Geogr. Helv., 71, 137–146, 2016
www.geogr-helv.net/71/137/2016/
doi:10.5194/gh-71-137-2016

+ GEOGRAPHICA HELVETICA + supported by sc|nat

Assemblage of the vertical: commercial drones and algorithmic life

Jeremy W. Crampton

Department of Geography, University of Kentucky, Lexington, KY 40506, USA

Correspondence to: Jeremy W. Crampton (jcrampton@uky.edu)

Received: 11 November 2015 – Revised: 28 May 2016 – Accepted: 30 May 2016 – Published: 20 June 2016

Abstract. This paper takes up the increasingly popular topic of drones – including unmanned aerial vehicles (UAVs), small unmanned aerial systems (sUAS), remotely piloted aircraft (RPA), and a vast panoply of commercial drones and copters – to argue that our analysis should lie not so much on drones as objects, but as assemblages of the vertical. Drones, I argue, constitute a socio-technical assemblage of the sky and vertical space, which means that our focus should be not (only) on their technological development and capacities but also on their effects and affects. The latter of these include increasing algorithmic data collection and circulation that follow anticipatory logics.

1 Introduction

This paper takes up the increasingly popular topic of drones – including unmanned aerial vehicles (UAVs), small unmanned aerial systems (sUAS), remotely piloted aircraft (RPA), and a vast panoply of commercial drones and copters – to argue that our analysis should lie not so much on drones as technological objects, but as assemblages of the vertical. Drones, I argue, constitute a socio-technical assemblage of the sky and vertical space, which means that our focus should be not (only) on their technological development and capacities (important as that is) but (also) on their effects and affects. In this way we can begin to conceptualize the political life of objects. By framing the enquiry in this way I am able to draw on the research agenda outlined by Klauser and Pedrozo (2015), who identify three major research objectives: the making of drones (in this paper the drone market and its attendant experts and knowledges); the functioning of drones (here their colonization of the vertical); and the implications of drones (here their place in an overall assemblage of algorithmic governance).

The paper is divided into two main sections. Following a brief elaboration and explanation of the main argument introduced above, I posit that the vertical is undergoing an enclosure and colonialization through the formation of a drone market. This market is constantly being brought into formation, or performed and re-formed by actors, institutions, commercial interests, and various knowledges by seeking to surmount obstacles and tensions in its formation. Second, I examine the implications of the drone assemblage for the ways in which it contributes to our increasingly algorithmic life. Here we get further from drones as technological objects, and closer to what they achieve – new forms of subjectivity and governance, or what can be called "algorithmic governance" after the Governing Algorithms conference (Musiani, 2013). Following Gillespie, I take a broad view of algorithms as "encoded procedures for transforming input data into a desired output, based on specified calculations" (Gillespie, 2014, p. 167). I conclude with a brief examination of the vulnerabilities of drones, in particular hacking global positioning system (GPS) and position, navigation, and timing (PNT) capabilities.

My deployment of the concept of the drone assemblage draws from Deleuze and Guattari (1983, 1987) on assemblage theory and the work of Foucault (2007) on governmentality. Assemblage allows us to see that previously "discrete surveillance systems [are converging] to the point that we can speak of an emerging 'surveillant assemblage'" (Haggerty and Ericson, 2000, p. 606). Their key point was that surveillant assemblages abstract (Latin: *abstractus*, to draw away) the data produced by an individual from that individual and place it into circulation. Once in circulation these "data dou-

bles" could be sold, and passed forward as variables for the creation of profiles. As Leszczynski has put it:

> Our movements, behaviors, and actions in, through, and across space are easily and seamlessly digitally generated, captured, registered, leaked, intercepted, transmitted, disclosed, dis/assembled across data streams, and repurposed by ourselves and others. Our personal spatial data flows freely and without friction across and between interoperable and synergistic geo-enabled devices, platforms, services, applications, and analytics engines (Leszczynski, 2016).

Haggerty and Ericson help us to think through what work is done in the world by our objects of analysis, to understand them in terms of a socio-technological "apparatus" rather than merely a technical one, and to apprise them as continuously forming (indeed performing), rather than remaining static. Though it is more than surveillance that is at stake with drones, rather surveillance, the drone market, and form of governance constitute an assemblage.

Although the rich work of Deleuze and Guattari resists summation, for our purposes we can use their well-known definition of assemblage as "a multiplicity which is made up of many heterogeneous terms and which establishes liaisons, relations between them... [i]t is never filiations which are important but alliances, alloys" (Deleuze and Parnet, 1987, p. 69). In other words, how do a wide variety of actors, institutions, and knowledges form and reform, and what work do they do in the world? The components of an assemblage such as that of the commercial drone have been brought together deliberately and always benefits someone or something outside the assemblage. In one important, perhaps critical sense then, the drone is an idea – one that is actively desired to come into being (Buchanan, 2015). What is this idea; which is to say, what affects does it have?

To address this question, I highlight two aspects of the drone assemblage. First, they serve to control and modulate, not by exercising an all-powerful sovereignty, but through a marshalling of people's behaviors and possible future behaviors, or what Foucault called "conduct of conduct" by which people are led, but not compelled (Foucault, 1983, 2007). Second, and not unrelated, drone assemblages are deployed to reduce and contain threat. Although this might be most obvious in the case of military or intelligence drones, my interests lie with commercial or non-military drones. Here too we may discern threat reduction although it takes different forms, including the reduction of risk to capital flows by decreasing uncertainty in the market. By creating certain kinds of vertical space (for example financial risk of investment in the new technology) risk is ameliorated. Both these effects are discussed in turn.

