than a rule. In case a court will allow use of investigation methods yielding high IRIA score (i.e. with high degree of privacy infringement) even though investigated crime is not very serious, the function could for instance be that a thorough substantiation is required, plus extra safeguards etc.

Of course, this is not about mathematics but rather evaluation based on fairness and morality in a wide sense. Notwithstanding this, we believe such more formal approaches could be helpful to structure and communicate relevant problems and to identify and highlight critical points of complex decision-making situations. In busy work situations, one risk is of course that a formal approach limits discussions. However, we assume that without formalised criteria including assignment of weights etc., chances are high that important elements will be neglected.

4 Concluding insights and remarks

From the start, WP7 of the Respect project was very much directed towards certain types of technologies (GSM, Wi-Fi/WLAN, GPS and RFID) and the ability to locate and track people by means of wireless and mobile devices. One important insight from the project has been that a variety of other technologies may also be used to locate and track. Thus, both in the perspective of the police and of citizens, the crucial point is not technological particularities, but the location and tracking *function* that technology may perform, regardless how they may be classified according to technological criteria.

We are not saying that technological distinctions are unimportant, but instead that they are first and foremost important when individual cases are scrutinised: On a principle level, the main question is whether or not privacy protection should limit police use of means which make it possible to follow whereabouts of suspects and other interesting subjects and objects. On this stage, technical how-questions are less important. In the next stage, technological features and characteristics are important in every concrete individual case, in particular regarding assessment of forensic qualities of available methods. Certain technologies may for instance be exposed to more sources of uncertainties and errors than others, and it may not be serviceable to apply a method if resulting data will not meet evidential requirements.[188]

The choice between an orientation towards technology versus the functions that technologies perform is mirrored in the choice of regulatory response. Our overview of relevant initiatives of the EU Commission[189] showed how special guidelines etc. have been developed regarding RFID and smart devices, i.e. with a technological orientation. Legislation, on the other hand, is held technological neutral applying utterly abstract, vague and discretionary language where technological features and conditions are hard to discover. It is of course a possible line of action to combine such technology neutral legislation with other documents explaining how technological particularities should be connected to the general and abstract legal rules. If so, it should be expected that all types of technology applicable for the location of people would be explained in similar ways as RFID and smart devices.

Today, the relation between privacy protection and all types of location-enabling technology is not explained (as in the case of RFID and smart devices), and given the rather large number of relevant technologies[190] we are very doubtful as to if such a strategy should be selected for every type of technology. Rather, it co-

188 Even methods giving unreliable results may however be found useful for internal police work, i.e. without data being used as evidence before the court, see Deliverable 1 and 2, section 5.3.

189 Cf. section 2.1 and 2.2.

190 Cf. our general technology model in Figure 1.

uld be serviceable to develop rules and/or guidelines which establish and discuss how important legal questions connected to general legal instruments should be solved in the case of localization and tracking of people. Many of the uncertainties and interpretations problems discussed on section 2.3 could in other words be solved or at least reduced, by making more detailed statements about how the general legislation should be understood in the case of localization and tracking – and regardless of the technology applied.

Our technological study[191] showed how various technologies and devices may be applied to determine location of devices and thus of connected individuals. On basis of current stage of technological development, we have given examples of how several services/devices may continuously map peoples whereabouts,[192] and we argue that it is very likely that in the future personal location data will be part of still more services.

Even though personal location only occasionally will come under the special categories of data reckoned as sensitive under a stricter legal regime, we have argued that such data should receive special regulatory attention due to the fact that i) they may be directly sensitive; ii) personal location data may easily become sensitive in combination with other data, and iii) the comprehensive and increasing collection of such data in civil society require special privacy consideration because of its omnipresence and potentials of revealing very many central aspects of the life of each individual. We have noticed that the draft Data Protection Regulation contains certain new special elements safeguarding location data,[193] and believe this line of action should be extended and enforced.

