

Formed in 1982, MAPPS (www.mapps.org) is the only national association exclusively comprised of private firms in the remote sensing, spatial data and geographic information systems field in the United States. The MAPPS membership spans the entire spectrum of the geospatial community, including Member Firms engaged in satellite and airborne remote sensing, surveying, photogrammetry, aerial photography, LIDAR, hydrography, bathymetry, charting, aerial and satellite image processing, GPS, and GIS data collection and conversion services. MAPPS also includes Associate Member Firms, which are companies that provide hardware, software, products and services to the geospatial profession in the United States and other firms from around the world. Independent Consultant Members are sole proprietors engaged in consulting in or to the geospatial profession, or provides a consulting service of interest to the geospatial profession.

Unmanned aircraft systems, or UAS (derisively called “drones”) have already become important new technologies in America that will have important and sizable impact on the American life and economy. The economic importance of this technology has been widely discussed and will, in our view, become even more important than most current estimates suggest.

The geospatial field is a \$73 billion market that drives more than \$1 trillion in economic activity. It is estimated that more than 500,000 American jobs are related to the collection, storage and dissemination of geospatial data, and another 5.3 million workers utilize such data. As much as 90 percent of government information has a geospatial information component and up to 80 percent of the information managed by business is connected to a specific location.

Geospatial technology has been identified by the Department of Labor as one of just fourteen high growth sectors of the United States workforce projected to add substantial numbers of new jobs to the economy or affect the growth of other industries or where there are existing or emerging businesses being transformed by technology and innovation requiring new skills sets for workers to prepare to take advantage of new and increasing job opportunities in high-growth, high-demand, and economically vital sectors of the American economy.

MAPPS wishes to discuss how our members operate, the benefits of aerial survey operations utilizing UAS technology, and the ramifications of how the application of small UAS (sUAS: under 55 lbs) in the national airspace will affect the “privacy” of our fellow U.S. citizens.

Issues of personal autonomy and anonymity are important considerations for UAS. Additional privacy interests include issues of aggregation, use, and retention of UAS-obtained information, especially when this information is distinctly “personal” in character and can be used to identify individuals.

Popular U.S. sentiment about what a “drone” is used for is mainly characterized by the first two: killing and spying. Neither is applicable to the aerial surveying, mapping or geospatial profession. Most people will not first think of UAS as used for surveying and mapping. However, society as a whole and citizens as individuals benefit every day from the application of geospatial data collected by ground, airborne and space-borne methods.

In simple terms, geospatial information is geography -- surveying and mapping. It is “place based” or “locational” information. It is data tied to points on the ground and portrayed on a map.

Today, a map is no longer something you fold up and put in the glove compartment of your car. It is the use of a global positioning system (GPS) and geographic information system (GIS) that accurately collects, stores, retrieves and displays vast amounts of information in a spatial context. Whether it is MapQuest, Bing Maps, Google Maps, or the in-dash navigation system in your car, everyday Americans use geospatial data more than they know it.

Consider the following:

It's 7:00 a.m. You are awakened by your clock radio and you get up and turn on the lights.

The radio and lights are powered by electricity. The electric company has used geospatial information to route transmission and distribution lines, locate or deliver the fuel (oil, gas, coal, hydro, geothermal, wind, solar), and manage its infrastructure (utility poles, underground conduits and local lines) to get power to your house.

Once in the kitchen you pour yourself some fresh orange juice.

Aerial photography was used to monitor crops. Water for irrigation to grow the trees depended on geospatial data to get from the reservoir aquifer to the farm. Farmers used "precision agriculture" – GIS and GPS – to plant, plow, and fertilize their crops, as well as to safely and effectively apply pesticides.

You shower, shave and brush your teeth.

Water is supplied to your home through a water distribution system that consists of thousands of miles of water mains. The utility uses geospatial data to plan routes, lay water lines, and monitor water flow. Local contractors use "One Call" or "Miss Utility" systems to make sure they don't hit an underground water or electric line when excavating. Once used, water goes down the drain, a wastewater collection system consisting of hundreds of miles of sanitary sewers and storm drains that was designed and built using geospatial data takes the wastewater to a treatment plant.

You see your kids off to the bus stop to go to school.