2 Enclosure of the vertical

As a number of authors have discussed, unmanned aircraft have been around in various guises for about a 100 years (Shaw, 2013). However, the market for drones beyond the military is a more recent innovation. In this section I trace the broad contours of this market and look at the key players constituting it. My main argument is that the market is being created on an ongoing basis, which we can call performing markets (MacKenzie and Millo, 2003; Callon, 1998). This does not reference how well markets are doing (under- or over-performing) but rather that markets need to be continually created through the actions and relationships of various material and non-material actors. Although I draw from earlier work on performing markets, in partial distinction to this literature, I argue that it is not so much the actors in elite positions (such as consulting economists and policy-makers) that perform markets, but rather a set of interconnected players that can take both a material and discursive form, who exist at a variety of scales, and at a variety of positions.

This commercial drone assemblage is constituted not only by drones themselves as technical objects, but also in the US (my primary focus) by state and federal regulations (e.g., the Federal Aviation Administration or FAA), specific knowledges, drone manufacturers, regional Chambers of Commerce, members of the public, universities, the Defense Advanced Research Project Agency (DARPA), drone interest groups, farmers, police, drone start-up companies, and lobbyists. The target of the drone market is not only the production of commercial drones, but regional development of the sky itself.

At the moment the main sources of risk derive from uncertainty about the legal, technical, and social implications of investing in the commercial drone market. Federal regulators such as the FAA in the USA have been charged with clarifying commercial drone usage (i.e., loosening restrictions) but this has put them in conflict with their core mission to preserve safety. Overall the FAA has reacted too slowly according to congressional testimony by Google and Facebook (both of which have ongoing drone programs). Amazon, which has received public attention for its proposal to deliver packages, is also lobbying Congress for increased access to the sky, doubling its lobbying spending to USD 9.4 million in 2015 (King, 2016).

Technologically there are also challenges but these seem more certain of being solved (both DARPA and NASA have announced early success in enabling drones to autonomously avoid obstacles, drawing on research in ground-based self-driving vehicles).

The size of the commercial drone market cannot be precisely determined, in part due to its rapidly changing form. Some proxy measures are provided by various players such as the lobbyist group Association of Unmanned Vehicle Systems International (AUVSI), but these are vested interests and cannot be taken as impartial; nevertheless, they are in-

dicative of what people expect or hope the market to be. AUVSI's economic analysis (Jenkins and Vasigh, 2013) states that more than 70 000 jobs will be created in the USA, with an economic impact of USD 13.6 billion. A recent overview of commercial drone market's size found estimates ranging from USD 125 million to USD 5.1 billion by 2019, indicating the still-emerging nature of the market (Oppenheimer & Co., 2016). By comparison, the US military UAV budget is only USD 3.95 billion for financial year (FY) 2017 (Gettinger, 2016). The FAA's drone registration program has been so successful that there are already more registered drone operators (325 000) than manned aircraft (Associated Press, 2016).

AUVSI's claim is an example of how various components of the drone market are performing the market – in this case framing the expectations, which leads to pressure on the FAA to adjust its policies to enable the creation of these jobs, for companies to enter the market in expectation of realizing returns, of chambers of commerce to seek regional investment, and so on.

This performativity of the drone market is reflective of what Anderson has called "anticipatory action" whereby preemption, preparation, and prevention of threats to neoliberal life are enacted in anticipation of future conditions and geographies (Anderson, 2010). In this case AUVSI anticipates a vast future economic market that would extend neoliberal capital into a new regional development of the sky, but it is one that will not come about unless various blockages and threats are identified and removed. AUVSI's ultimate intent in issuing the economic forecast is not so much to estimate market size, as to preempt obstacles to it.

Non-military drone operation in the USA occurs in one of two categories: public and civil (including commercial). In the former, which includes federal, state, and local government including law enforcement and universities, the FAA will provide airspace authorization through Public Certificates of Waiver of Authorization (COA). According to the FAA, the review process for a COA is about 60–90 days. In the latter, the FAA issues a civil COA for airspace permission and certifies the equipment used through a so-called Section 333 exemption. The latter takes about 120 days for the approval process, and derives from Section 333 of the 2012 FMRA. This section grants authority to the Department of Transportation (including the FAA) to issue exemptions on a case by case basis. Since the first exemption in September 2014 through to May 2016, more than 5000 exemptions have been issued, with a further 17 000 in the queue. (These may cover multiple uses and units.)

Interestingly, 333 exemptions were initially highly constrained geographically because the applicant also had to apply for a COA in a specific airspace. In March 2015, the FAA allowed drone operators to fly in any permitted geographic airspace. This has encouraged a lot of start-up companies, who are taking a drone for hire business model, i.e., a new form of business not permitted under the original regulations.

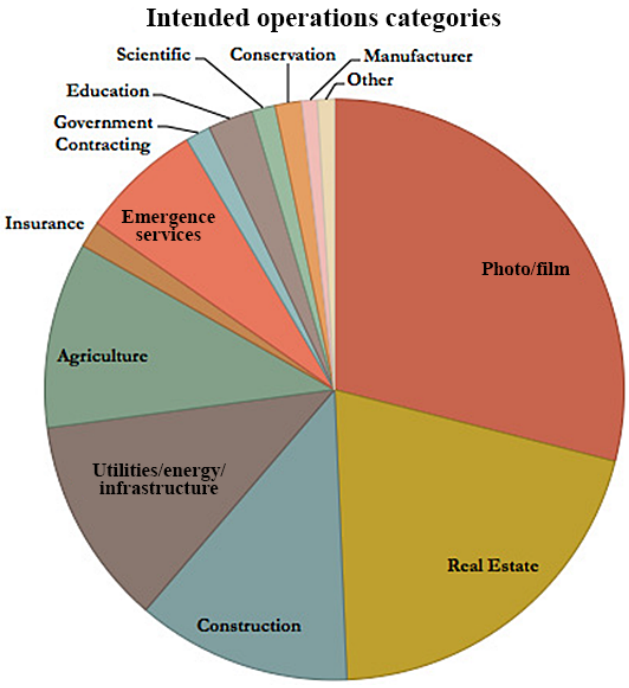

Figure 1. Intended primary operations categories of small drones in the USA. Source: Michel and Gettinger (2016).

