



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
62/098,968	12/31/2014		130	PA6875PRV		

CONFIRMATION NO. 2173

22830
CARR & FERRELL LLP
120 CONSTITUTION DRIVE
MENLO PARK, CA 94025

FILING RECEIPT



Date Mailed: 01/12/2015

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Benjamin Daniel Marcus, Santa Monica, CA;

Applicant(s)

Benjamin Daniel Marcus, Santa Monica, CA;

Power of Attorney:

Brian Hennessey--51271

If Required, Foreign Filing License Granted: 01/12/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 62/098,968**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

System and Method For Personal Airspace Exclusion Zones

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international

application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national

security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

SYSTEM AND METHOD FOR PERSONAL AIRSPACE EXCLUSION ZONES

Inventor

Benjamin Daniel Marcus

Summary

Various exemplary embodiments of the present technology provide systems and methods for establishing no-fly zones (also referred to herein as personal airspace exclusion zones and no-fly areas) for drones. Individuals or organizations interested in preventing, limiting or monitoring access by drones to airspace above their private property may input information into a database of no-fly zones. Drone manufacturers may program drones during the manufacturing process, or establish an updating protocol during operation, charging or at any other appropriate time. During programming or updating, the drone receives information related to no-fly zones, and thereafter is programmed to avoid flying into, and/or photographing, no-fly zones.

Background

[0001] Drones are increasing popular, but are currently lightly regulated or unregulated in the private sphere, and prohibited in the commercial sphere. Additionally, enforcement of any regulations is difficult and inconsistent. Commercial drone operation is currently prohibited, but will likely soon become common place, for example for deliveries. People are concerned about drones for safety reasons (i.e., concerns about being struck by a drone) and for privacy reasons, since drones often have cameras. The Federal Aviation Agency (FAA) regulates air travel in the United States, and generally allows travel through airspace above 500 feet. Drones are

typically height limited to 400 feet, and therefore pass through private airspace if traveling above private property.

Brief Description of the Drawings and Appendix

[0002] FIG. 1 is a diagram illustrating a no-fly zone tied to property lines according to an example embodiment.

[0003] FIG. 2 illustrates an example computer system that can be used to implement embodiments of the disclosed technology.

[0004] Appendix A includes additional description of exemplary embodiments of the present technology.

Detailed Description

[0005] The technology disclosed herein provides a system and method for controlling drones and preventing them from trespassing, violating property rights, or otherwise accessing prohibited areas. In this manner, drone operators and manufacturers may limit their liability. Likewise, property owners or other responsible parties (hereinafter referred to as users) may prevent, control or monitor access to a private area and/or a controlled area. Users input address or location information into a database, for example an online form or internet webpage. The users may be required to verify ownership or control of the property. The system may use the address to determine a location, for example latitude and longitude coordinates, or alternatively by any other appropriate location designation.

[0006] The system may use the location to create a no-fly area, which may be a circle or square, or other shape positioned around the location. The size of the circle or other shape may be a function of the density of the area, or may be predefined, or may be selectable by the user or a database operator (also referred to herein as a controller).

Alternatively, the system may access property records based on the address and identify the exact shape of the property being identified. Then the property shape, with or without a buffer zone of a predefined or selectable amount, may be determined. The property, or the circle or other shape, may then identify a no-fly area. The no-fly area may be added to a database of no-fly areas to form a comprehensive no-fly zone database. The no-fly zone database may also include information related to prohibited flying areas, for example airports, military facilities, schools, nuclear plants, etc.

[0007] The no-fly zone database may be accessed by a drone manufacturer or operator, and may be downloaded to a drone. A communication protocol, and/or data format may be utilized which may be specific to types of drones, or alternatively may be standardized. Drones may be programmed to respect the areas identified in the no-fly zone database and not to fly into them. Additionally, drones may be programmed to not direct any onboard cameras into a no-fly zone. The disabling of a camera may therefore be dependent on both a position and an orientation of a drone. The position and orientation of the drone may be determined based on an initial position, acceleration, velocity information, GPS, compass bearing, and/or from any other appropriate position and orientation information source.

[0008] The no-fly zone database may be delivered to a drone manufacturer periodically to include updates. Alternatively, a Wifi-enabled or other internet-connected drone may update the no-fly zone database or file during operation and/or charging. The present technology may thereby aggregate the privacy preferences and/or access rights published and/or requested by many individuals and/or entities, and disburse those preferences and/or rights to many nodes, for example drones.

