Privacy aware restricted areas for UAS's

PETER BLANK, SABRINA KIRRANE, SARAH SPIEKERMANN
Vienna University of Economics and Business
Institute for Management Information Systems
firstname.lastname@wu.ac.at

Abstract— Although drones are receiving a lot of attention from industry and academia alike, the protection of citizen privacy is still an open issue. To this end, we demonstrate how basic principles of information privacy could be integrated with existing infrastructure to build up a framework for privacy aware UAS dispatch considering restricted areas. The software framework proposed, enables UAS operators to determine whether a selected UAS flight path intersects with a restricted area, by considering privacy preferences that can be configured by citizens themselves.

Index Terms—Privacy, Unmanned Aerial Vehicles, Drones

1 Introduction

Unmanned Aerial Vehicles (UAVs) otherwise known as 'drones', are flying platforms that are controlled remotely. Recently, drones, which come in many shapes and sizes, have experienced increasing attention due to expanding capabilities, such as longer flight durations and interesting application areas (for instance face recognition or tracking). UAVs combined with analytical systems form unmanned aerial systems (UASs) that have already shown great potential especially in governmental applications, such as law enforcement and rescue service domains. A first investigation into this potential was conducted in 1999, when Murphy and Cycon proposed the use of mini-UAVs in law enforcement surveillance applications [1]. While, a subsequent study in 2007 by the European Commission indicated high potential usage of UASs not only by law enforcement, but also by border security and the coastguard [2]. Already police forces have started testing and deploying UASs in practice. For example, UASs have been used for crime scene or accident photography [3], and in order to locate (injured) persons [4]. Considering the ongoing advancement of UAS technologies, UASs have the potential to become an important support in a variety of public and private sector activities.

That said, drones can cause privacy harms as they can potentially invade people's private space, and accidentally expose them by processing personal data against their will. Additionally, privacy violations can occur through the unsuspecting collection of information concerning random citizens without any purpose, simply due to constant video recording while flying. For example, Finn and Wright [5], show that UASs can be used to monitor large crowds, which can be used in terms of border patrol or crime prevention. Police operated UAVs may frequently cross private property on their way to an operational area, e.g. when flying to an accident or simply monitoring an area. For citizens living in the approach corridor, near the landing and starting places of UASs or frequently passed routes, this can be disturbing because of the close proximity and noise, the frequency or both. With a UAS sensor system capturing citizens property, the citizen can be recorded, identified or recognized on his or her property even though the reason for dispatch is another subject or target.

From a societal perspective, it is necessary to assess privacy related considerations, such as the impact constant flying and filming of property in the surrounding area has on individuals. From a legal perspective, it is necessary to get consent from individuals before they are recorded and also to provide transparency with respect to the data that is captured and the type of processing. Although this could prove burdensome for UAS operators compliance is imperative to gain broad acceptance of the technology by society. One way to avoid unnecessary or 'unintended' privacy violations is to check the flight path for potential privacy violations a priori. Depending on the reason for UAV deployment, for instance in the case of maintenance or routine flights, flying over private property can be avoided by rerouting the UAV.

Despite these obvious privacy issues, recent research efforts focus primarily on optimizing the UAV platform, such as UAS routing in larger groups (swarms), their sensor capabilities or software algorithms. Most of the emphasis is put on the technical advancement of potentially privacy-invasive activities, such as monitoring of crowds or airborne surveillance and tracking. However, the legal cases around the deployment of drones in the US already show that privacy aware UAS deployment is

of crucial importance for UAS usage. This paper aims to address this gap by examining privacy challenges associated with tactical UASs. We propose a framework that deals with privacy aware UAS deployments by granting citizens some degree of control over the UAS flight paths. The proposed dynamic UAS routing framework can be used to ensure that drones do not fly over private property.

2 PRIVACY AND DRONE DEPLOYMENT - THE STATUS QUO

When it comes to UASs and privacy related research in the US, to date the focus has been on the legal implications. McBride highlights that law enforcement agencies are pushing for (small) UAVs in tactical operations supporting ground police units. He further discusses three famous supreme court decisions regarding aerial surveillance by police forces. In the first of these three cases, California v. Ciraolo, the police were informed of illegal activities on a private property. The police forces subsequently deployed an airplane to fly over a private property which was protected by fences and took photos of growing marijuana. The supreme court dismissed the case as the police forces violated the privacy rights of the suspect. In Dow Chemical Co. v. United States, the supreme court ruled that privacy privileges in regard to aerial photography do not apply in the context of industrial facilities spanning over 2000 acres. The supreme court decided that commercial property is subject to the 'open fields doctrine' as opposed to the 'curtilage doctrine'. The third case investigated, was Florida v. Riley, where police observed a partially overgrown greenhouse, located in a backyard. The observation which was carried out from a helicopter was judged to be a 'search' for which a warrant would have been required [6]. Together these three cases have had a major impact on aviation based surveillance under the Fourth Amendment in the US, as they defined aerial surveillance as a 'search' when a considerable expectation of privacy is breached. However, such an expectation is not applicable for industrial facilities, but rather protects private property under the 'curtilage docrtine'. Following the privacy discussion about UASs, Calo, (2011) [7], expects UAVs to become a privacy catalyst. He predicts that UASs related privacy concerns will "gain serious traction among courts, regulators and the general public" [7, p. 32].