Personal location data are produced everywhere in civil society and constitute a huge potential as a source for the police, both regarding investigation and intelligence. We have not considered the extent and means of access by the police. However we have pointed out that the current situation with common regulation pursuant to the Data Protection Directive of personal location data in most parts of civil society, combined with the absence of common rules when such data are collected by the police and thereby fall under national criminal procedural regimes, should be seen as a problem. Although we have not investigated the degree of protection under various national criminal procedure legal regimes, we take it that standards of legal protection vary. We also take for granted that in the foreseeable future, common criminal procedural rules in EU are not realistic. Thus, to the extent that better protection of personal location data is desired within the realm of national legislation, it will be necessary to regulate these data as part of

191 Cf. Deliverable 1 and 2, chapter 4.

192 See section 3.2.5 (above).

193 See section 3.2.2 (above).

the general data protection laws.[194] Our argument is that because personal location data flow from civil society to the domain of police and judiciary, general regulation of such data may even have effect in domains governed by national rules. Questions of autonomy of data subjects, data retention, quality and transparency are probably among the issues which could be regulated on the EU level with important indirect effects on the extent and ways personal location data may be processed by national police, courts etc.

Regardless of the nature of future legal regulation, considerations of the need for protection of individuals associated with location-enabling technology will always be complex and difficult. Types of situations where personal location data play an important role are so many and manifold that it will be impossible to provide fixed provisions with universally unambiguous meaning to determine conclusions. Thus, we believe a scheme for individual rights impact assessment (IRIA) may be an adequate and necessary tool to assist the discretion of controllers, investigation leaders, judges etc. There are many ways of shaping and using such a scheme, and in chapter 3 of this report we have shown some of the possibilities. Of course to be efficient, in practical life, such tools must be ICT-based.

We have also suggested the development of apps as a measure to support protection of individuals and their personal location data.[195] This could be carried out according to several models, for instance as standard elements in every app where location data are processed, or as an independent app which only functions to assist people in their consideration of questions regarding location data and privacy. Further description and requirement specification falls outside the scope of this project.

194 That is the Data Protection Directive, eventually the draft Data Protection Regulation and the draft Directive regarding data protection within the police, judiciary etc.

195 See section 2.3.10.

Figures

Tables

References

Literature

Brock, D. L. (2001) *The electronic product code (EPC): a naming scheme for physical objects* (Report: Auto-ID Center White Paper WH-002) Cambridge, MA: MIT.

Bygrave and Schartum 2009. Bygrave, Lee Andrew & Schartum, Dag Wiese (2009). Consent, Proportionality and Collective Power, In Serge Gutwirth; Yves Poullet; Paul De Hert; Cécile de Terwangne & Sjaak Nouwt (ed.), *Reinventing Data Protection?*. Springer Science+Business Media B.V.. ISBN 978-1-4020-9497-2. Kapittel 9. s 157 - 173

Kaplan, E. D. (2005) *Understanding GPS: Principles and Applications, Second Edition*. Boston: Artech House.

Rfidjournal (2007) *Alzheimer's Care Center to Carry Out VeriChip Pilot,* last updated: 2007-05-25, (nettavis), http://www.rfidjournal.com/article/view/3340/ (retrieved: 2008-11-19).

Tranvik (2013) *Det gjennomsiktige arbeidslivet. Erfaringer med feltteknologi i utvalgte yrker.* [*The transparent working life. Experiences with field technology in selected professions.*] CompLex 2/2013, Norwegian Research Center for Computers and Law, Akademika, Oslo, 2013.

Van der Hilst 2013. Rozemarijn van der Hilst, *Putting Privacy to the Test: How Counter-Terrorism Technology is Challenging Article 8 of the European Convention on Human Rights*, dissertation submitted in partial fulfillment of the requirements for the degree of Ph.D, University of Oslo, Faculty of Law, Oslo 2013.

Welbourne, E., et al. (2009) Building the Internet of Things Using RFID: The RFID Ecosystem Experience, *IEEE Internet Computing*, no. May/June, pp. 48-55.

Worldnetdaily.com (2006) *Employees get microchip implants,* last updated: 2006-02-10, (nettavis), http://www.wnd.com/news/article.asp?ARTICLE_ID=48760 (retrieved: 2008-11-17).

Conventions, treaties, directives etc.