[0009] The completeness of the no-fly zone database, including FAA determined no-fly areas as well as user input no-fly areas, is a selling point for manufacturers. Use of the no-fly zone database limits the liability of the drone manufacturer by limiting or eliminating the damage possibly caused by the drones produced. The categories of no-

fly zones may be selectable by a manufacturer. In this manner, a drone produced for the military may not include the no-fly zones of military facilities, and/or may be modified in any appropriate way by the database operator, the drone manufacturer and/or drone operator.

[0010] In further exemplary embodiments, certain types of passage by a drone over private property may be permitted by a user designating the area a no-fly area. For example, a user may allow drones delivering packages to land and takeoff from the property when delivering packages there. Additionally or alternatively, a user may allow drones to pass over the designated no-fly area if the drone operator agrees to pay a fee for passage. Further description of the present technology may be found in Appendix A.

[0011] FIG. 1 is a diagram of a no-fly zone. The no-fly zone may be designated by a user or other responsible person by reference to an address. The exemplary system may access a property database to determine property lines. The system may additionally add a buffer zone of a predetermined or user selectable distance from the property line, and may include the property area plus the buffer zone in a no-fly zone database. The database may be uploaded during manufacture, or uploaded and updated in real-time during operation and/or charging of a drone. The no-fly zone may also identify a no-look zone, in which the drone is prohibited by internal programming from directing a camera into the no-fly zone.

[0012] Various embodiments of the present technology can be practiced with a local computer system, and/or a cloud-based system. FIG. 2 illustrates an exemplary computer system 200 that may be used to implement some embodiments of the present disclosure. The computer system 200 of FIG. 2 may be implemented in the contexts of the likes of computing systems, networks, servers, or combinations thereof. The computer system 200 of FIG. 2 includes one or more processor units 210 and main memory 220. Main memory 220 stores, in part, instructions and data for execution by

processor units 210. Main memory 220 stores the executable code when in operation, in this example. The computer system 200 of FIG. 2 further includes a mass data storage 230, portable storage device 240, output devices 250, user input devices 260, a graphics display system 270, and peripheral devices 280.

[0013] The components shown in FIG. 2 are depicted as being connected via a single bus 290. The components may be connected through one or more data transport means. Processor unit 210 and main memory 220 are connected via a local microprocessor bus, and the mass data storage 230, peripheral device(s) 280, portable storage device 240, and graphics display system 270 are connected via one or more input/output (I/O) buses.

[0014] Mass data storage 230, which can be implemented with a magnetic disk drive, solid state drive, or an optical disk drive, is a non-volatile storage device for storing data and instructions for use by processor unit 210. Mass data storage 230 stores the system software for implementing embodiments of the present disclosure for purposes of loading that software into main memory 220.

[0015] Portable storage device 240 operates in conjunction with a portable non-volatile storage medium, such as a flash drive, floppy disk, compact disk, digital video disc, or Universal Serial Bus (USB) storage device, to input and output data and code to and from the computer system 200 of FIG. 2. The system software for implementing embodiments of the present disclosure is stored on such a portable medium and input to the computer system 200 via the portable storage device 240.

[0016] User input devices 260 can provide a portion of a user interface. User input devices 260 may include one or more microphones, an alphanumeric keypad, such as a keyboard, for inputting alphanumeric and other information, or a pointing device, such as a mouse, a trackball, stylus, or cursor direction keys. User input devices 260 can also include a touchscreen. Additionally, the computer system 200 as shown in FIG. 2

includes output devices 250. Suitable output devices 250 include speakers, printers, network interfaces, and monitors.

[0017] Graphics display system 270 include a liquid crystal display (LCD) or other suitable display device. Graphics display system 270 is configurable to receive textual and graphical information and processes the information for output to the display device.

[0018] Peripheral devices 280 may include any type of computer support device that adds additional functionality to the computer system.

[0019] The components provided in the computer system 200 of FIG. 2 are those typically found in computer systems that may be suitable for use with embodiments of the present disclosure and are intended to represent a broad category of such computer components that are well known in the art. Thus, the computer system 200 of FIG. 2 can be a personal computer (PC), hand held computer system, telephone, mobile computer system, workstation, tablet, phablet, mobile phone, server, minicomputer, mainframe computer, wearable, or any other computer system. The computer may also include different bus configurations, networked platforms, multi-processor platforms, and the like. Various operating systems may be used including UNIX, LINUX, WINDOWS, MAC OS, PALM OS, QNX ANDROID, IOS, CHROME, TIZEN, and other suitable operating systems.