What do drones do? Commercial drones are flown for a variety of purposes. According to the Center for Study of the Drone, which has tabulated 2733 Section 333 exemptions through the end of 2015, the most common intended usage of small drones was for photo/film purposes (29 %), followed by real estate (18.2 %). See Fig. 1.

The survey noted, however, that applicants intended to use their drones for multiple purposes (on average about two purposes per exemption). Thus, an applicant may state that the intended purpose is to collect aerial footage for monitoring utility infrastructure. This appears to be a way that the FAA can loosen its requirements because one application can now cover different drones and different uses. Additionally, the one big increase in intended use is emergency services, which grew from 3 to 19 % from the start to the end of the survey period. Because these exemptions do not include civil uses provided by law enforcement agencies (LEAs) it is interesting to note that these companies anticipate their drones being hired for security and emergency services. Indeed, currently, fewer than 50 police departments operate drones (US Congressional Research Service, 2016).

A second area of tension lies between federal and state regulations. Some states have attempted to pass their own UAS regulations either permitting or more frequently banning drones from certain activities such as flying close to properties in order to protect privacy. However, the FAA continues to assert that it possesses exclusive sovereignty of airspace and that it can preempt local and state requirements.

A third area of concern for the drone market lobbyists is how drones are perceived and understood, or what might be called the affective politics of drones. This has two elements – negating concerns that commercial drones are a threat to well-being (primarily issues of privacy and safety), and controlling the narrative (e.g., in the media or legislatures) by promoting their beneficial potential. Drone registration addresses the first of these by requiring an identifying mark on each drone, to enable monitoring and enforcement of UAS regulations. Similarly, geofencing technologies are increasingly written into control software to disable drone operations in specific spaces (say within 5 miles of an airport) and are now used by drone companies as a competitive advantage for safety. For example, DJI touts its geofencing, known as Geospatial Environment Online (GEO), as the best-in-class geospatial information system that provides drone operators with information that will help them make smart decisions about where and when to fly. It combines up-to-date airspace information, and a warning and flight-restriction system (DJI, 2015).

According to the Congressional Research Service (CRS) a whole raft of other technologies for detecting drones in flight and even destroying them are in development (US Congressional Research Service, 2016). But as a source in government told us "ultimately, even once the FAA makes its decisions, the shape and size of this industry is going to be determined by the insurers" (interview, November 2014).

Industry stakeholders have expressed frustration at the delays, and have pushed back against privacy concerns. In an interview, the Director of UAVSI, Michael Toscano, stated that drones did not represent a new threat to privacy: "It does not make a difference how you collect [information]. ... I do not think privacy is really the issue. ... The issue is safety" (Toscano Interview, November 2014).[1] In this way, Toscano seeks to shift the debate from a contentious policy issue (privacy) to a solvable technical issue.

Industry has also proposed safety solutions. Amazon's drone program, known as Prime Air, has proposed a new subdivision of the sky to allow for small UAS operations. In their scheme, heights between ground level and 200 ft would be dedicated to hobbyist flying drones and kites, heights between 200 and 400 ft would be a dedicated "drone lane" to be used by small fast UAS, the zone between 400 and 500 ft will be a no-fly zone, and heights above 500 ft would be reserved for other aircraft as is the current case (Amazon Prime Air, 2015). However, the FAA has so far taken a dim view of this proposal, stating this is "segmentation" rather than "integration" of airspace (US Federal Aviation Administration, 2015).

Google announced in late 2015 that they expect to start drone deliveries by 2017. David Vos, who runs Project Wing, was quoted in the media as stating that "we are pretty much on a campaign here", and that they would like to see a new class of airspace, Class G, created especially for drones (Morgan, 2015), similar to the Amazon proposal. To this end, one of the six FAA test sites includes a component in Iceland, where approvals can be obtained in as few as 10 days (US Congressional Research Service, 2015). According to *Forbes*, Amazon is also scanning private properties in high resolution, which may indicate it is developing its automated sense-and-avoid capabilities (Mac, 2015). The FAA has also responded to industry pressure to accommodate its line-of-sight restriction by announcing a new program, known as the Pathfinder Program, which would work with companies on a test basis to develop beyond line-of-sight capabilities (McFarland, 2015). But the proposal of a new class of airspace has not been received favorably by the FAA, which sees it as an infringement on its core mission, and is waiting for new technologies that can track and manage drones flying below 500 ft. For example, NASA is developing a low-altitude UAS traffic management (UTM) system, which it will turn over to the FAA in 2019 (Carey, 2016).

There is also pressure from competition abroad. Many countries around the globe have programs and processes that allow far more UAS activity than in the USA. Japan, for example, has permitted UAS use in agriculture since the 1980s. In Europe, the European Aviation Safety Agency (EASA) has sought regulations for UASs that would integrate them into national airspace by forming three categories of use (open, specific, and certified). The latter category would allow beyond line-of-sight operations (US Government Accountability Office, 2015). By contrast, the USA has announced further regulation, requiring that some publicly available drones be registered to their owners (Associated Press, 2015). As a source in the US government explained: "you are seeing already the emergence of significant markets for small commercial UAVs overseas... but until there is a market for it [in the US], no one can move out of their garage" (Interview, November 2014).

All of these developments raise the question of what is happening to the vertical. It has been long established that the sky is public – otherwise each airplane would have to get permission to fly over your property.[2] This is akin to the concept of international waters on the ocean. But as with international waters, this public space is becoming increasingly and deliberately enclosed, in what might constitute a modern "enclosure of the commons". (China, for example, has recently built on low-lying islands in the Spratly Islands in the South China Sea, and claimed not just sovereignty over the seas,

[1] Interviews cited in this paper were carried out by the author and Dr. Susan Roberts, University of Kentucky.