When it comes to UAS privacy in Europe, a number of laws regarding the design of privacy aware drones need to be considered; mainly the EU data protection directive (95/46/EC), the EU Regulation on the protection of processing by community bodies and the free movement of data (2001/45/EC), the General Data Protection Regulation (enforcement to start in May 2018), and the forthcoming Data Protection Directive for public authorities (DPD). The upcoming EU regulation specifies, amongst others, the impact of compliance breaches, which are discussed later in the paper. However, as community law is usually not applicable for law enforcement, when it comes to public authorities, the DPD is the most relevant. Although there has been very little research on privacy for UASs, [8] propose several comprehensive privacy-by-design principles. At the most basic level UAS privacy should be *proactive and preventative*, it should be the *default setting*, usable without adaptions. It must be an integral part of the solution, *embedded into the system* from the very beginning. It needs to be *fully functional* in coherence with other relevant principles, such as security. Additionally, *visibility and transparency* with respect to processing are required in order to gain broader acceptance from the public and its various stakeholders. Essentially, *respecting privacy* requires UASs to offer user friendly options, such that for example strong privacy defaults are set and adequate warnings of UASs gathering data are setup in the relevant regions. While, the *life time protection* of the proposed privacy mechanisms should be guaranteed via regular privacy impact assessments, that allow privacy principles to be translated into required actions, which can be addressed by privacy enhancing technologies [9], [5]. Further principles for personally identifiable information in information privacy are discussed by [10], which specifies that organizations must process data only collected for a specific, explicit and legitimate purpose which are relevant adequate and limited to this purpose and processed lawfully, fairly and transparent for the data subject. Also, data must be accurate and kept up to date with reasonable effort, kept in a form that does not permit identification and be processed under the responsibility and liability of a controller that has to show compliance with the regulation.

3 TECHNICAL ADVANCES TO PROTECT CITIZENS' PRIVACY RIGHTS THROUGH UAS ROUTING

Against the background of the legal situation it is important to see where we stand in terms of privacy by design for UASs: what technical research and development could be used to address some of the legal thinking? Can we technically ensure that police forces don't violate the private rights of individuals by crossing their territory, potentially filming? In Europe, we expect that citizen's consent to UASs data collection over their private property could become an issue, as well as the desire of citizens not to be disturbed by UAVs i.e. their right to be let alone. One crucial enabler necessary in order to respect citizen preferences is to equip UASs with intelligent routing technology. Smart routing technology would allow UAVs to routinely avoid areas that are marked as 'private'.

To date, a number of authors have tackled and industry has proposed routing algorithms for UASs. DJI, a UAV manufacturing industry company, developed a static approach for restricted area recognition in which property coordinates are compiled into the UASs software. By forcing GPS equipped UASs to stop at the border of a restricted property, the software allows the UAS to recognize restricted areas without requiring internet access. This approach is intended for small UAVs and is used to block access to specific properties, such as airports or military areas.

The UAS will stop at the very border of the restricted area (in both, height and planar coordinate) and wait for new instructions while hovering. If the UAS runs out of energy, it tries to perform a save emergency landing at its current position. Another complementary industry solution is offered by the website 'NoFlyZones.org'. Participating UAV manufacturers are able to consult a database that contains names and addresses of property owners, and integrates the relevant restriction into the UAV software, by looking for coordinates that are associated with the addresses.

One of the limitations of existing systems is the fact that property restrictions are compiled into the UAS software, meaning it is difficult to make changes. In addition, it is not possible to specify permissions for specific contexts e.g. in an emergency situation a privacy infringement may be acceptable. The framework proposed in this paper intends to solve these problems by catering for real-time querying of context specific permissions and by enabling

One of the limitations of existing systems is the fact that property restrictions are compiled into the UAS software, meaning it is difficult to make changes. In addition, it is not possible to specify permissions for specific contexts e.g. in an emergency situation a privacy infringement may be acceptable. The framework proposed in this paper intends to solve these problems by catering for real-time querying of context specific permissions and by enabling citizens to amend these permissions at any time. As the software itself does not need to be updated, citizens are given a greater degree of control over their privacy preferences.

