MedCrave
Step into the World of Research
Aeronautics and Aerospace Open Access Journal

Mini Review

Open Access
CrossMark

Lost in GNSS: a need for commercial space policy for positioning, navigation and timing

Abstract

Global Navigation Satellite System (GNSS) has seen a rapid and tremendous growth. GNSS is one of the best space applications that have been commercialized very well resulting in numerous digital applications available in the market. Any rapid growth has to be checked, regulated and contained properly. There is an awareness increase by the public that causes concern among the users being exploited in privacy by the Data Analyst Society. This article deals with the roles to be played by the public, regulators and the lawmakers in understanding the GEOSPATIAL information and how this information is collected, analyzed and processed that imposes privacy risk. The article also identifies the liability for the GNSS signals and information technology driven by space platforms. GNSS has millions of users due to its capability of replicating its receivers in mobile phones at very cheap cost. GNSS has many unresolved legal issues enclosing its operations, applications, and facilitation. Autonomous transport systems such as Unmanned Aerial Vehicle (UAV) and auto-steering cars also incorporate GNSS. GNSS failure may cause loss of life, injuries, material and financial damage. In conclusion, recommendations and future prediction of GNSS markets were done.

Keywords: GNSS, data analyst society, privacy, international law regulators, UAV

Volume 3 Issue 3 - 2019

Aurthur Vimalachandran Thomas Jayachandran,[1] Oluwafemi Funmilola Adebisi[2]
[1]Department of Space Technology, Samara University, Russia
[2]Space Physical and Life Science Unit, Engineering and Space Systems Department (ESS), National Space Research and Development Agency (NASRDA), Nigeria

Correspondence: Aurthur Vimalachandran Thomas Jayachandran, Department of Space Technology, Samara University, Moskovskoye sh., 34, Samara, Samarskaya oblast', Russia, 443086, Email aurthur01@gmail.com

Received: August 21, 2019 | **Published:** September 17, 2019

Abbreviations: GNSS, global navigation satellite system; UAV, unmanned aerial vehicle; IS, interface specification; PS, standard of performance; GPS, global positioning system; ITU, international telecommunication union; ASDV, autonomous self-driving vehicle

Introduction

Space activities are majorly categorized in three sectors as national security, commercial application, and civil applications. These entire industry sectors are overlapped with same technology protocol. However, for Global Navigation Satellite System (GNSS), there is a very thin layer between these domains in aiding the function of GNSS. Creation of money in the space industry is majorly from the back and forth of signals from satellites. These uplink and downlink signals carries data, thus the value of the information carried by this signal creates revenue. GNSS has been a great commercial success because its necessity is driven by both public and government.[1]

The technology of navigation by the means of satellite signals is present widely due to its commercial technologies. Navigation services are essential for automotive, ships, smartphones, railways, airlines etc. The need of GNSS is so vast that many countries are keying into the segment. Currently the navigation systems are provided by BeiDou and Compass of China, DORIS of France, Galileo of the EU, GLONASS of Russia, GPS of the United States of America, IRNSS of India and QZSS of Japan.[2] The signals from the satellite are sent continuously at constant intervals. The accuracy of the signals has external impacts such as the solar storms and the impact of the ionosphere, weather, space debris, reflected signals and malfunctioning devices. The inaccurate clock signals would cause damages to the services which may be physical or monetary. One such example is the failed rescue operation due to bad navigation signals. This is where liability questions arise. The GNSS operators or the signal receiver manufacturers are held to compensate for losses.

The important goals of GNSS providers are to predict the errors and mitigate the errors of the signals. The operators of GNSS provide Interface Specification (IS) and standard of Performance (PS). The users are made to be aware of such documents and the failures of them. The users are needed to be alerted using a flagged signal when the error occurs. These flagged signals are to be sent immediately to the users as soon as the error occurs to avoid failure of operation in GNSS. The liability is to be shared by the GNSS hierarchy. The GNSS systems earlier worked on earlier Doppler Effect but the current generations are based on triangulation techniques thus the technology of future is uncertain.