The local school board has used geospatial information to draw school boundaries. A bus efficiently picks up the children in your neighborhood based on a routing system built from a geographic information system (GIS), combining demographic data, street data, and data about location of both the students' homes and the school.

You drive to work.

Engineers have used surveys, mapping and geospatial information for planning, corridor analysis, environmental impact studies, design, construction, operation, and maintenance of the roads you travel by car or bus, or for the subway you've ridden. Your in-dash navigation system may have helped identify an accident or traffic jam and suggested an alternate route.

You make a phone call or send an email.

Land line or cellular telephones and broadband internet are dependent on geospatial data. Your telecom service provider uses this data to lay lines and fiber optic cables, site cell towers, and manage their infrastructure.

You feel ill and can't get to a doctor or the hospital on your own.

You dial 911. The operator uses the latest geospatial technology to identify the location from which you made your call. An ambulance uses GIS to get from the EMS station to you via the quickest possible route, and then gets you to the nearest hospital through an automated mapping system. After you've been diagnosed and treated, a health care professional enters information about your illness into a GIS, plots where you were stricken and finds there have been several others affected by similar symptoms in recent weeks. An epidemiology analysis, using geospatial data, is begun to find the cause and begin remediation.

Back at work, you begin serving customers, clients or constituents.

At your desktop, you are targeting a specific neighborhood for your product, or if you work in a political office, you are micro-targeting a mail campaign or town hall meeting. A government employee uses GIS to assure that services are being delivered to the constituents who are in need. GIS lets you identify key customers, clients or constituents and research data you have on their preferences and interests.

The day is done. You've done a lot. And geospatial information helped you through the day more than you realized. Geography affects your life nearly every step of the way, helping you to be safer and more productive.

Without maps, you're lost! Each of these is a peaceful, beneficial and common application of geospatial data. Some data was collected by a high resolution commercial remote sensing satellite (licensed to operate by the Department of Commerce), other data acquired by aerial photography (which the U.S. Supreme Court ruled is **not** an unlawful or unwarranted search under Fourth Amendment of the Constitution. (See: Dow Chemical Company, v. United States, 476 U.S. 227 (1986)), and other data by traditional ground or terrestrial surveying and mapping methods, much of which is under the responsible charge of a state licensed professional surveyor. The use of a UAS for such data collection only changes the platform. The collection technologies and applications of the data remain the same – and safe.

Indeed, the following are examples of beneficial applications of surveying, mapping and geospatial data, regardless of the method of data acquisition:

- geospatial data is essential to E911 emergency response and dispatching of police personnel, fire trucks, emergency medical technicians, and ambulances;
- geospatial data is utilized in precision agriculture to assist farmers with maximizing crop yields, minimizing non-source point pollution into America's lakes, streams, and rivers;
- geospatial data is the underpinning for topographic mapping used in hunting, fishing, hiking, skiing and other recreational activities;
- geospatial data is used for management of storm-water runoff and mapping of impervious surfaces, flood plain mapping, and equitable assessment of local property taxes levied and collected by municipalities;

- geospatial data is used in a variety of applications by all levels of government on a daily basis, such as mapping to provide for zoning and comprehensive planning; efficient routing of trash collection trucks; safe, energy-efficient, and time-saving routing of school buses;
- the timely acquisition of geospatial data is critical to assessment, realtime decision making, and mitigation during and immediately following both natural and anthropogenic disasters, including earthquakes, tornados, blizzards, floods, volcanic eruptions, wildfires hurricanes, infrastructure disasters including collapsed buildings, bridges and dams, ruptured pipelines, various types of terrorist incidents and in emergency “blue tarp” surveys to support post-disaster response;
- geospatial data is the foundation to engineering design and construction of wide range of infrastructure improvements, including roads, water, electric, fiber-optic and other utilities;
- geospatial data is routinely integrated into GPS and navigation systems, on-board vehicles and handheld devices that are so popular among consumers today;
- geospatial data is essential to the Census and to establishment of electoral districts for municipal, state legislative, or Congressional representation;
- Congress and government agencies are increasingly reliant upon geospatial imagery and data for the management of natural resources, economic development, the management, adjudication, and prevention of future disruptions in the home mortgage system, the development and implementation of a smart energy grid, the deployment of universal domestic broadband service, the management of Federal real property assets, emergency preparedness and response, homeland security, the delivery of efficient health care and other services provided, financed, or regulated by the Federal Government, measuring, monitoring, verifying and validating the effects of climatic and environmental phenomena, and the maintenance, rehabilitation, and enhancement of public works, transportation, and other infrastructure of the United States;
- geospatial data is derived from images and data collected from a variety of airborne and spaceborne platforms, as well as other mobile and terrestrial-based acquisition systems; and
- geospatial imagery and data is regularly and historically collected, utilized and applied by companies engaged in the free market commerce of the United States and by government authorities operating within the safeguards, rights and framework established by the Fourth and Fourteenth amendments to the Constitution of the United States.