[2] See *US v. Causby* 1946 (328 U.S. 256), which held that the doctrine of ad coelom (that is, property rights up to the sky) was not relevant to the modern world, and that airspace above a certain minimum was the public domain. On the other hand, property owners have some air rights in connection with their property, although they cannot dictate what flies there since that is the sovereign right of the USA (i.e., the FAA).

but over the airspace as well.) As Don Mitchell has argued, when space is taken from the public domain and privatized (enclosed):

> The threat here is not from the disorderly behaviors... but rather from the steady erosion of the ideal of the public, of the collective, and the steady promotion of private, rather than democratic, control of space (Mitchell, 2004, p. 137).

How is this occurring in the drone context? Is it possible to privatize the sky and effectively overturn *US v. Causby*? It is already happening incrementally. Some companies have sought and received special FAA dispensations to control airspace over their businesses. Airspace over Disney theme parks for example is restricted up to 3000 ft, with the FAA categorizing this zone as national defense airspace. Some private entities (such as ski resorts) have also banned drones (US Congressional Research Service, 2016). This raises the very issue, however, of their legal right to do so, given that the FAA controls all airspace (especially if the operator is outside the property). Similarly, activist groups sometimes fly drones over mountaintop removal (MTR) mining sites, although this (and indeed government overflights) is strongly objected to by the coal industry. There are also numerous FAA restrictions, known as NOTAMs (notices to airmen), such as one restricting drones from flying within 15 mi of Washington D.C. Reagan National Airport, 3 times the usual distance.

Not all airspace privatization occurs because of drones. The proliferation of POPS or privately owned public spaces (including malls but also many parks, buildings, and riverfronts) and the UK's recent introduction of PSPOs (public space protection orders) are steadily eating away at public access through privatization. (PSPOs are similar to ASBOs or antisocial behavior orders, and criminalize activity in public space that is not normally a crime.) According to one author, PSPOs act as "spatial control orders... making predefined activities within a mapped area prosecutable" (Garrett, 2015). As authorities seek to further conduct behaviors in nominally public spaces, drones can provide an additional form of surveillance for areas not already covered by CCTV, or where a mobile aerial viewpoint is needed. Although PSPOs are horizontal, ground level spaces, there is also a vertical dimension. Air rights – the space immediately above a property – can be sold separately from the building itself, and although these do not extend indefinitely into the sky, it is nevertheless a "hot market," with its own brokers and traders. In some places, the price can be as high as USD 230 per square foot of air (Hershipps, 2013).

Drone assemblages and the marketplace are thus actively performed by various interested actors in very material and discursive ways. I argue that the drone market will continue to develop by extending this control and enclosure of the vertical (i.e., through increasing privatization and monetization of the sky). In the next section, I offer some reflections on the effects of this market in terms of governance.

3 Algorithmic governance

In this paper, algorithmic governance refers to the manifold ways that algorithms and code/space enable practices of governance by conducting and mediating behavior. I am particularly interested in the manner this occurs in geographic contexts. I therefore broaden my view of the drone assemblage to see it as only part of a set of developments that I call "algorithmic governance". Here we get furthest from drones as objects but closest to what effects they achieve through the creation of new forms of subjectivity. These new subjectivities have the purpose of identifying and containing threat, through various mechanisms of control, and have geographical outcomes. I take an expansive view of threat, to include, like Anderson (2010), threats to profitable neoliberal activities.

What is algorithmic governance? As stated above, an algorithm is any form of calculation that takes input and yields desired output. They are increasingly essential because of the vast amounts of data being produced – big data – that outpace human computational capacities. The output I am concerned with is modulated (affected) conduct, or what Foucault calls the "conduct of conduct". Thus an algorithm is data plus calculation is equal to conduct of conduct. Algorithmic governance is therefore the increasing prevalence of algorithmically derived decisions made on the basis of personally identifiable information (PII), data profiles that may or may not say something meaningful about your life, but act to form spaces of possibility, whether you are aware of them or not. For example, algorithms may impact your chances of employment (or keeping employment), getting credit and education, health services, travel, and basic control over online information about you (Pasquale, 2015).

For what reasons are behavior, attitudes, and beliefs affected (conducted)? For Amoore (2014), the various assemblages of big data, everywhere sensors, and algorithms "are less interested in who a suspect might be than in what a future suspect may become" (Amoore, 2014, p. 109). Algorithms are therefore directed at producing certain *kinds* of subjects (the proto-suspect) in order to reduce, allay or redirect risk. Nguyen for example, provides a case study of how algorithmic biometrics in US schools modulate spatial behavior. The biometric devices "not only verify identity; they also shape how, where, and for what purposes authorized school bodies can move" (Nguyen, 2015, p. 2).

In the drone context the most obvious example (beyond the military) is the use of drones for policing. Indeed, Neocleous goes so far as to argue that air power *is* police power (Neocleous, 2013). For example, Aeryon Labs, a Canadian manufacturer of small drones has partnered with Microsoft to produce real-time aerial imagery for police and intelli-

gence surveillance. Known as the Microsoft Advanced Patrol Platform (MAPP) the system is aimed at police departments around the country, and "law enforcement and security personnel" (Microsoft, 2015). Similarly, Nigeria just announced the use of drones to supplement the 1000 CCTVs (closed circuit TVs) it has in place across the city of Lagos, as part of a crime prevention initiative (Akinola, 2015). Some US states have also passed laws allowing drones to be equipped with tasers and other "non-lethal" weaponry (della Cava, 2015). But perhaps the most notable usage has been by the US Customs and Border Patrol (CBP), which has flown unarmed drones (Predator B) since 2004, and currently operates 10 drones. According to a government report, however, this program has yet to prove its value, and recommended that CBP cancel its plans to spend USD 443 million on 14 additional drones (US Department of Homeland Security, 2015). Although the CBP agreed officially with the report, they were later quoted in the media as strongly disagreeing. The CBP assistant commissioner in charge of acquisitions, Mark Borkowski, stated "there are a zillion things" drones can do, and that the value of the drugs they had interdicted outweighed the cost of the program (Ortega, 2015).