European Convention of Human Rights (ECHR)

The Treaty on the Functioning of the European Union (TFEU)

Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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

Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD))

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data {SEC(2012) 72 final} {SEC(2012) 73 final}

Other documents

ARTICLE 29 Data Protection Working Party

- Opinion 4/2007 on the concept of personal data
- Opinion 13/2011 on Geolocation services on smart mobile devices
- Opinion 02/2013 on apps on smart devices

European Commission

- Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism
- COMMISSION RECOMMENDATION of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification
- Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS (Brussels, 22.10.2013), COM(2013) 739 final. Commission Work Programme 2014

Case law

ECJ: Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist (C-101/01).

ECtHR: Uzun v Germany Fifth Section Judgement 2 September 2010 (application no. 35623/05).

Inquiries conducted in D1 and D2 on which this work is partly based

- Inquiry directed to the national telecommunication authorities ("telecom inquiry")

- Replies from national telecommunication authorities of Austria, Bulgaria, Germany, Italy,[196] Norway, Romania, Slovakia and Slovenia
- Inquiry directed to the national data protection authorities ("data protection inquiry")
- Replies from national data protection authorities of Austria, Bulgaria, Germany, Italy, Norway, Romania, Slovakia and Slovenia
- Inquiry directed to Internet service providers operating in the national marked of each country ("ISP inquiry")
  - Austria: replies from 2 Internet Service Providers (ISPs)
  - Bulgaria: replies from 6 ISPs
  - Germany: reply from 1 ISP
  - Italy: replies from 3 ISPs
  - Norway: reply from 1 ISP
  - Romania: reply from 1 ISP
  - Slovakia: reply from 1 ISP
  - Slovenia: replies from 3 ISPs
- Reports from document studies in government dossiers etc. in each country ("document study").
- Reports from Austria, Bulgaria, Germany, the Netherlands, Norway, Slovakia and Slovenia.
- Interpol inquiry

Replies from 12 European countries, 2 North American countries, 6 countries of the Middle East and North Africa, 3 Asian countries, 2 West African countries, 6 East African countries, 2 South American countries, and 4 Central American countries.

196 Two central authorities gave their reply.

Annex 1: List of home institutions of national research groups participating in WP7

- Australia, Edith Cowan University,
- Austria, University of Vienna
- Bulgaria,Law and Internet Foundation,
- Czech republic, Masaryk University,
- Germany, Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts,
- Italy, Laboratorio di Scienze della Cittadinanza,
- Malta, Universita ta Malta,
- Netherlands, University of Groningen
- Norway, Universitetet i Oslo,
- Romania, Babes-Bolyai University of Cluj Napoca
- Slovakia, Univerzita Komenskeho v Bratislave,
- Slovenia, University of Ljubljana

Tidligere utgitt i Complex-serien

CompLex er Senter for rettsinformatikks skriftserie. Serien startet i 1981, og det har blitt utgitt mer enn hundre titler. Bøkene i CompLex-serien kan bestilles fra Akademika (se bestillingsskjema bak i boken eller www.akademika.no).

2013

1/13 **Retten til ikke å vite**
Marit Stubø.....*NOK 192,-*

2012

2/12 **To arbeider i prosjektet Road to media-aware user-Dependent self-aDaptive Networks (R2D2)**
Darren Read og Dag Wiese Schartum.....*NOK 171,-*

1/12 **Fra kontrollør til aktør: Behov for nye roller for fagdepartementene i styring av tverrgående IKT-prosjekter?**
Arild Jansen og Ivar Berg-Jacobsen
IT governance in Norwegian public sector – business as usual?
Arild Jansen and Tommy Tranvik
The functions and roles of ICT in public sector and its impact on management and governance
Arild Jansen.....*NOK 138,-*

2011

1/11 **Styring av den elektroniske forvaltning i Norge – en tilstandsrapport**
Arild Jansen og Ivar Berg-Jacobsen.....*NOK 108,-*

2/11 **Tilgang til og videreformidling av helseopplysninger**
Herbjørn Andresen.....*NOK 589,50*

3/11 **Automatisert inndragning**
Inger Marie Sunde.....*NOK 502,50*

4/11 **Senter for rettsinformatikk: Bibliografi 1970-2010**
Anne Gunn B. Bekken.....*NOK 327,-*

5/11 **Om avgrensing av arbeidsgivers styringsrett på grunn av arbeidstakers personvern – En gjennomgang av norsk rettspraksis**
Mette Borchgrevink ..... *NOK 179,-*