4 A FRAMEWORK FOR PRIVACY-FRIENDLY UAS ROUTING

The proposed privacy framework, which is depicted in Figure 1, distinguishes between four types of actors: system operators, service providers, citizens and authentication service providers. When considering police forces using UASs, the system operator can be a police officer in a UASs control center and the service provider can be a police organization or a ministry. Any citizen holding a legal property title may use the system in order to set their privacy preferences. While, it is envisaged that the authentication service providers are trusted Eidentity providers. These actors interact with six different modules in our privacy framework: Firstly, the property coordinates must be represented using a specific *Geospatial projection* and *associated with certain attributes*, for instance specific permissions for flying over a property. In order to enter data, citizens need to identify themselves via an *authentication infrastructure*, which is offered by an (external) authentication provider. After authentication the citizens can enter *details about their private properties using a web interface* that is offered by the service provider. Based on the data input, a checking entity is required to confirm the correctness of the request. After the correctness check, *convex hulls* can be calculated to increase the efficiency of the calculation of the flight path. The system operator can select and request *the flight path calculation from the system*. If there is no intersection between flight path and restricted areas, the flight path can be submitted to a UAS control program. Finally, the UAS control program handles the communication to the UAV, allowing it to be dispatched according to the flight coordinates chosen. This section provides a detailed description of each of the six system modules.

4.1 Representing geospatial data using a digital map

The selection and assignment of a *geospatial* projection, which is a representation of the earth surface, is of utmost importance for the accuracy of the UASs flight path selection. The flight path and the coordinates used for storing restricted areas are displayed in the chosen projection on a digital map. To date there is no perfect representation of an oblate spheroid therefore projections differ significantly and are even prone to distortions. The most common projections are either cylindrical (e.g. Mercator projection), planar (e.g. Un-Projected Latitude and Longitude) or conic (e.g. Lambert Conformal Conic) projections. Figure 2 depicts an example of those differences by showing three projections of the United States in red (Mercator), blue (Labert Conformal Conic) and green (Un-Projected Latitude and Longitude). The distortion of projections can also be assessed by consulting Google Maps, which uses the Google Web Mercator WGS84 (EPSG:3857) projection. By comparing Greenland to Australia on Google Maps, Greenland appears much larger then Australia whereas in fact it is only ~28.16% of its size. Once the *geospatial projection* is assigned, geometric data types such as GEOM can be used to store coordinates associated with private properties as polygons. Therefore, it is either necessary to use a standard projection, e.g. the Mercator projection, that is compatible with the particular GPS sensor of the UASs or to convert between the sensor data and another projection on demand. Spatial database extensions such as PostGIS allow for the conversion between or storage of coordinates associated with different projections.

4.2 Efficient storage and querying of property data

The data properties and storage module caters for the efficient storage and querying of property data that is gathered via a web interface. As property databases may need to hold a vast amount of data and real-time processing may be necessary for privacy considering police operations, the efficiency of the database is of utmost importance. For instance, if one is considering Germany,