What is important to note here is that this affect is operating on data. Amoore (2014) calls these the "data derivatives" and they are increasingly uncoupled from underlying values associated with a living person. As several authors have noted, such derivatives were postulated during the 1980s by Deleuze, who proposed the concept of the "dividual" (Deleuze, 1992).

It is worth pausing to explicate this notion of the dividual. If for Foucault the period of modernism up to the early twentieth century was marked by the so-called disciplinary societies, then Deleuze argues that the current moment is better understood as societies of control. Discipline has too heavy a hand, as Foucault himself recognized through his own discussion of governmentality as management and conduct of conduct. With societies of control it is more a matter of modulating, of continually adapting and affecting, than enclosing people in institutions such as prisons (Foucault, 1977). Deleuze observes "The disciplinary societies have two poles: the signature that designates the *individual*, and the number or administrative numeration that indicates his or her position within a *mass*" (Deleuze, 1992, p. 5). This is a very interesting observation because it comports with a recent history of data that identified three time periods: the nineteenth century, the period up to WWII, and the period since about the late 1970s to the present (Bouk, 2016). During the nineteenth century the focus was on collecting personal data in order to fit them into biopolitical populations – this was after all the century of the Census, and the Census atlas (Hannah, 2000). During the next period, starting from the first couple of decades of the twentieth century, personal data collection is marked by a practice of mass production, mass consumption, mass marketing, etc., or in other words a proliferation of massification (in pursuit, no doubt, of mass profit, though Bouk does not say this directly). The primary purpose here was to fit the individual into the mass, through for example, sorting and prediction achieved by ever-more metrics in testing. In education alone we could cite in the USA the Educational Testing Service (ETS), GRE scores to get into graduate school, the h-index for individuals, journal impact factors, and a whole array of student performance metrics. In the current moment, which Bouk dates from the 1970s (or about the time that productivity increases come adrift from wage increases, linked to the increasing computerization and robotization of the work place), the rise of the "data double" takes place. Analogous to Amoore's data derivatives and coined by Haggerty and Ericson (2000), the data double feeds big data and the internet of things (IoT). The data abstracted from individuals becomes commoditized, and not surprisingly has a metric, the ARPU or average revenue per user. For a company such as Facebook, the ARPU can be as high as USD 9.30 in North America, and over USD 2 globally. One of the controversies over social media is that none of this revenue is currently returned to Facebook's 1.5 billion users.

In addition to monetization, however, data doubles and big data lead to policy outcomes – what some have called computational politics. This is not a new dream of course, as the post-war work by scientists such as John von Neumann on "cybernetics" evidences (etymologically, *cyber* means control or governance). As long ago as the early 1970s for example, Allende's Chile was the site of a radical experiment in governing the economy of a nation through a central control room, in project CyberSyn (Medina, 2011). Data doubles in our era could thus be understood in political economic terms.

Deleuze's dividual is neither an individual (especially not a unitary self) nor an aggregate. Instead, the dividual is made up, perhaps even assembled, of strands that keep coming together and apart, and can divided and redivided (Delueze also calls this the nomadic subject, rather than the traditional monadic subject). A consequence of this is that data doubles can circulate around in many ways not necessarily following predetermined paths, a question of networks rather than centers, of relays. Deleuze's relays, I suggest, should not be thought of simply as automatically passing forward the information. Rather, he importantly notes that "what is important is no longer either a signature or a number, but a code: the code is a *password*" (p. 5). Later he adds

> Felix Guattari has imagined a city where one would be able to leave one's apartment, one's street, one's neighborhood, thanks to one's (dividual) electronic card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position – licit or illicit – and effects a universal modulation (Deleuze, 1992, p. 7).

Here Deleuze speaks to how our movement and behaviors are modulated (i.e., not disciplined, but affected) by codes and passwords. But how would this work with drones? Would we be aware that it is happening?

Drones have the capacity to extend the surveillant state further into what has been called code/space (Kitchin and Dodge, 2011). These are capacities that can digitally surveill, and include biometrics, automatic facial recognition, and location tracking. The media has already reported that planes with cameras were flown over the Ferguson and Baltimore protests in the USA, and that police departments have access to a database of over 2 billion scans of vehicle license plate records with locations (Jouvenal, 2016) collected via ANPR (automated number plate recognition). These help locate, identify, and assess potential suspects, which, coupled with other technology that ingests social media postings and other public data, creates an actionable threat score. Drones are likely to add to this monitoring, especially as the Supreme Court has held that warrants are not required for aerial observation in public airspace (see *Florida v. Riley*, 488 US 445 (1989)).[3] Drones would be most useful to police as cheaper alternatives to mobile or temporary events, such as marathons, or to monitor temporarily regulated spaces such as PSPOs in the UK.

Depending on the legislative landscape, police may also be able to deploy automated facial recognition technologies with drones. This capability already exists. In 2011 biometrics company Progeny Systems Corporation won a contract from the US Army for drone-based automated facial recognition, and is only one of several companies working on this issue. An advantage to this form of surveillance is that a drone could autonomously decide, depending on its algorithmic programming, to track an individual through public spaces. Similar to the advent of predictive policing one need not be aware of this monitoring, nor have given consent. For example, in Illinois the Biometric Information Privacy Act, passed in 2008 prohibits the collection of biometric information without prior consent (including retina scans, face geometry, voiceprint, and fingerprints). Under its terms, class-action lawsuits have been filed against Google, Snapchat, and Facebook. It is apparent that drone-based tracking based on facial geometries would be regulated by such a law, and so the police dream of flying drones above crowds for purposes of recognition would be problematized. In 2016, Illinois legislators proposed amendments to the law that would severely curtail its remit, and which would doubtless allow drone-based biometric identification (Brandon, 2016).