6/11 **Legaldefinisjoner i nyere norske lover**
Dag Wiese Schartum
Legaldefinisjoner og juridisk interoperabilitet i helsesektoren
Marius Raugstad og Ivar Berg-Jacobsen ..... *NOK 299,-*

2010

3/10 **Extended collective licences – the compatibility of the Nordic solution with the international conventions and EC law**
Christian Rydning ..... *NOK 192,-*

2/10 **Air Passenger Data Protection – Data Transfer from the European Union to the United States**
Olga Mironenko ..... *NOK 132,-*

1/10 **Using Citation Analysis Techniques for Computer-Assisted Legal Research in Continental Jurisdictions**
Anton Geist ..... *NOK 210,-*

2009

5/09 **Anvendelse av straffeloven § 343 hvor det handles mot et konvensjonsstridig ytringsforbud fastlagt ved midlertidig forføyning**
Ranveig Tufte Fjerdrumsmoen ..... *NOK 87,-*

4/09 **Personvern og informasjonssikkerhet**
Tommy Tranvik ..... *NOK 195,-*

3/09 **Vurdering af PersonVernnemndas Praksis 2001–2008**
Peter Blume ..... *NOK 852,-*

2/09 **Legal issues regarding whois databasis**
Dana Irina Cojocarasu ..... *NOK 258,-*

1/09 **Åpen programvare – noen rettslige problemstillinger**
Odd Randgaard Kleiva ..... *NOK 225,-*

2008

8/08 **Rett og rimelighet i moralsk belysning og andre grunnproblemer i norsk rettsliv**
Jens Petter Berg.....*NOK 657,-*

7/08 **Vern av tekniske beskyttelsessystemer etter åndsverkslovens §53a**
Andreas Norum.....*NOK 156,-*

6/08 **Grunnloven § 100 (4) som hinder for bruk av midlertidige forføyninger mot ytringer – med spesielt fokus på forestående, antatte opphavsrettskrenkelser**
Frederik Langeland.....*NOK 132,-*

5/08 **Telekirurgi i et rettslig perspektiv – med spesiell vekt på etikk, samtykke og ansvar**
Bjørn Ivar Christie Østberg.....*NOK 201,-*

4/08 **IT-støtte for arbeid med lovsaker**
Dag Wiese Schartum.....*NOK 144,-*

3/08 **Juristopia: Semantic Wiki for Legal Information**
Ole Christian Rynning.....*NOK 243,-*

2/08 **Electronic Contracting in Europe. Benchmarking of national contract rules of United Kingdom, Germany, Italy and Norway in light of the EU E-commerce Directive**
Maryke Silalahi Nuth.....*NOK 192,-*

1/08 **Internet search engines» collecting and processing of web pages – from the perspective of copyright law**
Ingvild Jørgensen.....*NOK 165,-*

2007

5/07 **Gjennomgang av arkivretten**
Martin Rødland......*NOK 129,-*

4/07 **Privacy & Identity Management**
Thomas Olsen, Tobias Mahler, et al......*NOK 234,-*

3/07 **Personvern og transportsikkerhet**
Dag Wiese Schartum.....*NOK 306,-*

2/07 **ZEBLEX 06 – Tre avhandlinger om fildeling, IT-sikkerhet og e-postkontroll**
Ida Otterstad, René Stub-Christiansen & Cecilie Wille Søvik ..... *NOK 348,-*

1/07 **Kontraktsregulering av domstolens kompetanse ved elektronisk handel**
Vebjørn Krag Iversen ..... *NOK 186,-*

2006

6/06 **Lover – fra kunngjøring til hyperstrukturer: to avhandlinger**
Per Marius Slagsvold & Kirill Miazine ..... *NOK 222,-*

5/06 **Retten til eget bilde**
Maria Jongers ..... *NOK 198,-*

4/06 **Legal, Privacy, and Security Issues in Information Technology Vol. 2**
Kierkegaard, Sylvia Mercado (editor) ..... *NOK 783,-*

3/06 **Legal, Privacy, and Security Issues in Information Technology Vol. 1**
Kierkegaard, Sylvia Mercado (editor) ..... *NOK 918,-*