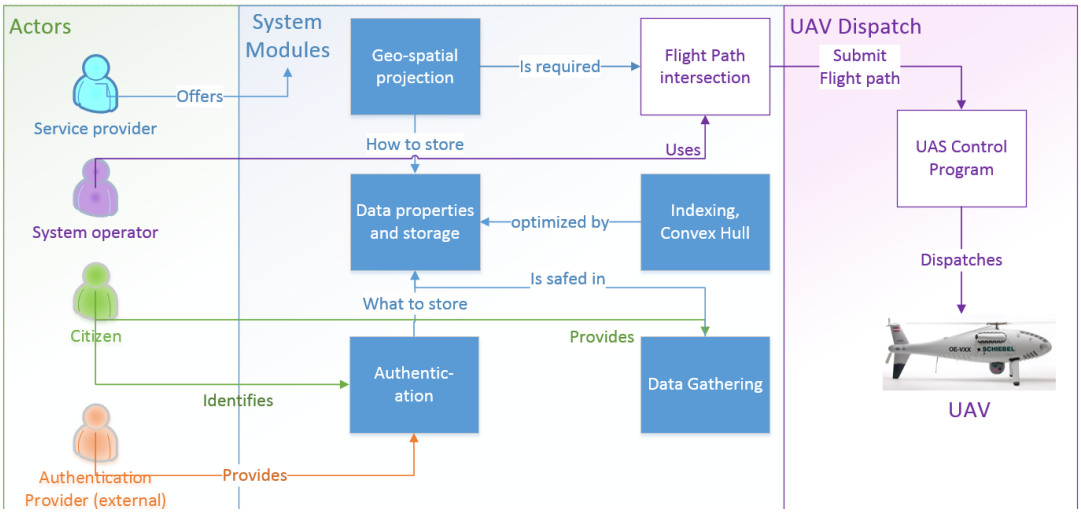

Fig 1: Software System Architecture

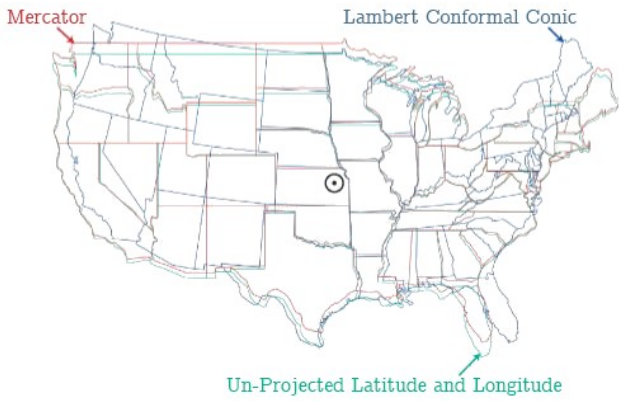

Fig. 1: Different Projections and their deviations, Adopted for better readability from Peter H. Dana, The Geographer's Craft Project, Copyright 1997

the private house-ownership rate is estimated at 48% (~19 million) [11]. If only 8% of these house owners define a privacy preference and each property has several border points (let's assume 5), one would find 7.6 million entries for Germany alone. Furthermore, for each property there can be a set of optional contextual permissions stored, e.g. that police UAS may only fly over a property in emergencies, but not for routine flights. Although the search space increases with the number of additional properties, scalability can be achieved by indexing the data based on attributes that are commonly used for querying e.g. the number of coordinates, regions, and political areas.

In some European countries like Germany, Austria, Great Britain or France there is no direct mapping between the land register or cadastral map and any of the available projections. In the United States the land registration is a matter of state regulations such that only public lands of the USA are centrally mapped by the Bureau of Land Management. China currently dictates that all land ownership and leaseholds are recorded in an official register, however there is no general procedure on how to register a property. To achieve a mapping between a projection and the registers of restricted areas, there are two different approaches to be considered. Firstly, the public authorities could include the (EPSG-) projection coordinates in their current registers and introduce a converting schema or update their existing registers to a digital format. However, it appears to be rather complex to establish a general mapping into a digital format. Secondly, it is possible to allow user generated input by choosing the coordinates via a digital map. The latter may appear to be less costly in the first place, but significant efforts may be needed in order to check the correctness of the user entered data. Such an approach would require a checking entity to gather information about the user's identity, whether the user is the property owner, and to verify the property borders in the chosen projection. Without the interconnection of existing data sources, such a validation of property claims cannot be conducted in an automated way.

4.3 Citizen authentication

When it comes to *authentication*, where available, an existing digital (e-) identity infrastructure for citizens can be used to verify individual users identities via electronic signatures. In Europe a 'eIDAS Regulation' governs electronic identification services, trust services, electronic signatures or seals [12].

Notably, several European countries have already set up infrastructures that support e-identities including Austria, Belgium and Estonia, among others. By using the existing e-identity infrastructure for authentication, users can register certain polygons as their private property. A checking entity can subsequently use the public land register to check the claim. Users may specify different kinds of permissions. Possible options could include: 'permit flights', 'prohibit flights' or 'permit flight for emergencies operations only'. Permissions may be changed at any time by the user.

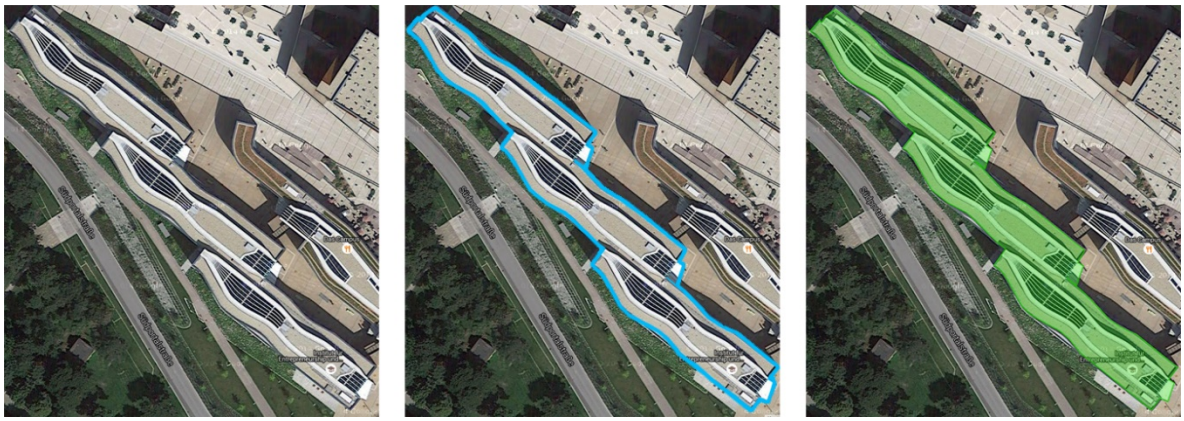

Fig 2: Polygon registration via map interface
(a) Satellite Image by Goolge Maps; (b) Selecting property borders (Blue line); (c) Registered Polygon (solid space – green)