Current advances in technology allow faces to be detected at an angle even when partially occluded, and can be used to train neural networks (Farfade et al., 2015). One Australian company, Imagus, claims to reliably detect and identify facial images in non-cooperative environments (e.g., in low light, face partially obscured, or without the subject's permission). This need not be limited to subject *identification* (matching a face to an identity). For example, Imagus offer a facial *matching* service, whereby a subject is tracked as they go from one point to another, such as at an airport terminal. The marketing industry has started contemplating how to use automated facial recognition for delivery of advertising. While current geofencing-based advertising is susceptible to being circumvented (e.g., turning off location in your mobile device), you cannot "turn off [your] face" as one marketer put it (Warnock, 2015).

4 Drone vulnerability?

Throughout the development of drones and especially their proliferation into domestic airspace there have been attendant anxieties over their failure, misuse, or dangers. In this last section, I wish to discuss some of the many vulnerabilities of drones. As the vertical is colonized therefore it is recognized that it is yet another domain where risks proliferate.

Technologically, the fact that many drones rely on Global Navigation Satellite Systems (GNSS), such as the US GPS, the Russian GLONASS (Globalnaya Navigazionnaya Sputnikovaya Sistema, or Global Navigation Satellite System) or European Galileo system is an exploitable vulnerability. This was brought starkly to light after the capture in 2011 of an American RQ-170 "Sentinel" UAV by Iran, when concern was raised about GPS/GNSS spoofing attacks. (Whether the RQ-170 was spoofed by GPS is uncertain, but such attacks are feasible because civil GPS signals are relatively weak and unencrypted.) GPS are also problematic because signals cannot travel underwater (and therefore cannot be used for amphibious UAVs) nor pass through buildings, urban canyons or underground. GPS spoofing has been demonstrated to work in several settings. In testimony before Congress, an engineering professor noted that he had successfully spoofed GPS in both the laboratory and in the field at White Sands Missile Test Range (Kerns et al., 2014; Humphreys, 2015). In 2015, at DEFCON 23, the annual hacker convention, two Chinese researchers demonstrated an inexpensive build your own GPS spoofer to trick a popular model of consumer drone (a DJI Phantom) to override its geofencing so that it would operate in a no-fly zone or appear to be in Tibet (Huang and Yang, 2015).

In that light, DARPA initiated a research project in 2015 to find alternatives to GPS. While this may involve solutions that improve inertial guidance, or distance measurement, DARPA is especially interested in alternative sources to GPS, such as from "television, radio and cell towers, satellites, as well as natural phenomena such as lightening" (DARPA, 2015). DARPA's program to develop an alternative to GPS, known as Spatial, Temporal, and Orientation Information in Contested Environments (STOIC), made its first awards

[3] However, note that this ruling only applied to naked eye observation. Additionally, many state legislatures are crafting drone-related legislation that would require warrants (McNeal, 2016).

to military contractors in 2015 (Raytheon BBN Technologies, Expedition Technology and Rockwell Collins). However, these technologies are still several years away, especially for commercial or civil drones.

The other major technological challenge lies in automatic sense-and-avoid (SAA) and line-of-sight requirements established by the FAA. The first of these requires the development of technical capability for drones to perform semi-autonomously when faced with physical obstacles (buildings, birds, and other aircraft including drones). For example, a drone can be programmed to follow a specific route from location to location, but like a self-driving car, would need to be able to detect (sense) intervening obstacles that may occur and successfully avoid them. (DARPA announced some early successes of SAA in early 2016.) Line of sight refers to the FAA requirement that (currently) all UASs must be kept in direct visual line of sight of a qualified operator (i.e., without using First Person Viewpoint (FPV) or sighting aids such as binoculars). Other prescriptions include no-fly zones within 5 miles of an airport or helipad, that drones weigh no more than 55 lbs., and that they not fly at night or over stadiums during games (the latter is covered by what the FAA calls a Temporary Flight Restriction, TFR).

5 Conclusions

In this paper I have introduced and analyzed the emerging market for commercial drones. I have done so by understanding drones not just as a technology, but as a socio-technological assemblage. By this I do not mean to diminish the real material constituents of drones, such as their physical capacities (surveillance, package delivery, or real estate inspection) and technological weaknesses (sense-and-avoid). In fact, these remain key areas for further research as they are doubtlessly tied to legal, political, and social mediation of commercial drones. The advantage of understanding drones as assemblage, however, is that we can begin to conceptualize the political life of objects. In conclusion therefore, I identify three areas where research can contribute to our understanding of commercially and civically available drones; their role in *biometric identification*, their *affective politics*, and the *datafication of subjectivities*.

Although perhaps an unfamiliar research domain for social scientists and geographers, drone-based mobile automated facial detection, recognition, and tracking are likely to have profound effects on people's sense of place and navigational possibilities. In particular, I would underline the arguments made by Virginia Eubanks that digital technologies are a domain of social justice, and that the future of surveillance is often discernible first among poor communities (Eubanks, 2014). As Klauser and Pedrozo (2015) pointed out, commercial drone usage "is sporadic and punctual rather than well-ordered and sequential or systematic" (p. 287) and it may be that we have to adapt our notion of surveillance as panoptic to something more geographically specific.

In that context, it is important to be attentive to the ways these algorithms operate. According to recent studies, algorithmic biometrics exhibit demonstrable racial bias (Angwin et al., 2016; Klare et al., 2012). In one case, an algorithm in use in police departments in multiple US states failed twice as often with African American subjects as with Caucasian subjects (Klare et al., 2012). Facial detection, tracking and recognition is fast becoming a significant factor in security discourses. One recent study for example sought to identify the most typical types of faces in different geographical areas (Islam et al., 2015). It would be important to further study how drone-enabled facial recognition could then identify individuals who were "out of place" in certain situations. In general, there has been little work on the effects of facial recognition, and its likely deployment from drones.