Assessment of existing legal framework

These include:

a. The liability mechanisms functions are limited unless the parties are involved in liability agreement.

b. The legal depends on local laws and not international laws; this questions the credibility and the profitability of the system.

c. The international law on the GNSS liability is deficient and inconsistent.

d. The insurance system is the only sort liability solution. This mechanism holds all parties with shared liability reparation.

e. Many proposals for related liability systems and interaction models are published.

f. The liabilities are hidden behind contractual relationships which are the contract signed by the parties. Local laws/national laws govern these contracts.

g. The liability of GNSS channeled into other sectors such as automotive, shipping community etc.

To consider the liabilities involving parties/actors to be identified in any liability scenario, the parties are brought in through two categories: Claimant and Defendant. Claimant consists of the end users or intermediate users while the Defendants are the GNSS signals/service providers. The Corpus juris spatial that is together with the 1969 Outer Space Treaty and the 1972 Liability Convention has years of understanding internationally. Considering it a tool to design further amendments is an easy solution. In this treaty, it is important to improve the liability due to indirect damages.[3]

GNSS hierarchy

The hierarchy of GNSS is required to understand the need for the policy and legislation control. In GNSS we understand the major involvements are between service providers along with infrastructure providers and end users. The end users, however, use the signal directly or with other technology platform providers in the form of complex software or embedded hardware. One of the recent time ventures in GNSS is the GALILEO systems. It developed on the view of providing navigation and positioning operated and controlled fully by civic bodies. It provides interoperability and is compatible with other GNSS systems such as (Global Positioning System) GPS and GLONASS.

GALILEO promises to deliver the first civil controlled system. It is compatible with GPS and GLONASS thus the monopoly in GNSS will slowly be of past as more efficient and accurate systems will be developed and available for market. The reason to perform this hierarchy is to validate the users involved in the entire sector of navigations. This will allow us to provide a clear pattern for the need of legal opinion beneficial for all the sectors involved. The GNSS technology is a few decade old and has limitations which need further improvements especially on the coding part. For example, error estimation such as Kalman filter, Least squares or the Filter manipulation enabled by Google maps. These are the GNSS core limitations and poses direct risks and vulnerabilities.

A long-term solution that is sought and recommended are shared liability concept. A GNSS expert panel has to be organized for encouraging the Digital platform providers to allow commercial scheme of GNSS for the market. Thus, any market product has to entail liabilities and the GNSS protection team could share liability with the commercial enterprises. This would protect the growth of GNSS commercial innovation hub from Risks due to liabilities. The risks in GNSS could be classified as a particular threat or recurring threats i.e., hardware failure or software failure. To prevent such threats, a monitoring segment is required at the end user. This causes a burden to the price of hardware in terms of power and mass. The individual must be aware of the risk and assess it in terms of continuous monitoring or relevant parameters monitoring. The GNSS providers, in any case, should be able to deploy corrective measures by suspending the service, this is to prevent danger. Based on the GNSS hierarchy it is possible to trace out the services that are provided in various sectors. This can be formulated in the Table 1 below.

Table 1 Mapping of GNSS users and the services provided

GNSS service	Quality of service
General civilian purpose	-Open service publicly available free of charge without discrimination.
	-With precision and accuracy as mentioned.
Commercial service	-To be used for most transport applications providing for system integrity information.
	-It will be certified and its performance will be guaranteed by the GNSS providers.
	-To allow control and access via encryption.
Life safety service	-It will be a value-added service offering.
	- Very high performances with a capital fee.
Public regulated	-Robust and access controlled service for governmental applications for example military.
Search/Rescue	-Increased availability of signals and tracking from the satellite.