2/06 **Rettslige reguleringer av informasjonssikkerhet**
Are Vegard Haug ..... *NOK 420,-*

1/06 **Anti-spam Legislation Between Privacy And Commercial Interest. An overview of the European Union legislation regarding the e-mail spam**
Dana Irina Cojocarasu ..... *NOK 155,-*

2005

1/05 **Renessansen som unnfanget Corpus Iuris Civilis. Keiser Justinians gjenerobring av Romerriket**
Halvor Manshaus ..... *NOK 249,-*

2/05 **Personvern og ytringsfrihet. Fotografering av siktede i straffesaker – et vern for ytringsfrihet?**
Anette Engum ..... *NOK 132,-*

3/05 **Rettigheter til geografisk informasjon. Opphavsrett, databasevern og avtalepraksis.**
Steinar Taubøll.....*NOK 206,-*

4/05 **«The Answer to the Machine is in the Machine» and Other Collected Writings**
Charles Clark.....*NOK 401,-*

5/05 **Digital Rights Management – Promises, Problems and Alternative Solutions**
Kristian Syversen.....*NOK 201,-*

6/05 **DRM og Demokrati. Argumentasjoner, rettferdiggjøringer og strategier bak endringen av åndsverksloven 2003–2005**
Jan Frode Haugseth .....*NOK 224,-*

2004

1/04 **Opphavsrettslige problemstillinger ved universitetene og høyskolene. Innstilling fra immaterialrettsutvalget, oppnevnt av Universitets- og Høgskolerådet 31. januar 2000. Avgitt til universitets- og høgskolerådet 8. oktober 2003**
Immaterialrettsutvalget.....*NOK 341,-*

2/04 **Ansvarsfrihet for formidler ved formidling av informasjonssamfunnstjenester**
Bård Standal.....*NOK 311,-*

3/04 **Arbeidsgivers adgang til å kontrollere og overvåke sine ansatte med hovedvekt på grunnvilkårene for behandling av personopplysninger i arbeidslivet**
Stefan Jørstad.....*NOK 191,-*

4/04 **Elektroniske spor fra mobiltelefoner – om politiets bruk og teleoperatørenes lagring av trafikkdata.**
Christian Dahlgren .....*NOK 117,-*

5/04 **International Jurisdiction and Consumers Contracts – Section 4 of the Brussels Jurisdiction Regulation.**
Joakim S. T. Øren.....*NOK 172,50*

6/04 **Elektronisk dokumentfalsk.**
Lars Christian Sunde.....*NOK 60,502003*

2003

1/03 IT i domstolene. En analyse av norske domstolers teknologianvendelse fra 1970 til 2001
Even Nerskogen.....*NOK 330,-*

2/03 Hvorfor vokser Norsk Lovtidend? En empirisk analyse av veksten
Martin Støren.....*NOK 87,-*

3/03 Etableringslandsprinsippet. En analyse av e-handelsdirektivet art 3 og prinsippet om fri bevegelighet av tjenester ved elektronisk handel
Jon Christian Thaulow.....*NOK 213,-*

4/03 The Law of Electronic Agents. Legal contributions to ALFEBIITE – A Logical Framework for Ethical Behaviour between Infohabitants in the Information Trading Economy of the Universal Information Ecosystem, IST-1999–10298
Jon Bing and Giovanni Sartor (eds) .....*NOK 351,-*

5/03 LEA 2003: The Law and Electronic Agents Proceedings of the Second LEA Workshop, 24th June 2003, in connection with the ICAIL 2003 Conference (Ninth International Conference on Artificial Intelligence and Law), Edinburgh, Scotland, UK
Seminarrapport).....*NOK 228,-*

6/03 Opphavsrettslige aspekter ved nettbasert formidling av musikk
Stig Walle .....*NOK 153,-*

7/03 Sceneinstruktørens opphavsrettslige stilling
Edle Endresen.....*NOK 119,-*

8/03 User-Centred Privacy Aspects In Connection With Location Based Services
Christian B. Hauknes.....*NOK 203,-*

2002

1/02 Koblingshandel og forholdet til fysisk og teknologisk integrasjon i relasjon til EØS-avtalens art.54(d)
Ole Jacob Garder.....*NOK 180,-*