Therefore, the regulation of geo-location data, or its collection from a UAS, would have severe, negative and unintended consequences for the government, business and individual U.S. citizens. Geospatial imagery and data collection, usage and application is a valued part of the modern American economy broadly applied to improve the analyses and decisions necessary to sustain and enhance the quality of life, and is not synonymous with “precise geolocation data” as such term is used by the Federal Trade Commission and in some regulatory and legislative proposals. The geospatial community functions in a manner that does not threaten the privacy of individual citizens, and in fact contributes to the quality of life of all Americans.

The real threat to surveying, mapping, and geospatial practitioners is that this common notion that “drones” are chiefly used by the government to spy on citizens and to kill our enemies will impact

regulations and cause unnecessary, unwise, and unfair burdens on the many commercial and legitimate applications of UAS in the national airspace to map and survey our lands, our infrastructure, and resources.

MAPPS strongly contends that regulations limiting the “technology” of UAS should be discouraged. Instead, regulations, when needed to protect the privacy of citizens, should be designed to regulate the “application” of this technology (or any other similar technologies like miniature cameras and recording devices, wire taps, etc.). For example, “Peeping Tom” laws already exist that prohibit the activity of spying on people regardless of what technology is used to “peep”. One could climb a ladder and peer in a person’s bedroom window, or put a USB-camera on a long pole. Walking down Main Street in any town in America, a citizen is “surveilled” far more than they ever will be by a UAS. These nefarious applications of technologies are regulated NOT the technologies themselves.

MAPPS supports the general approach of little or very limited government regulation affecting commercial UAS operations. Because this technology is new and for all practical purposes have not been used commercially within America, MAPPS encourages the courts (not government agencies) to formulate rules more cautiously over time based on concrete facts in an adversarial setting. This method of rule-making fosters less risk of creating unnecessary, counter-productive, and economically burdensome rules with unintended consequences. However, it is warranted to establish baseline regulations now that erect firewalls that safeguard privacy from the government application of this technology (as discussed below).

Operators of UAS fall into three general categories:

- a. Public (government)
- b. Commercial
- c. Recreation

Regulations should wisely reflect the different impacts and risks these different types of operations have on privacy.

MAPPS supports regulations of UAS that are necessary to protect the privacy of individuals. However, it does not support any federal entity to establish these regulations of the following types:

- a. Regulations or restrictions that target UAS technology specifically. Instead they should define the application of a technology, that is, “spying” or “harassment” is outlawed not “the flying of UAS”.
- b. Regulations should not be made by the NTIA or other government entities until after there are legitimate cases that call for it. UAS technology is new and evolving. Privacy issues are not yet known, nor is public attitude about UAS based on experience or fact. UAS regulation on privacy at this time would be premature and likely will do more harm than good.

Public (Government) Use of UAS

As UAS become more common it is likely every government agency (federal, state, or otherwise) will find an important use for them. It is the government use of UAS, not the private sector, that could have the most direct and harmful impact on privacy. The Fourth Amendment’s protection against

unreasonable searches is of foundational importance to American citizens and is threatened considerably by the misapplication of UAS technology (or any other common technologies that enables the surveillance of American citizens). For these reasons, robust protections of privacy need to be in place for those government applications of UAS to safeguard citizen privacy.

When UAS (or any technology) are used to obtain information about individuals such that personal identities can be discerned, the government should be required to obtain a warrant and follow written data use and retention policies. However, consistent with previous law and court cases, warrants should not be required when the person has no reasonable expectation of privacy regardless of what technology (UAS or other) is used. For example, the courts have established a reasonable precedent that citizens forfeit their rights to privacy or “anonymity” (in some cases) when in public spaces. The government and private applications of UAS should be allowed in public spaces consistent with these precedents especially when anonymity is not easily negated.

