The impact of the European privacy regime on indoor and outdoor location technology development: the new challenges in light of the future EU General Data Protection Regulation

Rome, 21 January 2016

Prof. Avv. . Alessandro del Ninno
adelninno@luiss.it
www.alessandrodelninno.it
The growing popularity of location-based services such as GNSS (Global Navigation Satellite System) navigation and the exploration of a user’s location gives rise to severe privacy concerns:

Big Data:

i. the data coming from Earth Observation operations over the next three years will be larger than the total collected by ESA in the last 30 years;

ii. Smartphones are by far the most popular platform to access location-based services (LBS). Most of these users are the general public, who agree to trade their privacy and data ownership for the convenience and functionality of “always on” location services.
The number of smartphone users worldwide will surpass 2 billion in 2016: smartphone users across the globe is expected near 2.16 billion this year. By 2018, over one-third of consumers worldwide, or more than 2.56 billion people, will use a smartphone: over half — 51.7%— of all mobile phone users shall be a smartphone user, so that feature phones will have finally become a minority in the telecommunications world (source: eMarketer).
iii) In 2014, there were an estimated 3.6 billion GNSS devices globally. This number is forecasted to increase to 7 billion (source: GSA).

As European Space Policy – and EU satellite navigation systems in particular – shift from technology and systems development to services and applications, the need for an appropriate and reliable regulatory and legal data protection framework is clear and it is the success key.
THE REGULATORY DATA PROTECTION APPROACH TO LOCATION-BASED SERVICES: AN OVERVIEW OF THE EUROPEAN DATA PROTECTION LAW RULES
AN OVERVIEW OF THE EUROPEAN DATA PROTECTION LAW RULES APPLICABLE TO LOCATION-BASED SERVICES

Data processing within the provision of GNNS location-based services implies three different perspectives regarding the protection of the interested subject’s personal data:

I. towards data processors represented by public authorities (ex: GALILEO Public Regulated Service (PRS) limited to authorized governmental bodies);
II. towards data processors represented by private providers of location-based services (ex: the electronic communication operators processing data by means of base stations and receivers);
III. towards other public or private third parties receiving the data from the above data processors.
The protection of personal data remains an important concern for EU citizens, according to a new Eurobarometer published by the European on data protection in 2015.

The central finding of the survey shows that trust in digital environments remains low. Two-thirds of the respondents (67%) say that they are worried about having no control over the information they provide within the electronic communication networks, while only 15% feel they have complete control.

At the same time, six out of ten respondents say that they do not trust online businesses (63%), or phone companies and internet service providers (62%).

Furthermore, citizens overwhelmingly believe that the protection of personal data should not be confined by borders. Nine out of ten Europeans (89%) believe that they should have the same level of protection over their personal information, regardless of the country in which the authority or private company processing their data is based.
There are a number of aspects of electronic data processing (and related eventual surveillance) made possible by the accurate GNSS technologies that raise privacy concerns (anyway assessed by the privacy laws).

Electronic data processing (and related eventual surveillance) may be:

a) **Hidden**: it may not be possible to detect the data processing;

b) **Intrusive**: the capabilities of the new technologies increase the intrusiveness (they can "see" almost anything and everything);

c) **Indiscriminate**: the capabilities of the new technologies resulting in an over-collection of information; and

d) **Continuous**: the capabilities of the new technologies may effectively create continuous surveillance of any given receiver/device.
ASPECTS OF ELECTRONIC SURVEILLANCE MADE POSSIBLE BY THE ACCURATE GNSS TECHNOLOGIES THAT RAISE PRIVACY CONCERNS

These characteristics give rise to some specific privacy concerns:

a) **Mission creep**: meaning in general that the tendency for a task to become unintentionally wider in scope than its initial objectives which applied to data protection could mean that it seems inevitable that other privacy-invasive uses would be found for such technology;

b) **Tracking**: the ability to maintain surveillance over an extended area for an extended period of time raises the possibility that individuals and vehicles could be tracked on an on-going basis;

c) **Proliferation**: as the cost of these technologies is rapidly falling.
Is there a comprehensive, organic and reliable data protection legal framework at a European level suitable for assessing all the privacy issues and concerns related to the protection of privacy within the GNSS?
AN OVERVIEW OF THE EUROPEAN DATA PROTECTION LAW RULES APPLICABLE TO LOCATION-BASED SERVICES

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;

Regulation (EU) no xxx/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);


THE REGULATION 45/2001/EC ON THE PROCESSING OF PERSONAL DATA BY COMMUNITY INSTITUTIONS AND BODIES
REGULATION (EC) NO 45/2001

Grounding Principle

The institutions and bodies set up by, or on the basis of the European Treaties establishing the European Communities, (globally the “Community institutions or bodies”, shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States.