2/02 **To opphavsrettslige arbeider:**
Bjarte Aambø – Opphavsrettslige rettsmangler
Erlend Ringnes Efskind – Skjermbildets rettslige natur
Aambø / Ringnes Efskind.....*NOK 201,-*

3/02 **Arbeidstakeroppfinnelser ved universiteter og høyskoler. Innstilling fra et utvalg oppnevnt av universitets- og høgskolerådet 31 januar 2000. Avgitt til universitets- og høgskolerådet i oktober 2001**
.....*NOK 213,-*

4/02 **Utøvende kunstneres direkteoverføringer på Internett – med hovedvekt på kringkastingsbegrepet**
Irina Eidsvold Tøien .....*NOK 225,-*

5/02 **Administrasjon av radiofrekvensspekteret. Rettslige problemstillinger knyttet til telemyndighetenes forvaltning av frekvensressursene**
Øyvind Haugen .....*NOK 177,-*

6/02 **Overføring av personopplysninger til tredjeland. Kravet til tilstrekkelig beskyttelse etter EU-direktivet om personvern art. 25**
Mona Naomi Lintvedt og Christopher J. Helgeby.....*NOK 198,-*

7/02 **Digitale mellomledds ansvar for videreformidling av ytringer. E-handelsdirektivet art. 12–14**
Just Balstad.....*NOK 186,-*

8/02 **Platekontrakten. Eksklusive overdragelser av utøverens rettigheter til eksemplarfremstilling og spredning**
Øyvind Berge.....*NOK 237,-*

9/02 **Varemerkerettslige konflikter under .no. I hvilken grad kan registrering og bruk av et domenenavn medføre inngrep i en varemerkerett? Hvordan løses konflikter under .no i dag, og hva kan være en mer hensiktsmessig tvisteløsningsmekanisme i fremtiden?**
Silje Johannessen.....*NOK 192,-*

10/02 Vegard Hagen – Pekeransvar. Spørsmålet om ansvar for publisering av pekere på verdensveven (World Wide Web) Hans Marius Graasvold – Pekeransvaret. Straffe- og erstatningsansvar for publisering av pekere til informasjon på Internett
Vegard Hagen / Martin Grasvold.....*NOK 234,-*

11/02 Personopplysningsloven § 7. En analyse av forholdet mellom personvern og ytringsfrihet slik det er uttrykt i person-opplysningsloven § 7
Karen Elise Haug Aronsen.....*NOK 198,-*

12/02 Databasevern. Sui generis-vern av sammenstillinger etter gjennomføringen av databasedirektivet i åndsverkloven § 43
Lisa Vogt Lorentzen.....*NOK 210,-*

2001

1/01 Internet and Choice-of-Law – The International Sale of Digitised Products through the Internet in a European Context
Peter Lenda.....*NOK 275,-*

2/01 Internet Domain Names and Trademarks
Tonje Røste Gulliksen.....*NOK 227.-*

3/01 Internasjonal jurisdiksjon ved elektronisk handel – med Luganokonvensjonen art 5 (5) og elektroniske agenter som eksempel
Joakim S. T. Øren.....*NOK 204.-*

4/01 Legal issues of maritime virtual organisations
Emily M. Weitzenböck.....*NOK 164.-*

5/01 Cyberspace jurisdiction in the U.S. – The International Dimension of Due Process
Henrik Spang-Hanssen.....*NOK 685.-*

6/01 Norwegian border control in a Europe without Internal Frontiers – Implications for Data Protection and civil liberties
Stephen Kabera Karanja.....*NOK 252,-*

2000

1/00 **Klassikervernet i norsk åndsrett**
Anne Beth Lange ..... *NOK 268.-*

2/00 **Adgangen til å benytte personopplysninger. Med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor**
Claude A. Lenth..... *NOK 248.-*

3/00 **Innsyn i personopplysninger i elektroniske markedsplasser.**
Line Coll..... *NOK 148.-*

1999

1/99 **International regulation and protection of Internet domain and trademarks**
Tonje Røste Gulliksen..... *NOK 248.-*

2/99 **Betaling via Internett**
Camilla Julie Wollan..... *NOK 268.-*

3/99 **Internett og jurisdiksjon**
Andreas Frølich Fuglesang & Georg Philip Krog..... *NOK 198.-*