Liability of GNSS

Failures in GNSS are due to many reasons and the liabilities could be tracked down to GNSS signal providers and GNSS solution providers. The GNSS is used by both military and civilians using the same system but are divided by selective availability. International civilian users have a fear that if the GNSS providers such as GPS, GLONASS or GALILEO drop their services or selectively block. There has been no assurance from these providers that the services would not be disrupted. There is a high probability of providing manipulative /interference processed data to the end users. The most important is no such GNSS liability treaties and the loss to the end user will not be compensated. The GNSS since it has dual use for both Military and Civilian has to follow strict defense codes such as deny use by the enemy and to be reliable.[4]

For decades GPS was dictating the GNSS market because they were the sole providers of the contents and it was open source and services. Thus the rules were accepted by the public as declared by the law pertaining to the USA. At the present times, there are various alternate providers such as Russia, Europe, and this list will extend significantly beyond the next decade. To integrate various service providers and to bring a common law and policy is going to be a very difficult and time delaying factor. The global providers have to come together to provide suggestions on the functionality, service continuation, liabilities and also budget aspects. Safety is one parameter that is non-compromisable. There are critical applications such as civil aviation and autonomous driving cars but there is a need of assurance about the quality of the signals. They wanted the signals to be provided on the basis of Non-Discriminatory. It should be compatible with others. Such signal providers and users should have known about the GNSS signals compliance (Table 2).

Table 2 Classification of liabilities based on functions

Liability	Functions
Availability	- A number of signals from various satellites.
Accuracy	- Elimination of error.
Integrity	- User data required for reliability.
Robustness	- Uncompromised signals (spoofing/jamming)
Indoor penetration	- No loss of signal strength
Continuity	- Uninterrupted signals

Most of the users are blindly obliged either forcefully or voluntarily to accept the terms and condition of the services provided resulting in a monopoly. The end users are never aware of the specification document that is provided by both GNSS signal providers or the GNSS sensors manufactures. The third party usually promotes the GNSS signals and the sensor manufacturer using services. Thus the party service providers could be easily mapped and could be held responsible. This is however done only by creating awareness. The GNSS signal providers inhibit liability to end users but also have other priorities manufacturing, launch, orbit operations and the current de-orbit or graveyard disposal of satellites. Thus the responsibilities of failure cannot be tracked since many private and government organizations are together creating such GNSS systems. The GNSS users would want to categorize the risks in 3 main levels, Injury/damage, loss of revenue and political risk (Table 3).

Table 3 GNSS enabled platforms for providers

3rd party providers	Platform exploration
Location and Navigation	Mathematical model for indicating direction
Geographical Information	Implementing co-ordinates on maps
Location-based marketing and advertising	The position of the user is collected for providing Ads relevant to nearby areas.
S.O.S	Alerts nearby people/user
Organizing Tools	To monitor and track goods, services, and resources.
Sporting Activities	Athlete's performance based on position and timings.
Virtual Reality and Augmented Reality	Positions of users are combined with education and entertainment.
Social networking	Nearby user locator.

Nowadays there are software based algorithm receivers and thus the signal, sensors, and algorithms must have standards and conformity before reaching the market. The provider of the service must promise the conformity of signals as promised at all levels.[5]

Cyber and national security

The International Telecommunication Union (ITU) clearly defines cybersecurity as anything that is involved in protecting the assets in the cyber world. In GNSS, the most common security threat that can be identified is the Jamming. Jamming is possible in GNSS due to the fact that it completely utilizes Radio Frequency as its basic function. The GNSS signals are too weak at the receiver's end thus making it a potential target using radio frequency interference.[6] There are possibilities of both unintentional and intentional frequency transmission near to GNSS frequencies causing both hazardous and fatal damages. This is due to the lack of knowledge or public education of using frequency spectrum.[7]

It is foreseen for a vast growth in the application of an Autonomous Self-Driving Vehicle (ASDV) and drones. These must have the necessary capabilities for monitoring its navigation environment without human intervention. This is essential to identify the signals required for identifying navigations paths appropriate for avoiding obstacles. The GNSS signal coverage is quite weak at the user end. These weak signals can be compromised by interferences by nearby RF signal with frequencies of the same order or nearby frequency spectrum. There is a huge potential risk when such systems are being used for ASDV and drones especially employed in collision avoidance system. The common method now being deployed during the compromised stage is the use of secondary mode. Thus, insurance agencies, the liabilities or policy regulators should be certain that the providers of service would take such protections during the attacked/compromised phase.