Agencies that collect information using UAS should ensure their policies and procedures adhere to the FTC’s Fair Information Practice Principles. Further, they should define how information is collected and used, retained, and disseminated when the information can be used to identify individuals and compromise personal privacy. However, for applications like remote sensing, mapping, and surveying (applications that inherently do not collect information that can be used to identify individuals, and particularly not in real time) but that simply measure the earth and features on or under the earth, or are merged with readily and publicly available information (e.g. parcel, address or other information from public records) no additional policies and procedures should be required other than those already in place today to guide the collection of aerial photography and other forms of remote sensing.

Commercial Use of UAS

UAS will be used for a plethora of important commercial, societal and humanitarian purposes. Any regulations limiting or burdening these applications should be minimal. When regulations are necessary they should not restrict the UAS technology itself.

Consistent with government use of UAS in public spaces (where individuals have no reasonable expectation of privacy), requiring UAS operators to obtain consent to be photographed before conducting aerial surveillance, mapping or surveying is entirely unwise, unwarranted, counterproductive (unless individuals can be identified using the information), and unreasonable to the point where compliance is impossible. Current commercial mapping and surveying camera technology is not capable of resolutions sufficient to enable facial recognition of individuals. The identities of individuals are protected. Aerial photography of the earth and people on the earth has been performed routinely by firms throughout America since the early 20th century. There have been no legitimate concerns about loss of privacy because of such surveying, mapping, geospatial and remote sensing data collection or application.

Citizens are not informed that their homes and persons are being photographed today by satellite or aerial photography. In many states, surveyors are provided “right of entry” onto private property by statute. UAS represent a new aerial platform on which to do this same type of remote sensing for mapping and surveying applications. MAPPS does not support the regulation of these activities nor a requirement that the consent of those being photographed be acquired if their identity cannot be discerned.

However, technology does not stand still. Eventually, commercial airborne sensors on UAS will enable the facial recognition of individuals. Applications of UAS of this nature should require that personal information about individuals be altered or redacted (by blurring or other digital obfuscation techniques to protect anonymity).

Concerns of “personal autonomy” (the ability of an individual to make life decisions free from interference or control by both government and private actors) are legitimate. MAPPS supports the position that any application of persistent aerial surveillance that poses risks to personal autonomy (through “aggregation” or loss of “anonymity”) should be regulated so privacy is protected from government and private actors. Today, citizens are continuously photographed while walking in public spaces by surveillance cameras located in such public and private spaces. Much of an individual’s activities through town could be assembled (“aggregated”) if an individual or agency could collect all the surveillance information from all the disparate private and government cameras. Precisely because a person’s activities are distributed across a large number of separate sensors, many controlled by non-government parties, that person’s privacy is protected. It is simply too hard and expensive to aggregate the disparate information concerning an individual. However, when a single camera controlled by a single actor (government or civil) can be positioned (possibly unseen) overhead for long periods of time surveilling all the activities of all the individuals in the public space over time, the ability to assemble (i.e., aggregate) a picture of an individual’s (or everyone’s) activities becomes far easier and much less expensive. This application of UAS should be regulated to balance the individual’s right to view (for commercial or recreational purposes) with the UAS operators right to observe people in public spaces that under other conditions have no expectation of privacy. Aerial mapping and surveying are not applications that threaten personal autonomy and are not typically used to aggregate information about individuals. These activities are not persistent and occur only at discreet moments in time for purposes of recording the position, shape or size of features on, above, or under the earth’s surface. MAPPS does not support regulations of these activities for these reasons.

Recreational Use of UAS

Consistent with the standards of privacy when individuals are in public spaces, recreationists should be allowed to view individuals with UAS when those individuals are in public spaces and they have no reasonable expectation of privacy. No consent should be required. Of course, there is a point at which this “viewing in public” becomes harassment or poses a threat to safety. What constitutes harassment or a “threat to safety” should be defined (by the courts over time), but, consistent with the discussion above, regulations that limit UAS technology specifically are unwelcome. Instead, regulations should be drafted that restrict the application of any technology that constitutes harassment, violates a reasonable expectation of privacy, or threatens the safety of the public.