1998

1/98 **Fotografiske verk og fotografiske bilder, åndsverkloven § 1 og § 43 a**
Johan Krabbe-Knudsen..... *NOK 198.-*

2/98 **Straffbar hacking, straffelovens § 145 annet ledd**
Guru Wanda Wanvik..... *NOK 238.-*

3/98 **Interconnection – the obligation to interconnect telecommunications networks under EC law**
Katinka Mahieu ..... *NOK 198.-*

1997

1/97 **Eksemplarfremstilling av litterære verk til privat bruk**
Therese Steen ..... *NOK 158.-*

2/97 **Offentlige anskaffelser av informasjonsteknologi**
Camilla Sivesind Tokvam ..... *NOK 175.-*

3/97 **Rettslige spørsmål knyttet til Oppgaveregisteret**
Eiliv Berge Madsen ..... *NOK 170.-*

4/97 **Private pengespill på Internett**
Halvor Manshaus ..... *NOK 160.-*

5/97 **Normative Structures in Natural and Artificial Systems**
Christen Krogh ..... *NOK 255.-*

6/97 **Rettslige aspekter ved digital kringkasting**
Jon Bing ..... *NOK 178.-*

7/97 **Elektronisk informasjonsansvar**
Tomas Myrbostad *NOK148.-*

8/97 **Avtalelisens etter åndsverksloven § 36**
Ingrid Mauritzen ..... *NOK 120.-*

9/97 **Krav til systemer for forvaltning av immaterielle rettigheter**
Svein Engebretsen ..... *NOK 168.-*

10/97 **American Telephony: 120 Years on the Road to Full-blown Competition**
Jason A. Hoida ..... *NOK 140.-*

11/97 **Rettslig vern av databaser**
Harald Chr Bjelke ..... *NOK 358.-*

1996

1/96 **Innsynsrett i elektronisk post i offentlig forvaltning**
Knut Magnar Aanestad og Tormod S. Johansen ..... *NOK 218.-*

2/96 **Public Policy and Legal regulation of the Information Market in the Digital Network Enviroment**
Stephen John Saxby ..... *NOK 238.-*

3/96 **Opplysning på spill**
Ellen Lange ..... *NOK 218.-*

4/96 **Personvern og overføring av personopplysninger til utlandet**
Eva I. E. Jarbekk ..... *NOK 198.-*

5/96 **Fjernarbeid**
Henning Jakhelln ..... *NOK 235.-*

6/96 **A Legal Advisory System Concerning Electronic Data Interchange within the European Community**
Andreas Mitrakas..... *NOK 128.-*

7/96 **Elektronisk publisering: Utvalgte rettslige aspekter**
Jon Bing og Ole E. Tokvam ..... *NOK 186.-*

8/96 **Fjernsynsovervåking og personvern**
Finn-Øyvind H. Langfjell..... *NOK 138.-*

1995

1/95 **Rettslige konsekvenser av digitalisering: Rettighetsadministrasjon og redaktøransvar i digitale nett**
Jon Bing..... *NOK 368.-*

2/95 **Rettslige spørsmål i forbindelse med utvikling og bruk av standarder innen telekommunikasjon**
Sverre Sandvik ..... *NOK 178.-*

3/95 **Legal Expert Systems: Discussion of Theoretical Assumptions**
Tina Smith ..... *NOK 278.-*

4/95 **Personvern og straffeansvar – straffelovens § 390**
Ole Tokvam..... *NOK 198.-*

5/95 **Juridisk utredning om filmen «To mistenkelige personer»**
Johs. Andenæs ..... *NOK 138.-*

6/95 **Public Administration and Information Technology**
Jon Bing and Dag Wiese Schartum ..... *NOK 348.-*

7/95 **Law and Liberty in the Computer Age**
Vittorio Frosini ..... *NOK 158.-*

1994

1/94 **Deon'94, Second International Workshop on Deontic Logic in Computer Science**
Andrew J. I. Jones & Mark Sergot (ed) ..... *NOK 358.-*

2/94 **Film og videogramrett. TERESA (60)**
Beate Jacobsen ..... *NOK 318.-*

3/94 **Elektronisk datutveksling i tollforvaltingen – Rettslige spørsmål knyttet til TVINN**
Rolf Risnæs ..... *NOK 225.-*