[0020] The processing for various embodiments may be implemented in software that is cloud-based. In some embodiments, the computer system 200 is implemented as a cloud-based computing environment, such as a virtual machine operating within a computing cloud. In other embodiments, the computer system 200 may itself include a cloud-based computing environment, where the functionalities of the computer system 200 are executed in a distributed fashion. Thus, the computer system 200, when configured as a computing cloud, may include pluralities of computing devices in various forms, as will be described in greater detail below.

[0021] In general, a cloud-based computing environment is a resource that typically combines the computational power of a large grouping of processors (such as within web servers) and/or that combines the storage capacity of a large grouping of computer memories or storage devices. Systems that provide cloud-based resources may be utilized exclusively by their owners or such systems may be accessible to outside users who deploy applications within the computing infrastructure to obtain the benefit of large computational or storage resources.

[0022] The cloud may be formed, for example, by a network of web servers that comprise a plurality of computing devices, such as the computer system 200, with each server (or at least a plurality thereof) providing processor and/or storage resources. These servers may manage workloads provided by multiple users (e.g., cloud resource customers or other users). Typically, each user places workload demands upon the cloud that vary in real-time, sometimes dramatically. The nature and extent of these variations typically depends on the type of business associated with the user.

[0023] The present technology is described above with reference to example embodiments. Therefore, other variations upon the example embodiments are intended to be covered by the present disclosure.

Claims

What is claimed is:

1. A method for limiting access to airspace by drones, the method comprising:
receiving position information from a user associated with a property identified by the position information;
assembling the position information with other position information to compile a comprehensive no-fly zone database; and
pushing the no-fly zone database to at least one drone, the drone accessing the no-fly zone database to determine if movement is allowed, the drone being programmed to not fly into areas identified in the no-fly zone database.
2. The method of claim 1, wherein the drone is further programmed to prohibit directing a camera into the areas identified in the no-fly zone database.
3. The method of claim 1, further comprising:
receiving further position information from a plurality of other users associated with other properties identified by the further position information;
wherein the pushing of the no-fly zone database is to a plurality of drones, the drones accessing the no-fly zone database to determine if movement is allowed, the drones being programmed to not fly into areas identified in the no-fly zone database.

Abstract

A method is provided for limiting access to airspace by drones. The method includes receiving position information from a user associated with a property identified by the position information. The method also includes assembling the position information with other position information to compile a comprehensive no-fly zone database. The method further includes pushing the no-fly zone database to at least one drone. The drone accesses the no-fly zone database to determine if movement is allowed, and the drone is programmed to not fly into areas identified in the no-fly zone database. In the method, the drone may be further programmed to prohibit directing a camera into the areas identified in the no-fly zone database.