There are some reasonable exceptions to this general forfeiture of privacy that may or may not have been established in precedent. For example, “persistent” staring from a public space becomes possible with sUAS and microUAS. For example, an individual could stand in a public easement behind a neighbor’s residence and watch the neighbor’s activities in his yard or through their open windows. The neighbor may not like this activity, but that individual has a right to stand in a public space and observe activities that have no reasonable expectation of privacy, except as limited by “Peeping Tom” and other similar laws. However, if that individual can position a microUAS in the national airspace (a public space) over the public easement and persistently stare for days into the neighbor’s yard and open windows

recording every activity, it is reasonable to expect this application of technology is an invasion of privacy and constitutes harassment. Regulations to govern this type of UAS application are reasonable. It should be noted this is not how the surveying, mapping and geospatial profession operates.

Post-Collection Activities

Another type of privacy risk posed by some applications of UAS (and other commonly used technologies) is how collected information is aggregated, used and retained by the operator. In some instances, the initial collection may not directly implicate an individual's privacy interests, but the subsequent manipulation and storage of that data may risk loss of privacy. UAS regulations that govern post-collection activities with information collected by UAS, should not be required for any application of UAS when the identity of individuals is not possible or when they are protected through some means of digital obfuscation.

How information obtained with a given technology is used and retained can also pose a risk to privacy. In the era of big data, information collected for one purpose could be used for other purposes by individuals or entities not involved in its collection. If UAS information can be used in such manner and put an individual's privacy at risk, it should be prohibited unless consent or a warrant is obtained. However, if the information collected is inherently "non-personal" and the identity of individuals cannot be discerned than there is no reasonable expectation that the information could be used later for nefarious purposes. As stated above, information that is or could be obtained from public sources, (e.g. an address or parcel identification from a government agency) such information should not be treated as personal. Therefore, there is no valid reason to require the person or entity acquiring the information to make any assurance that it can't be used for other purposes by others sometime in the future.

The Federal Trade Commission (FTC), in its March 2012 report, "[Protecting Consumer Privacy in an Era of Rapid Change](#)" said:

"With respect to use of geolocation data for mapping, surveying or similar purposes, if the data cannot reasonably be linked to a specific consumer, computer, or device, a company collecting or using the data would not need to provide a consumer choice mechanism. Similarly, if a company takes reasonable measures to de-identify smart grid data and takes the other steps outlined above, the company would not be obligated to obtain consent before collecting or using the data."

Summary

UAS represents a new and developing technology. The courts and UAS community should be granted time to formulate rules and best practices to promote safety and privacy. MAPPs supports the general approach of little to no regulation now in the commercial and private sectors as this technology is being created, innovated, and deployed within America. Given this time guided by real application allows a more cautious and thorough discussion based on concrete facts in an adversarial setting. This method of rule-making runs less risk of creating unnecessary, counter-productive, and economically burdensome rules with unintended consequences.

Because of common misconceptions of “drones” as killing, spying machines, MAPPS favors protection *from* regulation of commercial mapping and surveying applications with UAS especially when the identity of individuals in that information is not possible. Just as importantly, MAPPS supports establishing regulations that restrict the government use of UAS by erecting constitutional firewalls that safeguard the privacy of individuals from the government.

In the aforementioned report, the FTC went on to note “the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the final privacy framework, to the extent they have not already done so.” Attached is a draft “best practices” guidance document currently under consideration by MAPPS, as recommended by the FTC. We believe the responsible collection and use of data, as outlined in these comments and the attached guideline, sufficiently protect individual privacy and minimize the need for government regulation.

John M. Palatiello
MAPPS Executive Director
1856 Old Reston Avenue, Suite 205
Reston, VA 20190
(703) 787-6996
www.mapps.org
john@mapps.org

MAPPS Best Practices on Privacy of Geospatial Data

MAPPS, Management Association for Private Photogrammetric Surveyors (MAPPS) is the only national association of private sector firms representing the broad base of surveying, spatial data and geographic information systems professionals in the United States. MAPPS member firms are engaged in surveying, photogrammetry, satellite and airborne remote sensing, aerial photography, hydrography, aerial and satellite image processing, GPS and GIS data collection and conversion services. MAPPS Associate Members include firms that provide products and services to our member firms, as well as others on world-wide scale.

