BHO LEGAL

Space and Data Protection

GLIS, 7 June 2016

Introduction

Space Policies all around the globe put emphases on space services supporting growth, jobs, innovation and competitiveness.

Technology advances lead to new space services potentials.

Increasing convergence of space services with other technologies and sectors, namely ICT and the Geospatial.

Increasing concerns of the public on privacy-invasive technologies and services, e.g. Google Earth, Google Street View, Location Based Services, Geo-Marketing, Cloud Computing, UAV/RPAS.

What about “Big Brother from Space”?

Data Protection and Satellite Communications

It is no secret that satellite communications can be intercepted. However, Interception is prohibited by international law and national law.

Article 37 of the ITU Constitution: "*Member States agree to take all possible measures, compatible with the system of telecommunications used, with a view to ensuring secrecy of international correspondence.*"

Article 17 (Secrecy) of the ITU Radio Regulation:

> *"In the application of the appropriate provisions of the Constitution and the Convention, administrations bind themselves to take the necessary measures to prohibit and prevent:*
>
> *a) the unauthorized interception of radiocommunications not intended for the general use of the public;*
>
> *b) the divulgence of the contents, simple disclosure of the existence, publication or any use whatever, without authorization of information of any nature whatever obtained by the interception of the radiocommunications mentioned in No. 17.2.*

Interception of satellite communications is mainly done by intelligence and law enforcement agencies, (hopefully) complying with the applicable national laws.

Data Protection and Earth Observation

Objectively, EO data per se are not very sensitive with regard to personal data.

The most advanced commercial imaging sensors provide a spatial resolution of around 30 cm (WorldView-3 image data from DigitalGlobe). With such resolution, it is not possible to directly identify an individual person from space.

Due to the high speed of low-orbiting satellites, a specific scene can only be captured for a short time – it takes then at least one orbit until revisit of the same scene. Therefore, it is not (yet) possible to "track" movements of individuals in real-time.

However, high-resolution optical data, depending on their spatial resolution, may have the same quality as aerial photography and therefore may raise respective privacy issues.

In addition, as for all types of geospatial data, EO data may be combined with other data sets and then may raise privacy concerns, even if the raw or pre-processed data as such do not.

Data Protection and Earth Observation

No specific national legislation exists worldwide addressing privacy concerns of EO data.

The German Satellite Data Security Act, which so far is unique in Europe , addresses national security and foreign policy interests of Germany with regard to VHR.

Some indications may however be derived from works by national authorities. A German data protection authority (ULD) clarified that EO data generally fall under the applicable legal framework for personal data protection. It however, noted that there are no generalized criteria to determine whether EO data are related to an identified or identifiable person. The pure mass of EO data collected by satellites does not allow an individual check of each data set, but rather requires a generalized normative approach.

To provide certain reliability for data providers, the ULD proposed that the legislator should determine a level of geometric resolution, beyond which the legitimate public and private interests to access EO data generally are considered as outweighing the interests of a data subject. This level of resolution was initially proposed to be 40 cm pixel.