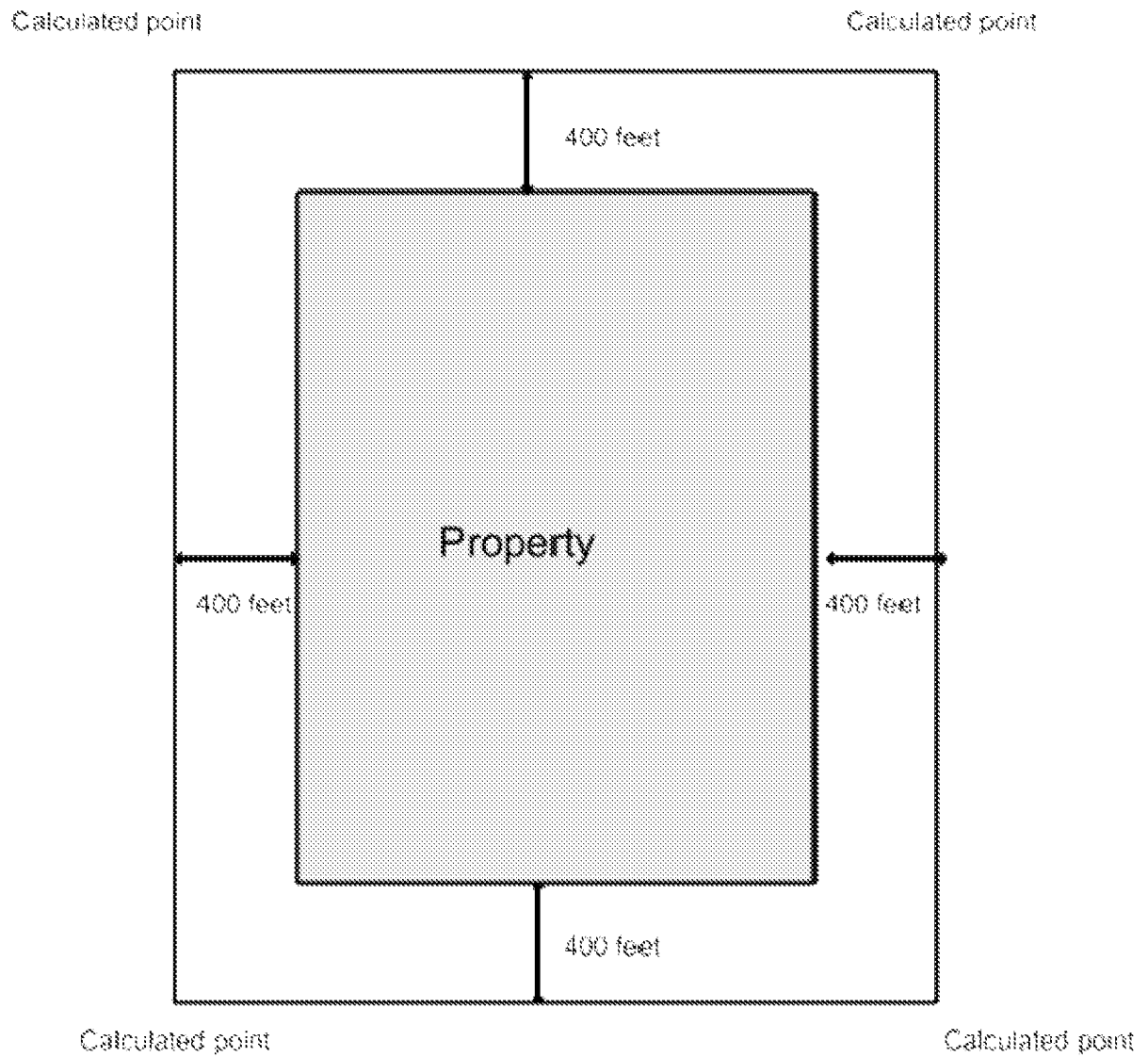


FIG. 1

200

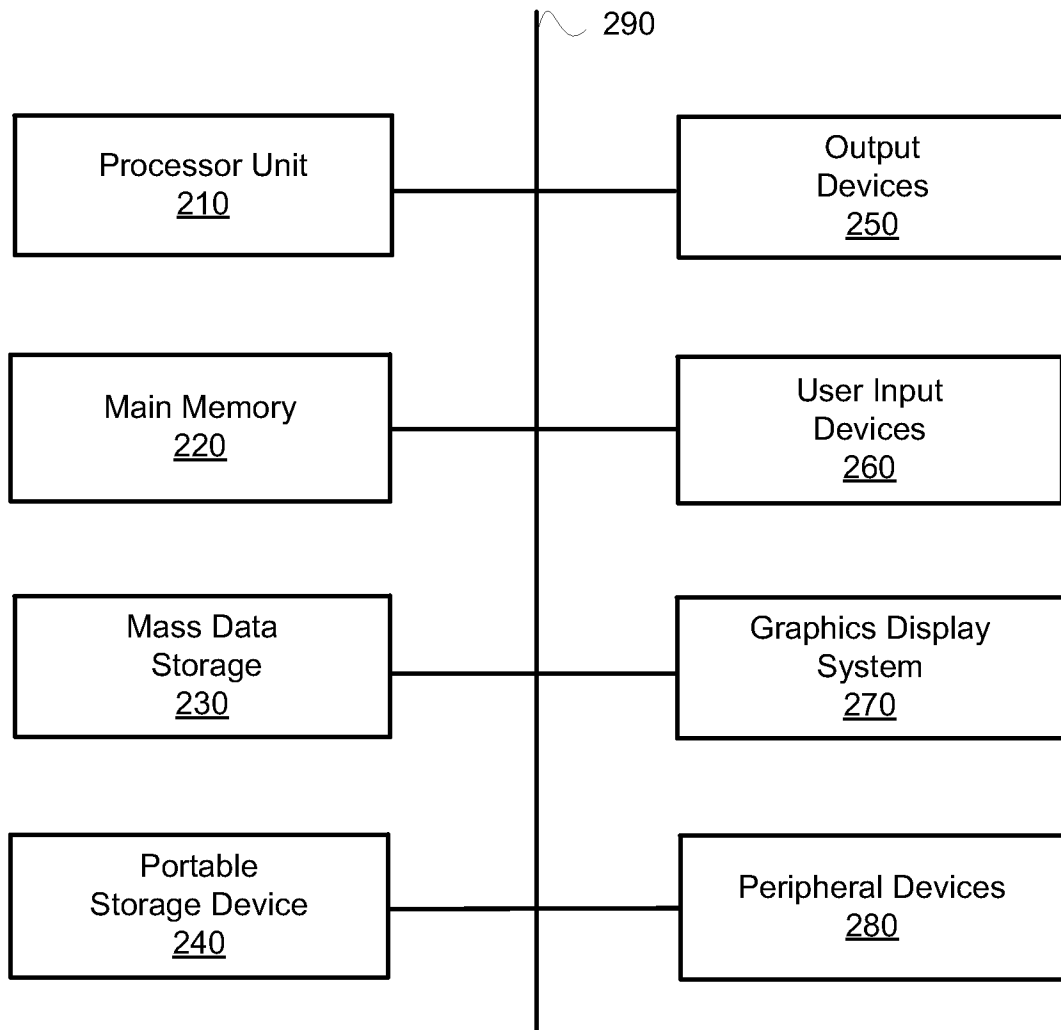


FIG. 2

APPENDIX A

Additional Description

Title of the Invention: Personal Airspace Exclusion Zones

Background of the Invention

Evolving technology is allowing drones to have a positively disruptive impact on everyday lives through many applications. However, drones may also disrupt lives in a negative way. While the FAA and other similar regulatory agencies around the world struggle with implementing rules about drones, drone manufacturers and operators want to take an affirmative step to self-regulate and deliver quality products and services while minimizing negative consequences.

Many people are concerned about privacy and safety. A dedicated website offers these people a method to control the airspace above their property and to prevent drones from flying over. The service physically prevents drones from flying over opted-out property by including those areas in the drone's no-fly database.

Additionally, the dedicated website provides drone manufacturers with a database of other sensitive areas, such as airports, military installations, schools, industrial plants, etc., limiting the manufacturers' risk and liability exposure.

Some drones have a no-fly database that includes certain airports, preventing drones from coming too close to manned aircraft that are taking off and landing. Also, some drones have an altitude limiter (usually 400 feet). However, there is no system yet that prevents drones from flying over land owned by individuals who do not wish for drones to fly there. This technology allows individuals to submit their address to be included in the database of opted-out properties that participating drones will automatically be prevented from entering.

Various governmental bodies have created rules and regulations to try to constrain the operation of drones. For example, certain cities have passed ordinances prohibiting remote-control aircraft from being flown in public spaces. Additionally, some property owners have taken to shooting down overflying drones.

Regulations are not effective because there is extremely limited enforcement capability and drone owners are mostly ignoring the rules.