MAPPS member firms conduct their business in accordance with high ethical, moral and legal standards, efficiently, in good faith and in the best interests of their respective companies, their employees, shareholders and other related stakeholders. Our member firms maintain business practice standards that earn the respect of everyone with whom the companies conduct business. MAPPS member firms are a part of the geospatial profession that provide geospatial products and services to a broad range of markets.

There is no longer any dispute that Geospatial information plays an important role in our society. Anyone following the debates over the appropriate use of UAS' or development of the "driverless" automobile understands the breadth and depth of the data production involvement of our membership. Almost all human activities and decisions have an inherent geospatial component; and, the value of personal information increases when it is connected to a location. Geospatial mapping links to consumer financial data, healthcare data, and other consumer behavioral data are just a few examples that have been utilized with great success in recent years. Predictive analytics is clearly a burgeoning success story as it relates to the data our members are regularly producing, analyzing and delivering to our clients. With the rapid technological development and wide uptake of smart mobile devices a whole new category of location based services is approaching a new level of maturity.

The phrase "precise geolocation information" is becoming a part of many legislative actions. The word "precise" may be misleading and if left undefined **WILL** directly wreak havoc in the geospatial community, and indirectly deny Nation's citizens of the best available processes and mapping data. Put simply, there has been no clear definition of the "precise" terminology and language; a vague definition of such a term is ambiguous at best and potentially dangerous at worst. Most importantly, a clear and concise definition will protect the public's well-being and safety by enabling citizens and consumers access to data, devices, and location based services such as E-911, electronic lost and found, and navigation. The "precise geolocation information" terminology must be defined with the actual goals of the legislation in mind; otherwise, the law of unintended consequences and not result in unintended consequences that will cause damage to include thwarting legitimate and desired business concerns, decrease the effectiveness of public safety and create a denial culture as it relates to market-driven

consumer demand. The products, technologies, and services they are demanding are clearly growing and expanding in the marketplace. Ostensibly, the stated purpose of most of the legislation is to protect personal and private information of individuals that have not given consent to collect such information. This MAPPS guidance will help define the best practices for protecting personal privacy when collecting geospatial data.

There should be a distinction between the term “precise geospatial information” and “**precise personal geospatial information**”.

MAPPS recognizes and agrees that everyone has the right to protect their personal data. **Precise Personal Geospatial Information** should only be gathered legally under strict conditions, for a legitimate purpose and as transparently as possible. Furthermore, persons or organizations which collect and manage personal information should protect it from misuse and while respecting rights of the data owners.

Individuals regularly disclose personal information such as their names, photographs, telephone numbers, birth date, and address while engaged in a whole range of everyday activities. This personal data may be collected and processed for a wide variety of legitimate purposes such as business transactions, joining clubs, applying for a job, and so on. Also, when purchasing devices with GPS technology such as smart phones individuals have typically agreed to share their location while using that device. Sharing your location can provide an enormous amount of personal information about your habits and behavior.

So an appropriate question might be to ask when a company should obtain individual consent when collecting geospatial data?

Any information about the location and shape of, and the relationships among, geographic features, including remotely sensed and map data.	No
Any graphical or digital data depicting natural or manmade physical features, phenomena, or boundaries of the earth and any information related thereto, including surveys, maps, charts, remote sensing data, and images.	No
Collection, storage, retrieval, or dissemination of graphical or digital data to depict natural or manmade physical features, phenomena, or boundaries of the earth and any information related to such data, including any such data that comprises a survey, map, chart, geographic information system, remotely sensed image or data, or an aerial photograph by surveyors, photogrammetrists, hydrographers, geodesists, cartographers, or other such mapping and geospatial professionals.	No
Data originating from commercial satellite systems licensed to operate by the U.S. government, global positioning systems, geographic information systems, and airborne or terrestrial mapping equipment.	No
Collection, storage, retrieval or aggregation of information about an individual that is publically available such as legal information found in deeds, property records, and property maps	No
Personal information about an individual's real time geospatial location	Yes
Personal information that is protected under law such as health and employment information.	Yes

John M. Palatiello
MAPPS Executive Director
1856 Old Reston Avenue, Suite 205
Reston, VA 20190
(703) 787-6996
www.mapps.org