4.4 Recording property coordinates and privacy preferences

Given the unavailability of relevant data about private properties and their coordinates in in the form of projections, we chose the second *data gathering* approach, that involves user input. A digital map, which is presented to the user, see Figure 3 (a), allows citizens to enter their information (e.g. contact details, restricted areas and permissions). By clicking on the borders of the relevant property, a polygon is generated on the map and its coordinates are fetched from the map, as depicted in Figure 3 (b). Privacy preferences are entered via a webform similar to the operator interface depicted in Figure 5. Once the user has confirmed that the private property is completely and correctly covered, the polygons' border (points) are stored as coordinates in the database. The user input may be edited, declined or accepted by a checking entity, e.g. the service provider. This entity has to take care that users property claims are correct and the property borders are defined accurately, for instance based on the prior mentioned land register and cadastral maps. After the correctness has been verified an overlay, which is visualized in Figure 3(c), is used to depict a restricted area and further serves as input by the flight routing algorithm.

For public or commercial users the treatment of areas, according to area classes can be useful. Special areas such as airports, military facilities, embassies, emergency areas or venues on specific dates and times may require extended *restricted fly* areas for UAVs, larger than their actual property border. Such properties may be assigned a different *class* and *color* than 'normal' private property. The calculation of a buffer zone around such areas can be generated, for instance a *restricted fly zone* of 5kms for military facilities and 3km for airports or emergency services. Depending on the country, different guidelines for the minimum distance of the buffer zone may apply. For instance, the US demand that UAV pilots that come within a five mile radius of an airport, contacts the airport authorities [13], to inform them about the flight. Additionally, buffer zones that cater for safety-related issues, such as accidents, fire-bursts or shootings, could be set up dynamically. For example, UASs belonging to private persons or media professionals, may not be allowed to enter the wider area, whereas UASs operated by police, ambulance or firefighter forces may be permitted access. In order to calculate such a buffer, two general approaches can be taken: first, each coordinate of an area is enlarged by a certain distance; or second a centroid coordinate is chosen and a circular buffer calculated based on the required distance from the centroid. The first solution results in an exact, extended geometry of the object that can be based on the distance calculation. Using a buffer that extends the coordinates by a specified distance may be preferable if high accuracy is demanded. Choosing the second option results in a circular shape around a central point, which usually requires less calculation effort and data transmission. However, it requires additional effort to calculate a centroid.

4.5 Reducing the number of property coordinates

A *convex hull* of a property is the smallest convex polygon which encloses that property. By using convex hulls the coordinates that need to be stored for each property can be decreased significantly, however the knock-on effect is that the accuracy of the restricted area is reduced. A convex hull may never be smaller than the actual polygon it is calculated for, but can hold an equal or smaller amount of points (coordinates). With less coordinates, the flight path processing becomes more efficient as less intersection testings between the flight path and the restricted areas are required. For calculating convex hulls we used the 'Quickhull' algorithm, which is based on the 'Quicksort' algorithm.

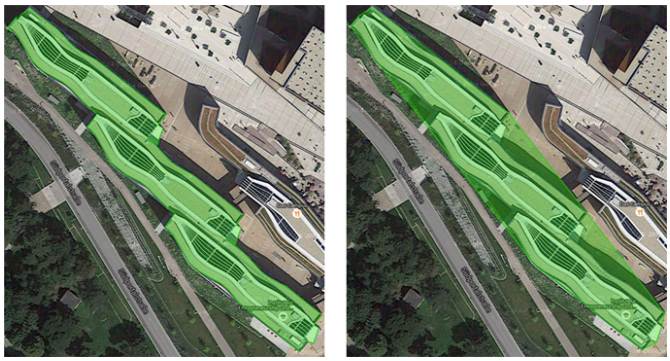

Fig 4: Convex hull of a property
(a) Registered Polygon; (b) Convex Hull

4.6 Flight path selection and calculation

The police operator uses the operator interface, in order to select and calculate a *flight path*. The interface allows waypoints (coordinates) to be selected and information about altitude (1), required accuracy (2), stay-time at waypoint (3), yaw angle at waypoint (4), take off at first waypoint (5), land at last waypoint (6), selectable UAV type (7) and select UAV control program (8) to be entered. The interface is depicted in Figure 5. The flight path evaluation is based on the intersection between the path and either the coordinates of the convex hull or the original coordinates. By intersecting each pair of coordinates from the polygon with each pair of coordinates from the flight path, it is possible to detect infringements. Once an intersection is found, the use of the flight path is prohibited by deactivating the export of coordinates to the control program. In the case of an infringement, the operator has to select a new route and test the route again.