Summary of the Invention

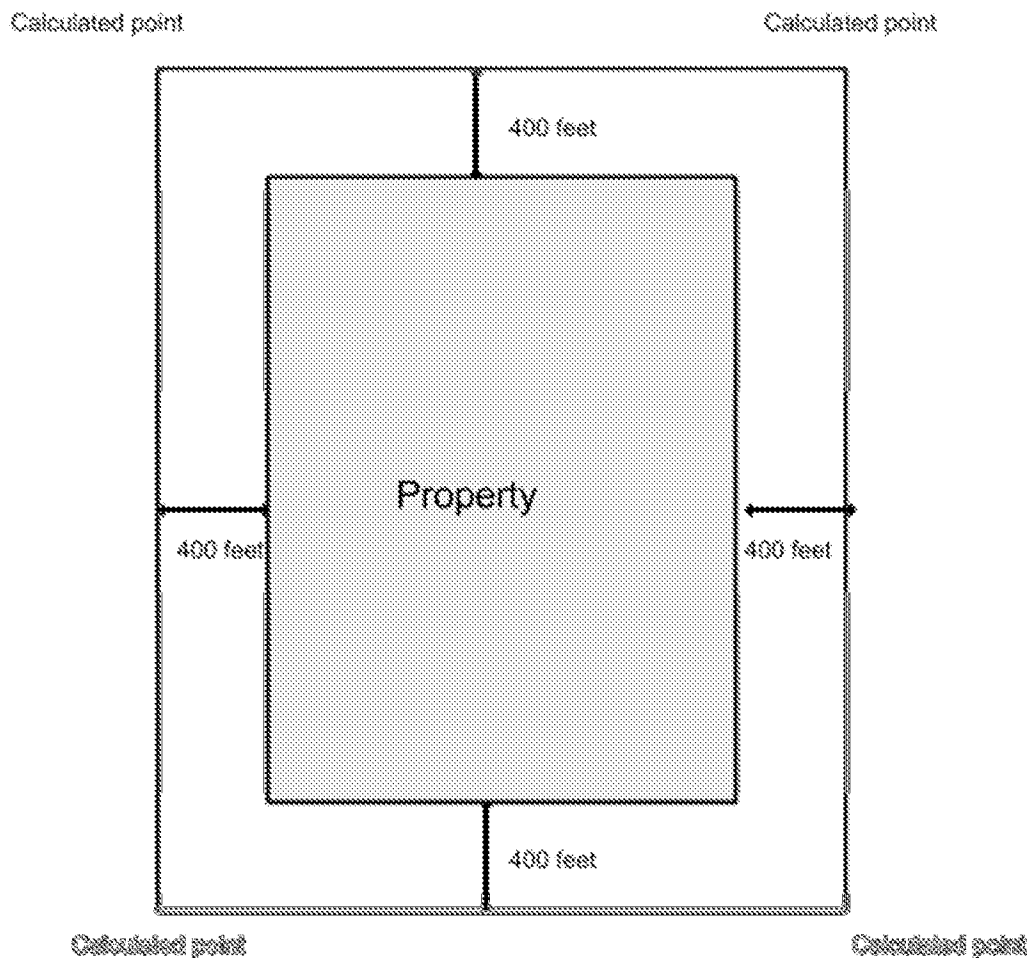
A customer enters his or her address on the dedicated website.

Initially, a 500 foot radius around the lat/long of the property address is blocked from drone flyovers. In alternative embodiments, the radius may be adjusted based on a size of the property, or by using GIS shape files to make the blocked area more precise. Additionally, there should be some buffer around the property to prevent people from flying on the outside and looking in.

Public information may be used to correlate an address to a latitude and longitude coordinate and create a database of those coordinates. A database may be provided to drone manufacturers, operators, platform developers, etc. who will incorporate the no-fly zone database in their controllers. The controllers may use algorithms to determine if a point is inside or outside of an exclusion zone, defined by either a radius from an individual point, or a set of points that draw the corners of a polygon.

In alternative embodiments, public information may be used to correlate an address to a set of latitude and longitude coordinates that define the corners of the polygon corresponding to the property lines. These points will then go into the database provided to the drone makers.

In further alternative embodiments, the polygons may be used with an algorithm to expand those boundaries by a certain distance (for example, 400 feet), such that there is a 400 foot buffer around the entire property. This will prevent higher-flying drones from being able to take a picture from outside the property looking in. See diagram below and presented as Figure 1:



Drones may be connected to a network, for example the internet, while flying or during a charging operation. This allows for real-time updates to no-fly zones. For example, if the FAA publishes a temporary flight restriction, in exemplary embodiments that information can be pushed to update all drones.

Internet-connected drones allow for more customization of personal airspace access rights. For example, If an individual property owner wishes to allow flights at his property on a Saturday, that is possible. Additionally or alternatively, an individual may elect to permit a particular drone operator, for example Amazon, to land and takeoff from their property. This permission may be limited such that transit through the airspace above the house is not permitted. This information and the associated permissions may be pushed in real time to drones.

In still further embodiments, property owners may collect revenue for permitting access to the airspace above their property. For example, a property

owner may prefer a drone operator, for example Amazon, to not over-fly their property, but may be willing to allow it if there is an appropriate compensation. In this manner, a bidding system may arise for drone operators to fly cost-optimized routes, with airspace access fees being one component of the total cost.

The present technology gives individuals the opportunity to make known their desire for privacy, and gives drone makers an easy way of automatically complying with those requests. In this manner, the development of the drone industry may be promoted by empowering the public to manage their participation in the system and/or their privacy. This solution provides a simple means for property owners to express their desire for privacy and for drone makers and operators to voluntarily comply with those requests.