The common ways of compromising the signal security of GNSS are performed with spoofing. Spoofing is a method of gaining unauthorized access by compromising the encryption using replication of GNSS signals. The devices to spoof are off the shelves components and easy to find or built with low cost. This sudden development has to be a greater concern and governments or Industries should fund Anti-attack GNSS systems hardware and software. The future is predicted to have many advanced technologies such as Unmanned Cargo Ships, Unmanned Submarines, and Civilian Aircrafts. These technologies and applications enable GNSS as their source of navigation hence funding in Anti-attack GNSS systems is very crucial and this would open up a huge market. The alternate and compromisable solution is to have interoperability by deploying GNSS mega-constellations. This would allow minimizing error and eliminating the compromised signal. The damage caused by GNSS should be contained because this would have a bad reputation by the public and acceptance of

its technology would start to break apart. The market capabilities of GNSS system would depend on the reliability, security and non-compromisable standards of signals. Results should be clear and concise.

Remote sensing technology

Data Analyst Society has evolved in such a way that could create privacy invasion by using physical world non-digital value and converting them to digital format. They are investing heavily in data minimization which is creating alternate ways of using the minimum information to collect data that may or may not lead to privacy invasion. That requires legal verification of privacy protection. The Data Analyst society even if it educates the public about its intention of using the privacy data, there could still be gathering of information that was created unexpectedly. This unexpected information could be misused for creating beneficial services as well as products both anticipated and unanticipated.[3]

There has been recently a lot of social injustice with the break out of the Data Analyst Society. Now, almost everyone is familiar with public outcry and outbreak of how technology is used to violate privacy. The invasion of privacy using remote sensing technology is a big problem that requires a lot of attention from lawmakers and regulators. A drone aided with a video camera and mobile app collecting user's location-based information are some of the examples how Data Analyst could invade privacy. There are lots of debates among lawmakers to understand if there is no protection from privacy of anything in the public. The major strike on privacy invasion is the DATA Fusion. This is a process of using technology to collect, capture and to process the data about personal information. The processed data can be used for obtaining and revealing the personal information for exchange of monetary or other benefits.[8]

The data bank that collects Geo-information should be legally pressurized on how they collect, store and process the information that they gather from the public. This information is needed to provide a default regulatory terms and condition. The monitoring body would thus provide the agreement, terms, and condition for the user rather than a monopoly. These reduce the obligation of blind click and accept the conditions laid by the provider. The data gathered and their usage will be provided as a knowledge support not only to see how they are collected but how they will be visualized. The process of collecting data, how they will be processed, and what information is extracted from them have to be very simple and need to be exposed to the public.[9]

Privacy sovereignty

Placing a device and monitoring the movements of an individual is an invasion of privacy. GNSS platform providers are entangled in legal issues due to privacy infringements from relocation technologies. Any user has his own rights to protect his privacy about the data and information surrounding his life and living habitats. There are many laws supporting that a person's private information are of confidence and that they are secured. The GNSS users have fundamental rights to be protected but unfortunately, all the digital contracts are created by the service providers thus obliging the users blindly consent to their use. This is exploiting by dictating terms and conditions to use their product or services. Privacy is related to culture and tradition, therefore, is different from one country to the other.

To determine if the privacy of the user has been violated is very complex because the user has a possibility to be aware of such situation and voluntarily accepted the terms and conditions. The geolocation service providers thus argue that the user has expected such privacy invasion due to the use of their products. This is also supported by the usual phrase that in public nothing is deemed private or invasion of privacy.[2] The biggest concern is with the use of open source programs. These programs come for free and they openly disclose they are not liable for any damages. The insurance has been helped a lot with GNSS data solution systems but there are no Insurance regulations for GNSS when data are corrupted or manipulated providing wrong information to the user. Hence a regulation has to be sorted.[10]

Risk management, mitigation and policy recommendations all small caps

One of the recommendations for GNSS service providers is to follow an obligation with the insurance company for making a contractual relationship to share liability for any compensation for damages due to an uncontrollable situation. The major GNSS providers such as GPS, GLONASS and GALILEO have committed themselves towards international navigation system that would provide and ensure interoperability services for international users. The GNSS system will require additional radio frequencies for civilian purposes that have to be coordinated with ITU. As the satellite and frequencies increases for the user benefits selective availability can be terminated.