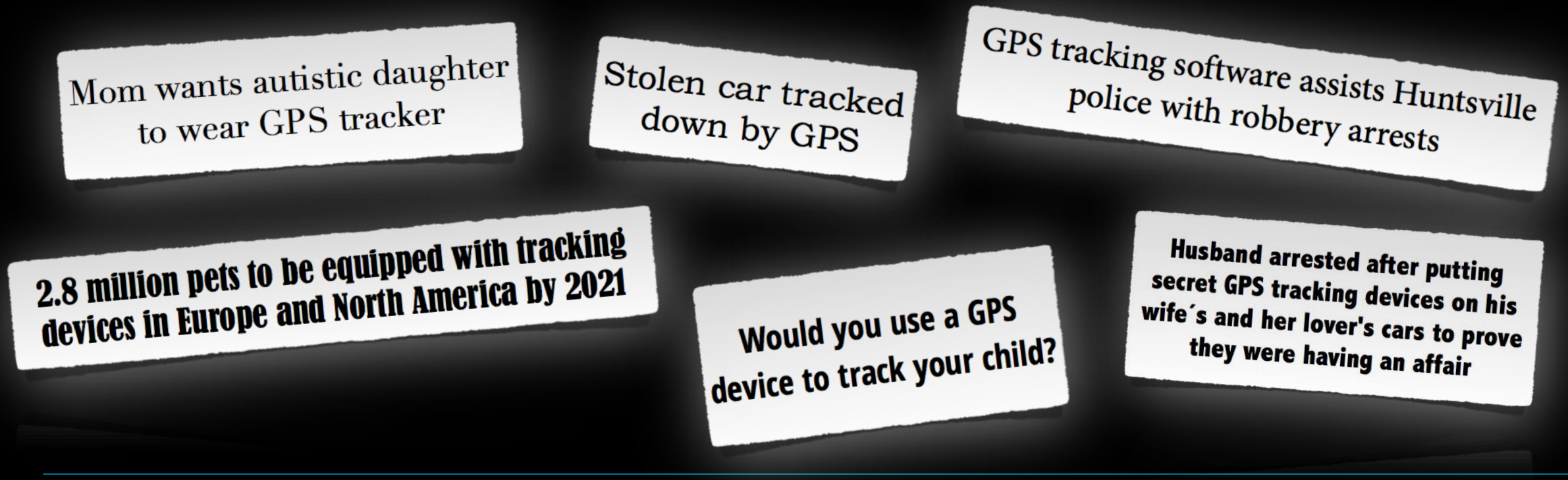
More recently, the ULD tends to apply an even more relaxed approach proposing a threshold of 20 cm pixel size resolution. The German Council for Social and Economic Data has subsequently adopted the 20 cm threshold.

Data Protection and Satellite Navigation

Satellite navigation is certainly the most privacy-invasive type of space services.

GNSS can be used to locate and track individuals with accuracy of few meters, if not centimeters.

GNSS tracking is widely used by law enforcement and other public agencies, but also by companies and individuals.



Data Protection and Satellite Navigation

Case law on diverse forms of GNSS tracking is rapidly evolving around the globe, most visible in the US:

Data Protection and Space (Programme) Legislation:

The European GNSS Regulation (Regulation (EU) No 1285/2013) includes an article data and privacy protection (Art. 37) providing that:

1. *The Commission shall ensure that personal data and privacy are protected during the design, implementation and exploitation of the systems and that the appropriate safeguards are included therein.*
2. *All personal data handled in the context of the tasks and activities provided for in this Regulation shall be processed in accordance with the applicable law on personal data protection, , …*

The Copernicus Delegated Regulation (Regulation EU) No 1159/2013) includes an article on conflicting rights (Art. 11) stating that:

"Where the open dissemination of certain GMES dedicated data or GMES service information……would affect in a disproportionate manner the rights and principles recognized in the Charter of Fundamental Rights of the EU, such as the right for private life or the protection of personal data, the Commission shall take the necessary measures …..to avoid any such conflict or to restrict the dissemination of the GMES dedicated data or GMES service information in question."

Conclusions

Space services converge with other technologies and services, such as mobile communications services, location based services, or geospatial services. GNSS is installed in virtually all modern smartphone devices.

EO data and GNSS-based positioning data are increasingly merged with other types of datasets, including geospatial data, social data, statistical data etc. Technology allows powerful data analytics.

EO data as such are not very sensitive with regard to personal data. However, high-resolution optical data, depending on their spatial resolution, may have the same quality as aerial photography and therefore may raise respective privacy issues.

No specific national legislation exists worldwide addressing privacy concerns of EO data.

Satellite navigation is highly sensitive with regard to personal data. GNSS tracking is increasingly used by law enforcement agencies, but also by companies and individuals. Courts around the globe are called to decide on the lawfulness of GNSS tracking under the applicable national law.

Programme-related legislation and space contracts start to include provisions on data protection.

It is time for the space industry to familiarize with applicable data protection laws!

Contact

www.bho-legal.com