Second, much more work is needed on what might be called the affective politics of drones. To date, only one (controversially received) study has been performed on what feelings are identifiable from "living under drones" (International Human Rights and Conflict Resolution Center and Global Justice Clinic, 2012). Do drones alter one's sense of self, especially around privacy? In what ways? There is a critical need to understand the specific ways algorithms and other forms of code – such as smart cities/technologies, the IoT and machine-based learning – have so successfully arisen to challenge, supplement, and, at times, replace human decision-making. What are the ethics of transferring so much decision-making to machines that used to be carried out by humans? What are the affective politics of the proliferation of metrics in neoliberal government, and considering their vulnerabilities how does the "fickle affectivity of statist encounters" play out with regards to drones (Woodward, 2014, p. 23)?

The datafication of subjectivities, for example what John Cheney-Lippold (2011) calls the "soft biopolitics" of algorithmic citizenship, is no doubt a prime target of value extraction. This value may be economic and we do need further studies of the drone market, who is contributing to it, and how particular ways of valuation are arising. But we also see an investment in what Shaw and Akhter (2014) calls "algorithmic technics" of constant capital (batons, body cameras, police dogs, facial recognition, drones) and a disinvestment in variable capital (the human). Further work on the drone market and the forms of subjectivity it is instituting is critically important here.

Acknowledgements. I would like to thank the editor, Benedikt Korf, and two anonymous reviewers. Thanks also to Francisco Klauser and Silvana Pedrozo for inviting me to the conference "Power and Space in the Drone Age" at the University of Neuchâtel, where a version of this paper was first presented.

Edited by: B. Korf
Reviewed by: two anonymous referees

References

Akinola, F.: Lagos to Deploy Drones to Combat Crime, The Daily Trust, 26 October 2015.
Amazon Prime Air: Revising the Airspace Model for the Safe Integration of Small Unmanned Aircraft Systems, 2015.
Amoore, L.: Security and the Claim to Privacy, International Political Sociology, 8, 108–112, 2014.
Anderson, B.: Preemption, precaution, preparedness: Anticipatory action and future geographies, Prog. Hum. Geog., 34, 777–798, 2010.
Angwin, J., Larson, J., Mattu, S., and Kirchner, L.: Machine Bias, ProPublica, 23 May 2016.
Associated Press: US to require drone registration amid wide-ranging safety concerns, The Guardian, 19 October 2015.
Associated Press: FAA: More Registered Drone Operators than Registered Planes, The Washington Post, 8 February 2016.
Bouk, D. B.: The History and Political Economy of Personal Data over the Last Two Centuries in Three Acts, Osiris, in press, 2016.
Brandon, R.: Someone's Trying to Gut America's Strongest Biometric Privacy Law, The Verge, 27 May 2016.
Buchanan, I.: Assemblage Theory and its Discontents, Deleuze Studies, 9, 382–392, 2015.
Callon, M.: The laws of the markets, Oxford, Malden, MA, Blackwell Publishers/Sociological Review, 1998.
Carey, B.: For Now, FAA is Not Considering Airspace Changes for Drones, AINonline, 3 May 2016.
Cheney-Lippold, J.: A New Algorithmic Identity, Soft Biopolitics and the modulation of Control, Theor. Cult. Soc., 28, 164–181, 2011.
Defense Advanced Research Projects Agency (DARPA): Breakthrough Technologies for National Security, Washington, DC, DARPA, 2015.
Deleuze, G.: Postscript on the Societies of Control, October 59 (Winter), 3–7, 1992.
Deleuze, G. and Guattari, F.: Anti-Oedipus : capitalism and schizophrenia, Minneapolis, University of Minnesota Press, 1983.
Deleuze, G. and Guattari, F.: A Thousand Plateaus. Capitalism and Schizophrenia, Minneapolis & London, University of Minnesota Press, 1987.
Deleuze, G. and Parnet, C.: Dialogues, New York, Columbia University Press, 1987.
della Cava, M.: Police Taser Drones Authorized in ND, USAToday, 29 August 2015.
DJI: DJI Introduces New Geofencing System for Its Drones, San Jose, CA, DJI, 2015.
Eubanks, V.: Want to Predict the Future of Surveillance? Ask Poor Communities, The American Prospect, 15 January 2014.
Farfade, S. S., Saberian, M., and Li, L.-J.: Multi-view Face Detection Using Deep Convolutional Neural Networks, Proceedings of the 5th ACM on International Conference on Multimedia Retrieval, 640–650, 2015.
Foucault, M.: Discipline and punish: the birth of the prison, 1st American ed., New York, Pantheon Books, 1977.
Foucault, M.: The Subject and Power, in: Michel Foucault: Beyond Structuralism and Hermeneutics, edited by: Dreyfus, H. L. and Rabinow, P., 208–226, Chicago, The University of Chicago Press, 1983.
Foucault, M.: Security, Territory, and Population. Lectures at the Collège de France, Houndsmills, Basingstoke and New York City, Palgrave Macmillan, 2007.
Garrett, B. L.: PSPOs: The New Control Orders Threatening our Public Spaces, The Guardian, 8 September 2015.
Gettinger, D.: Drone Spending in the Fiscal Year 2017 Defense Budget. Annandale-on-Hudson, New York, Center For the Study of the Drone, 2016.
Gillespie, T.: The Relevance of Algorithms, in: Media Technologies, edited by: Gillespie, T., Boczkowski, P. J., and Foot, K. A., Cambridge, MA, MIT Press, 2014.
Haggerty, K. D. and Ericson, R. V.: The surveillant assemblage, Brit. J. Sociol., 51, 605–622, 2000.
Hannah, M.: Governmentality and the Mastery of Territory in Nineteenth-Century America, Cambridge, Cambridge University Press, 2000.
Herships, S.: The Air Up There, Marketplace, 2013.
Huang, L. and Yang, Q.: GPS Spoofing. Low-cost GPS Simulator, in: DEF CON 23, Las Vegas, 2015.
Humphreys, T.: Statement on the Security Threat Posed by Unmanned Aerial Systems and Possible Countermeasures, in: Oversight and Management Efficiency Subcommittee, Homeland Security Committee, Washington, DC, US House, 2015.
International Human Rights and Conflict Resolution Center, and Global Justice Clinic: Living Under Drones: Death, Injury, and Trauma to Civilians from US Drone Practices in Pakistan, 2012.
Islam, M. T., Greenwell, C., Souvenir, R., and Jacobs, N.: Large-scale geo-facial image analysis, EURASIP Journal on Image and Video Processing, 2015, 1–17, 2015.
Jenkins, D. and Vasigh, B.: The Economic Impact of Unmanned Aircraft Systems Integration in the United States, Arlington, VA, AUVSI, 2013.
Jouvenal, J.: The New Way Police are Surveilling You: Calculating your Threat "Score", The Washington Post, 10 January 2016.
Kerns, A. J., Shepard, D. P., Bhatti, J. A., and Humphreys, T. E.: Unmanned Aircraft Capture and Control Via GPS Spoofing, J. Field Robot., 31, 617–636, 2014.
King, C.: Amazon Leans on Government in its quest to be a Delivery Powerhouse, The New York Times, 20 March 2016.
Kitchin, R. and Dodge, M.: Code/space software and everyday life, Cambridge, Mass., MIT Press, 2011.
Klare, B. F., Burge, M. J., Klontz, J. C., Vorder Bruegge, R. W., and Jain, A. K.: Face Recognition Performance: Role of Demographic Information, IEEE T. Inf. Foren. Sec., 7, 1789–1801, 2012.
Klauser, F. and Pedrozo, S.: Power and space in the drone age: a literature review and politico-geographical research agenda, Geogr. Helv., 70, 285–293, doi:10.5194/gh-70-285-2015, 2015.
Leszczynski, A.: Forthcoming. Geoprivacy, in: Understanding Spatial Media, edited by: Kitchin, R., Wilson, M., and Lauriault, T., New York, SAGE, in press, 2016.
Mac, R.: Amazon Scanning Backyards In Seattle, Suggesting Drone Delivery In Its Sights, Forbes, 2 July 2015.