The Regulation shall apply to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.
Main definitions

**personal data**: any information relating to an identified or identifiable natural person; 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 or her physical, physiological, mental, economic, cultural or social identity;

**processing of personal data**: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

**personal data filing system**: any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
Main definitions

**Controller:** the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Community act, the controller or the specific criteria for its nomination may be designated by such Community act;

**Processor:** a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
REGULATION (EC) NO 45/2001

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Personal data must be:

(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.
REGULATION (EC) NO 45/2001

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Personal data may be processed only if:

(a) processing is necessary for the performance of a task carried out in the public interest on the basis of the EU Treaties or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or
(b) processing is necessary for compliance with a legal obligation to which the controller is subject, or
(c) 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, or
(d) the data subject has unambiguously given his or her consent, or
(e) processing is necessary in order to protect the vital interests.
Transfer of personal data

Personal data may only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient.

Personal data may only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest.

Personal data may only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out.
Exemptions and restrictions

The Community institutions and bodies may restrict the application of the rules related to data processing principles, information to be given to the data subject, rights of data subject (access, rectification, blocking, etc) where such restriction constitutes a necessary measure to safeguard:

(a) the prevention, investigation, detection and prosecution of criminal offences;
(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;
(c) the protection of the data subject or of the rights and freedoms of others.
(d) the national security, public security or defence of the Member States;
(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority.
SECURITY

The Community institutions and bodies take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks.

Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

In the event of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.
THE GENERAL DATA PROTECTION REGULATION AND THE EU REFORM OF THE EUROPEAN LEGAL FRAMEWORK ON PRIVACY
On December 2015 the European Parliament and Council have reached agreement on the data protection reform proposed by the Commission in 2012.

The reform is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market.

Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 28 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement.

A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year.
Relationship with the Regulation 45/2001/EC

For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies.

Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation.
Territorial scope

The Regulation applies:

I. to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not;

I. to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

III. to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.
personal data: 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 identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

profiling: any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
GENERAL DATA PROTECTION REGULATION

Main definitions

**pseudonymisation**: means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person;

**personal data breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

**Information Society service**: any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
Controller: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

Processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
GENERAL DATA PROTECTION REGULATION

The main law rules principles affecting the GNSS location-based principles: the privacy by design

‘Data protection by design’ is now an essential element in EU data protection rules. Data protection safeguards will be built into products and services from the earliest stage of development:

Art. 23.1

Having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
The eCall emergency response service

From 31 March 2018, all manufacturers of cars to be sold in Europe will be required to equip their new models with an in-vehicle GNSS-based eCall device. The wireless system will automatically trigger a distress signal to the 112-based eCall interoperable service in the event of an accident, using EGNOS and GALILEO to indicate the precise location of the incident.

Vehicles equipped with the system will not be subject to constant tracking, and data on the location of the vehicle will be continuously erased. The eCall system remains dormant until either manually activated or automatically activated following a serious accident, therefore no tracking or transmission of data takes place during the normal operation of the system. Nor will any data be communicated to third parties without the specific consent of the vehicle owner.
The main law rules principles affecting the GNSS location-based principles: the privacy by default

‘Data protection by default’ is an essential element as well, since privacy-friendly default settings will be the norm – for example on social networks or mobile apps.

Art. 23.2

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of individuals.
GENERAL DATA PROTECTION REGULATION

The main law rules principles affecting the GNSS location-based principles: the data protection impact assessment

In order to enhance compliance with the Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller is responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of this risk. The outcome of the assessment must be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with the Regulation. Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the
GENERAL DATA PROTECTION REGULATION

The main law rules principles affecting the GNSS location-based principles: the data protection impact assessment

‘A data protection impact assessment is in particular be required, amongst the others, in the following cases:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling;

(b) processing on a large scale of special categories of data;

(c) a systematic monitoring of a publicly accessible area on a large scale.
GENERAL DATA PROTECTION REGULATION

The main law rules principles affecting the GNSS location-based principles: the data protection impact assessment

The assessment contains at least:

(a) a **systematic description** of the envisaged processing operations and the **purposes of the processing**, including where applicable the legitimate interest pursued by the controller;

(b) an assessment of the **necessity and proportionality** of the processing operations in relation to the purposes;

(c) an assessment of the **risks to the rights and freedoms of data subjects**;

(d) the **measures envisaged to address the risks**, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
GENERAL DATA PROTECTION REGULATION

The main law rules principles affecting the GNSS location-based principles: the data protection impact assessment

The controller shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Where the supervisory authority is of the opinion that the intended processing would not comply with the Regulation, in particular where the controller has insufficiently identified or mitigated the risk, it shall within a maximum period of eight weeks following the request for consultation give advice to the data controller and may use any of its powers (ex: banning the data processing).
GENERAL DATA PROTECTION REGULATION

The main law rules principles affecting the GNSS location-based principles: Data security

Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor must implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, including inter alia, as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
GENERAL DATA PROTECTION REGULATION

The main law rules principles affecting the GNSS location-based principles: Data security

(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
GENERAL DATA PROTECTION REGULATION

The main law rules principles affecting the GNSS location-based principles: Notification of personal data breach

In the case of a personal data breach ("breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"), the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.