Another approach would be to deactivate the sensor recording when flying over a private property. This could in principle be based on the framework above, by changing the requirement from avoid flight paths to deactivate the sensors. Notably, the noise and visibility of the UASs would not be solved by extending the framework to cater for sensor deactivation. Additionally, sensor systems like cameras can record an area even if they are not above or in close proximity to it. Thus, a simple deactivation of sensors when flying over a property is insufficient. For a privacy aware system, a more complex calculation that considers contextual information from the sensor system would be required. Alternatively, one could edit the sensors recording in the live stream from a camera, such that only those properties without a restriction are recorded. This can for instance be done by secure visual object coding, pixelating the recorded data stream [14].

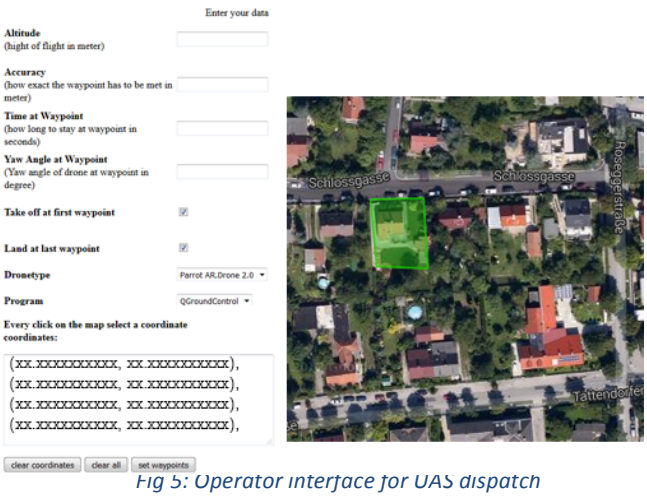

Fig 5: Operator interface for UAS dispatch

5 PROTOTYPICAL IMPLEMENTATION

In order to verify the effectiveness of the proposed framework, we developed a web based prototype that uses software known as QGroundControl (QGC) in order to interact with a Parrot AR.Drone 2.0. A Microsoft SQL Server database with spatial functions was used for data storage and querying. The operator and citizen interface, were developed in HTML5, CSS, JavaScript, PHP and used the Google Maps API. The flight path intersection testing itself was implemented in TSQL, while PHP was used for other server side processing such as the calculating convex hulls with the 'Quickhull' algorithm, when setting new restricted areas. The server side processing is required in order to use thin-clients, such as mobile phones. JavaScript, together with the Google Map API, enables citizens to select their property and operators to view restricted properties, as shown before in Figure 3. A screen shot of the user interface is presented in Figure 5. Although the responsiveness of the map decreases with the number of restricted areas to be displayed, this limitation can be mitigated by the just-in- time loading of properties that are within the borders of the current map.

The police operator interface caters for the configuration of the flight path attributes outlined in the preceding section. These attributes are based on the capabilities of the QGC software, which was used for testing the software. While altitude, accuracy, take-off and landing are mandatory

attributes, the stay-time and yaw angle can be left empty. The UAV type and control program selection attributes provide support for different control programs and give metrics about the flight duration, based on the average speed of the UAV. QGC allows routing information to be imported or exported and handles the communication with the UAV via the MAVLink protocol. Moreover, distance and flight time calculations are performed via PHP and displayed on a flight checking interface. In order to distinguish between different property categories or permissions, different color schemas were introduced. Green denotes private property, orange airports and red military zones. A blue line is used to depict the flight path in the Google Map. The buffer around specific areas have not been implemented, but could be introduced by using a mechanism comparable to the distance calculation that was implemented as part of the flight metrics.

5.1 Evaluation of the Prototype

The effectiveness of the proposed system is evaluated from both a usability and scalability perspective.

Evaluating the Usability of the User Interface

In the first experiment, thirteen people were asked in isolation (i.e. the participants were not able to talk to one another after the sessions) to use the software and apply a think aloud technique. The participants were asked to create at least one restricted area by themselves and to select several flight paths, whereby one or more flight paths intersect with their restricted area. Participants were asked to verbalize their thoughts immediately when interacting with the system [15]. Based on the feedback received we refined the layout and added a more precise instruction manual. While the map itself was intuitively usable and demanded no further work, changes were made to achieve a more usable menu structure. In addition, buttons, an introductory tutorial describing how to use the software and the export functionality were developed. Also, as some participants asked for the duration, distance and whether the selected UAS type could even make it, more information was offered once the route was selected, for instance the flight distance and the minimum time required to reach the destination.

In the second experiment, eight participants were asked to evaluate the user interface. To better resemble a real world application, basic authentication functionality was introduced and dummy accounts, tailored to the participants names, were constructed and tested. Again, a think aloud technique was employed, however, on this occasion only minor changes were suggested by participants. Most participants intuitively construct restricted areas for either their own or their relative's buildings. The terminology used e.g. UAS or UAV, was updated in order to make the software more accessible. The coloring used on top of the Google map was adapted to cater for easier selection and better visibility, as suggested by several participants.