MacKenzie, D. and Millo, Y.: Constructing a Market, Performing Theory: The Historical Sociology of a Financial Derivatives Exchange, Am. J. Sociol., 109, 107–145, 2003.
McFarland, M.: FAA Launces Program to Test Drones Outside of Pilot's Line of Sight, The Washington Post, 6 May 2015.
McNeal, G.: Drones and the Future of Aerial Surveillance, George Washington Law Review, forthcoming, 2016.
Medina, E.: Cybernetic revolutionaries : technology and politics in Allende's Chile, Cambridge, Mass., MIT Press, 2011.
Michel, A. H. and Gettinger, D.: Analysis of US Drone Exemptions 2014–2015, 14. Annandale-on-Hudson, Bard College, 2016.
Microsoft: Microsoft at the FBINAA Conference: Introducing MAPP, 30 June 2015, available at: http://www.msgsoc.com/2015Jun30.html, last access: 31 October 2015.
Mitchell, D.: Geography in an Age of Extremes: A Blueprint for a Geography of Justice, Ann. Assoc. Am. Geogr., 94, 764–770, 2004.
Morgan, D.: Google aims to begin drone package deliveries in 2017, Reuters, 3 November 2015.
Musiani, F.: Governance by Algorithms, Internet Policy Review, 2 (3), 2013.
Neocleous, M.: Air power as police power, Environ. Plann. D, 31, 578–593, 2013.
Nguyen, N.: Chokepoint: Regulating US Student Mobility Through Biometrics, Polit. Geogr., 46, 1–10, 2015.
Oppenheimer & Co.: Drone Industry Report, New York City, 2016.
Ortega, B.: Is pricey Border Patrol drone program worth the cost?, The Republic, 21 June 2015.
Pasquale, F.: The black box society : the secret algorithms that control money and information, 2015.
Shaw, I. G. R.: Predator Empire: The Geopolitics of US Drone Warfare, Geopolitics, 18, 536–559, 2013.
Shaw, I. G. R. and Akhter, M.: The Dronification of State Violence, Crit. Asian Stud., 46, 211–234, 2014.
US Congressional Research Service: Domestic Drones and Privacy: A Primer, ed. C. R. Service, Washington, DC, 2015.
US Congressional Research Service: Unmanned Aircraft Operations in Domestic Airspace: US Policy Perspectives and the Regulatory Landscape, Washington, DC, Congressional Research Service, 2016.
US Department of Homeland Security: U.S. Customs and Border Protection's Unmanned Aircraft System Program Does Not Achieve Intended Results or Recognize All Costs of Operations, ed. Office of Inspector General, Washington, DC, 2015.
US Federal Aviation Administration: Unmanned Aircraft Systems (UAS) Frequently Asked Questions, FAA 2015, available at: https://www.faa.gov/uas/faq/#qn3, last access: 18 October 2015.
US Government Accountability Office: Unmanned Aerial Systems, FAA Continues Progress Toward Integration in the National Airspace, ed. GAO, Washington, DC, 2015.
Warnock, J.: How Facial-Recognition Software Will Shape The Future Of Email Marketing, Marketing Land, 8 December 2015.
Woodward, K.: Affect, state theory, and the politics of confusion, Polit. Geogr., 41, 21–31, 2014.