The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.
The controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment; and

(f) any other information requested by the supervisory authority.
The controller and the processor shall designate a data protection officer, amongst the others, in any case where:

the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

The data protection officer may be a staff member of the controller or processor, or fulfill the tasks on the basis of a service contract.

A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each
Article 89
Relationship to Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.
OPINION 13/2011 ON GEOLOCATION SERVICES ON SMART MOBILE DEVICES
Opinion 13/2011 on Geolocation services on smart mobile devices

The objective of the opinion is to clarify the legal framework applicable to geolocation services that are available on and/or generated by smart mobile devices that can connect with the Internet and are equipped with location sensitive sensors such as GPS.

Examples of such services are: maps and navigation, geopersonalised services (including nearby points of interests), augmented reality, geotagging of content on the Internet, tracking the whereabouts of friends, child control and location based advertising.

The opinion also deals with the main three types of infrastructure used to provide geolocation services, namely GPS, GSM base stations and WiFi. Special attention is paid to the new infrastructure based on the location of WiFi access points.
Opinion 13/2011 on Geolocation services on smart mobile devices

Given the rapid technological developments with regard to especially the mapping of wireless access points, in combination with the fact that new market entrants are preparing to develop new location based services based on a combination of base station, GPS and WiFi data, the Working Party has decided to specifically clarify the legal requirements for these services under the data protection directive.
Opinion 13/2011 on Geolocation services on smart mobile devices

The relevant legal framework is the data protection directive (95/46/EC) and – soon to be – the General Data protection Regulation. It applies in every case where personal data are being processed as a result of the processing of location data.

The e-privacy directive (2002/58/EC, as revised by 2009/136/EC) only applies to the processing of base station data by public electronic communication services and networks (telecom operators) with reference to the:

i. “location data” meaning any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

ii. the combination of the unique MAC address and the calculated location of a WiFi access point.
Opinion 13/2011 on Geolocation services on smart mobile devices

Data Controllers

Three types of controllers can be discerned. They are:

i. controllers of geolocation infrastructure (in particular controllers of mapped WiFi access points);

ii. providers of geolocation applications and services;

iii. developers of the operating system of smart mobile devices.
Opinion 13/2011 on Geolocation services on smart mobile devices

Legitimate ground

Because location data from smart mobile devices reveal intimate details about the private life of their owner, the main applicable legitimate ground is prior informed consent.

Consent cannot be obtained through general terms and conditions.

Consent must be specific, for the different purposes that data are being processed for, including for example profiling and or behavioural targeting purposes from the controller.
By default, location services must be switched off. A possible opt-out mechanism does not constitute an adequate mechanism to obtain informed user consent.

The Working Party recommends:

i. limiting the scope of consent in terms of time and remind users at least once a year;

ii. sufficient granularity in the consent with regard to the precision of the location data.
With regard to the mapping of WiFi access points, companies can have a legitimate interest in the necessary collection and processing of the MAC addresses and calculated locations of WiFi access points for the specific purpose of offering geolocation services.

The balance of interests between the rights of the controller and the rights of the data subjects requires that the controller offers the right to easily and permanently opt-out from the database, without demanding additional personal data.
Opinion 13/2011 on Geolocation services on smart mobile devices

Information must be clear, comprehensive, understandable for a broad, non-technical audience and permanently and easily accessible. The validity of consent is inextricably linked to the quality of the information about the service.

Retention periods

Providers of geolocation applications or services should implement retention policies which ensure that geolocation data, or profiles derived from such data, are deleted after a justified period of time.

If the developer of the operating system and/or controller of the geolocation infrastructure processes a unique number such as a MAC address or a UDID in relation to location data, the unique identification number may only be stored for a maximum period of 24 hours, for operational purposes.
Data Subjects’ rights.

The different controllers of geolocation information from mobile devices should enable their customers to obtain access to their location data in a human readable format and allow for rectification and erasure without collecting excessive personal data.

Data subjects also have a right to access, rectify and erase possible profiles based on these location data.
THANK YOU!

Prof. Avv. Alessandro del Ninno

www.alessandrodelninno.it

adelninno@luiss.it