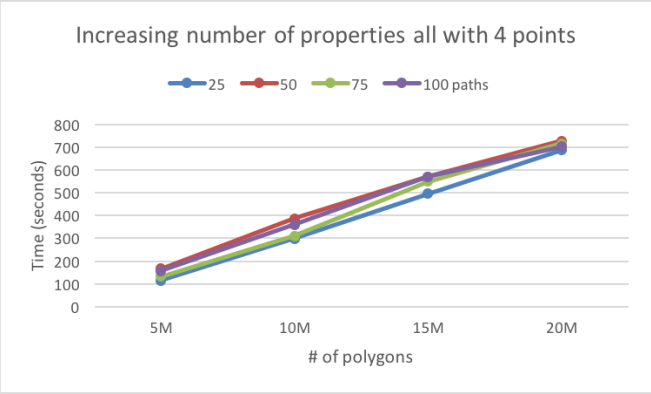

Fig 6: Query performance over increasing datasets

After incorporating the aforementioned changes, in the final experiment, a real-world application evaluation was conducted. For this experiment, two small restricted areas were assigned to a field in Lower Austria. One restricted area was used with its convex hull, the other without. Six participants selected several flight paths that either went around or through the restricted areas. If an intersection with a restricted area was found, the coordinate export was disabled, making a start of the UAS impossible. The participants managed to successfully deploy the UAS via QGC, while selecting a flight path without restricted areas without further instructions or help.

5.2 Examining the Performance and Scalability of the System

To test the feasibility of the approach in terms of performance and scalability, we simulated 20,000,000 polygons. This is slightly more than the before mentioned 19 million private households in Germany [11]. In the experiment described above, all participants were asked to create their own restricted areas.

Those areas consisted of several points. However, after applying the convex hull algorithm we found that the majority of polygons consisted of only four points. Thus, the evaluation was conducted over increasing datasets containing between 5 and 20 million polygons (5M, 10M, 15M, and 20M) with a relatively small number of points per polygon (i.e. 4, 6, 8, and 10). In order to assess the impact of increasingly complex flight paths, we also tested for increasing flight path complexity, whereby a flight path had several different points that needs to be checked (i.e. 25, 50, 75, and 100).

Figure 6 shows that querying scales linearly with the number of points that need to be checked. Polygons with 6, 8, and 10 points exhibited similar behaviour. Likewise, the disk space requirement to store the 5M, 10M, 15M and 20M polygons scales linearly (i.e. 563408, 1126776, 1690152 and 2253536 kilobytes respectively). In order to improve the efficiency of the flight path checking it is possible to generate indexes based on commonly queried attributes e.g. the range of coordinates, regions, and polit-

ical areas. By reducing the search space e.g. to 5 million polygons, we find that the flight path testing takes on average 143 seconds for a flight path with 4 points. At 10 million polygons in the same setting, we find a duration of 338 seconds. However, it is worth noting that in a realistic setting the number of properties along a route than need to be checked would be much less than 5 million.

5.3 Social and Legal Implications and Limitations

If privacy aware solutions are not introduced, not only social acceptance is affected but the legal implications can be drastic. In Europe, failing to comply with the upcoming data protection regulations, e.g. processing data without sufficient legal basis like consent, may result in fines of up to 2% of annual turn-over or up to 1 million whichever is higher [10]. In the US, fines have been traditionally higher but data protection regulations less strict, which could lead to comparable effects. Yet, not only fines are relevant for operators, but the permission to operate UASs on large scale will be heavily dependent on the operators ability to comply with both, data protection and aviation regulations. However, UAS operators face a lot of uncertainty with the upcoming and existing regulations as shown by [6]. Additionally, a lack of sophisticated privacy technologies for UAS is making compliant UAS operating even more difficult for both, commercial and private operators.

Frameworks such as the one proposed in this paper are a first step towards greater privacy awareness and legal compliance in the field of UAS operations. However, it is worth nothing that while legal compliance can be imposed more easily on commercial operators by regular controls and checks, in the case of private operators it may be difficult to enforce. For example, compliance could be circumvented by UAV operators that build their own drones or disable the privacy protection mechanisms of commercial drones. Although the risk of getting caught is negligible, we argue that high penalties should be put in place in order to discourage such behaviour.

The proposed framework is a stepping stone towards more socially acceptable and legally compliant UASs. Guided by the privacy-by-design principles proposed by [8], we describe how the proposed framework can be used to enable a *proactive and preventative* approach to privacy whereby *respecting privacy* is achieved by obtaining consent for flying over private property. In the proposed framework privacy is the *default setting* that is *embedded into the system* from the very beginning. Although the system is *fully functional* from a consent perspective, further discussion is needed in order to determine what form of *visibility and transparency* is appropriate in such a setting. Also, when it comes to the *life time protection* of the proposed privacy mechanisms, further research is needed especially in the context of the recording capability that is inbuilt into many UAVs.