4/94 **Sykepenger og personvern – Noen problemstillinger knyttet til behandlingen av sykepenger i Infotrygd**
Mari Bø Haugestad ..... *NOK 148.-*

5/94 **EØS, medier og offentlighet. TERESA (103)**
Mads Andenæs, Rolf Høyer og Nils Risvand ..... *NOK 148.-*

6/94 **Offentlige informasjonstjenester: Rettslige aspekter**
Jon Bing *NOK148.-*

7/94 **Sattelittfjernsyn og norsk rett. MERETE (3) IV**
Nils Eivind Risvand ..... *NOK 138.-*

8/94 **Videogram på forespørsel. MERETE (14) IV**
Beate Jacobsen (red) ..... *NOK 158.-*

9/94 **«Reverse engineering» av datamaskinprogrammer. TERESA (92) IV**
Bjørn Bjerke ..... *NOK 198.-*

10/94 **Skattemessig behandling av utgifter til anskaffelse av datamaskinprogrammer. TERESA (75)**
Gjert Melsom ..... *NOK 198.-*

1993

1/93 **Artificial Intelligence and Law. Legal Philosophy and Legal Theory**
Giovanni Sartor ..... *NOK 148.-*

2/93 **Erstatningsansvar for informationstjenester, særlig ved databaseydelser**
Connie Smidt ..... *NOK 138.-*

3/93 **Personvern i digitale telenett**
Ingvild Hanssen-Bauer ..... *NOK 178.-*

4/93 **Consumers Purchases through Telecommunications in Europe. – Application of private international law to cross-border contractual disputes**
Joachim Benno ..... *NOK 198.-*

5/93 **Four essays on: Computers and Information Technology Law**
Morten S. Hagedal ..... *NOK 218.-*

6/93 **Sendetidsfordeling i nærradio MERETE (3) III**
Marianne Rytter Evensen ..... *NOK 148.-*

7/93 **Essays on Law and Artificial Intelligence**
Richard Susskind ..... *NOK 158.-*

1992

1/92 **Avskriving av mikrodatamaskiner med tilbehør – en nordisk studie TERESA (87)**
Beate Hesseltvedt ..... *NOK 138.-*

2/92 **Kringkastingsbegrepet TERESA (78)**
Nils Kr. Einstabland ..... *NOK 208.-*

3/92 **Rettskilderegistre i Helsedirektoratet NORIS (94) I & II**
Maria Strøm ..... *NOK 228.-*

4/92 **Softwarepatent – Imaterialrettens enfant terrible. En redegjørelse for patenteringen af softwarerelaterede opfindelser i amerikansk og europæisk ret**
Ditlev Schwanenfügel ..... *NOK 158.-*

5/92 **Abonnementskontrakter fro kabelfjernsyn TERESA (78II)**
Lars Borchgrevink Grindal ..... *NOK 248.-*

6/92 **Implementing EDI – a proposal for regulatory form**
Rolf Riisnæs ..... *NOK 118.-*

7/92 Deponering av kildekode»escrow»-klausuler TERESA (79)
Morten S. Hagedal.....*NOK 128.-*

8/92 EDB i juridisk undervisning – med en reiserapport fra England og USA
Ola-Kristian Hoff.....*NOK 228.-*

9/92 Universiteters ansvar for bruk av datanett TERESA (94)
Jon Bing & Dag Elgesem.....*NOK 198.-*

10/92 Rettslige sider ved teletorg
Andreas Galtung.....*NOK 148.-*

BESTILLING

Jeg bestiller herved følgende CompLex-utgivelser:

Number / year: _____
Title: _____

Number / year: _____
Title: _____

Number / year: _____
Title: _____

Number / year: _____
Title: _____

Number / year: _____
Title: _____

Name: _____
Adress: _____
Zip code: _____
Telephone number: _____

The reports can be ordered from Akademika:

akademika"

Avd. juridisk litteratur Aulabygningen
Karl Johansgt. 47, 0162 Oslo
Telefon: 22 42 54 50
Telefaks: 22 41 17 08
(www.akademika.no) or Unipub (www.unipub.no)