A private GNSS provider will be able to provide service with high quality through more precise positioning for a small fee and could take up the liability for such services. They will also be able to notify the users on all levels if there is any interference and could quickly provide software upgrades. One of the main and important needs for commercial GNSS system is the ability to provide services without any non-discrimination and the reliability for such services. There would be a listed solution for liability agreement; this agreement is the prior arrangement to minimize system malfunctions efficiently.

However, the biggest risk for private GNSS providers is the data fusion that is associated with the geospatial community. This is quite alarming as the data of location plays a huge role in privacy invasion. Thus the regulators such as lawmakers and policy makers should step in before the breakout of private GNSS sector. The more constellations of GNSS are in space, the more high-frequency waves are being sent to the earth and the more the adverse effects on the living organisms on the earth. The long-term effects of high powered radio frequency waves have a negative impact on the lives of living organisms. Thus it is the duty of the regulators to safeguard nature and its survival. This opens up a new liability clause where the medical bills rise upon the use of high radio frequency waves that are being beamed on to the surface of the earth resulting in brain damage or other organ malfunction. It is a long vision and quickly needs to be studied upon.

The GNSS signal providers may need to provide Cooperation and Mutual Assistance for the safety of public use. There should be one point of International Treaty for regulation.[11] The Growth of private GNSS system providers will allow commercialization of GNSS systems for worldwide private players. These paid-up operations of GNSS will solve the liabilities as the private players. The development of technology that can be used properly or misused always is ahead of time. It is really important for the lawmakers to catch up with them. The technology doesn't come under laws, legal framework during the prototype stage but it should have a proper legal framework before

they are commercialized. The GNSS data provides vast information when implemented with remote sensing and imaging technology. They are part of day to day life of people as they are used extensively. Any new technology should not violate the promised conformity to the services provided in the supporting documents.

Conclusion

The GNSS signal providers may need to provide Cooperation and Mutual Assistance for the safety of public use. There should be one point of International Treaty for regulation. The Growth of private GNSS system providers will allow commercialization of GNSS systems for worldwide private players. This paid up operations of GNSS will solve the liabilities as the private players.

Acknowledgments

None.

Conflicts of interest

Authors declare that there is no conflict of interest.

References

1. Fernandez-Hernandez I, Vecchione G, Diaz-Pulido F, et al. *Galileo high accuracy: A program and policy perspective*. Proceedings of 69th International Astronautical Congress (IAC); 2018.
2. Pomfret K. *Implications of Evolving Expectations in the United States*. GNSS & the Law: Geolocation Privacy. Inside GNSS; 2016.
3. Report to the President. *Big Data and Privacy: A Technological Perspective*. President's Council of Advisors on Science and Technology; 2014. 76 p.
4. Larsen PB. Issues relating to civilian and military dual uses of GNSS. *Space Policy*. 2001;17(2):111–119.
5. AI Franken. *Sen. Franken Presses Makers of 'Pokemon GO' Smartphone App Over Privacy Concerns*; 2016.
6. Pullen S. *GNSS Jamming In The Name of Privacy (Potential Threat to GPS Aviation)*. USA: Stanford University; 2012. 10 p.
7. Moskoff DB. *GPS Jammers a Top Concern in Maritime Cyber Readiness*. Professional Mariner Magazine; 2014.
8. Lewis JJ, Caplan LR. *Drones to Satellites: Should Commercial Aerial Data Collection Regulations Differ by Altitude?* USA: Holland & Hart; 2015. 5 p.
9. Rees C. *How the IBA Is Facilitating the Development of 'Information Law*. International Bar Association; 2013.
10. Bollweg HG. *Initial Considerations regarding the Feasibility of an International UNIDROIT Instrument to Cover Liability for Damage Caused by Malfunctions in Global (Navigation) Satellite Systems*. Rome, Italy: International Institute for the Unification of Private Law (UNIDROIT); 2008. 21 p.
11. Lisi M. *GNSS Jamming Detection, Localization and Mitigation*. Warsaw: Navigation, Surveillance and Signal Intelligence Conference; 2015.