One of the limitations of the existing system is the fact that even if the UAV does not fly over a certain property, a sensor, for instance a camera lens, may be able to take records of it. Depending on factors, such as altitude, camera angle and yaw angle, records can be taken from a significant distance, which is not even close to a restricted area. Furthermore, our approach is limited to those citizens holding a legal property title. Nevertheless, when it comes to privacy-by-design solutions for UASs deployment, the proposed solution is a fundamental building block, on top of which, other applications, e.g. calculating which parts of an image have to be pixelated, can be built.

REFERENCES

[1] D. W. Murphy and J. Cycon, "Applications for mini vtol uav for law enforcement," in Enabling Technologies for Law Enforcement and Security. International Society for Optics and Photonics, 1999, pp. 35–43.

[2] European Commission, Enterprise and Industry Directorate-General, "Study analysing the current activities in the field of uavs," ENTR/2007/065, 2007.

[3] E. Pilkington, "'we see ourselves as the vanguard': The police force using drones to fight crime," The Guardian, 2014.

[4] C. Franzen, "Canadian mounties claim first person's life saved by a police drone," online, The Verge, 05 2013, 10. [Online]. Available: http://www.theverge.com/2013/5/10/4318770/ canada-draganflyer-drone-claims-first-life-saved-search-rescue

[5] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," Computer Law & Security Review, vol. 28, no. 2, pp. 184–194, 2012.

[6] P. McBride, "Beyond orwell: The application of unmanned aircraft systems in domestic surveillance operations," J. Air L. & Com., vol. 74, p. 627, 2009.

[7] R. Calo, "The drone as privacy catalyst," Stanford Law Review Online, vol. 64, pp. 29–33, 2011.

[8] A. Cavoukian, Privacy and drones: Unmanned aerial vehicles. Information and Privacy Commissioner of Ontario, Canada Ontario, Canada, 2012.

[9] M. C. Oetzel and S. Spiekermann, "A systematic methodology for privacy impact assessments: a design science approach," European Journal of Information Systems, vol. 23, no. 2, pp. 126–150, 2014.

[10] Council of European Union, "Proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)," 2012, http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX: 52012PC0011.

[11] Eurostat, "Homeownership rate in selected european countries in 2014," 2014. [Online]. Available: http://www.statista.com/ statistics/246355/home-ownership-rate-in-europe/

[12] European Commission and Frost & Sullivan, "Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec," Official Journal of the European Union, 08 2014, 28.

[13] 112th Congress, "Faa modernization and reform act of 2012," 2012, public Law No: 112-95.

[14] K. Martin and K. N. Plataniotis, "Privacy protected surveillance using secure visual object coding," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 18, no. 8, pp. 1152–1162, 2008.

[15] J. Nielsen, T. Clemmensen, and C. Yssing, "Getting access to what goes on in people's heads?: reflections on the think-aloud technique," in Proceedings of the second Nordic conference on Humancomputer interaction. ACM, 2002, pp. 101–110.

Author biographies:

Peter Blank:
Peter Blank is a process and data analytics professional at PwC Switzerland since June 2016. Before that, he was a research assistant at the Vienna university of economics and business, where he primarily focused on privacy related Drone questions. His main fields of interest are privacy for emerging technologies, process mining and data analysis in spatial applications.

Sabrina Kirane:
Dr. Sabrina Kirrane joined the Vienna university of economics and business as a postdoctoral researcher in September 2015. Prior to taking up the position at WU she was a researcher at the Insight Centre for Data Analytics, Ireland. Her PhD focused on the problem of access control for the Web of Data. Before that she spent several years working in Industry on topics around data integration and security, such as system security requirements their and implementation in an application service provider environment. Sabrina's research focuses on the privacy issues that can result from interlinked machine-readable data. Dr. Kirrane is a guest editor for the Journal of Web Semantics special issue on Security, Privacy and Policy for the Semantic Web and Linked Data and besides others organiser of the PrivOn workshop series on Society, Privacy and the Semantic Web - Policy and Technology.

Sarah Spiekermann:
Univ.Prof. Dr. Sarah Spiekermann is a professor for Business Informatics at Vienna university of economics and business since 2009 and chairs the IMIS. Her main areas of expertise are electronic privacy, RFID, personalization/CRM, attention and interruption management (notification platforms) and context-adaptivity. She has been advising the EU Commission in the area of privacy for RFID since 2005, served as a reviewer of RFID FP7 projects SMART and BRIDGE, co-authored and negotiated the PIA-Framework for RFID (signed in April 2011 by the EU Commission) and developed the PIA guidelines for privacy-friendly RFID systems for the German Federal Institute of Information Security (BSI) (published in November 2011).

Author Emails:
Peter Blank: Peter.Blank@Tutanota.com
Sabrian Kirrane: Sabrina.Kirrane@wu.ac.at
Sarah Spiekermann: Sarah.Spiekermann@wu.ac.at