Civilizing Drones: Military Discourses Going Civil?

Sven Braun, Michael Friedewald and Govert Valkenburg

This article presents an account of how a technology being transferred from one area of deployment to another entails that specific discourses travel along. In particular, we show that the development of Unmanned Aircraft Systems (UAS, often referred to as drones) is importantly determined by its military progeny, as the civilian context inherits specific discourses from the military context. Contemporary ideas of privacy and security in drone use can be largely traced back to this original context. We show that concepts and their relative importance primarily depend on the discourses that travel together with the technologies on which the concepts aim to act. There is no technological reason for privacy and security to be implemented the way they are, nor can their implementation be explained merely from socio-political or moral discourses. Instead, material and discursive mechanisms successfully enact and reproduce the dominant military viewpoint.

Keywords: drones, privacy, security

Introduction

Whenever technologies migrate from one context to another, concepts by which people understand and harness those technologies travel with them. While unmanned aircraft systems (UAS) or 'drones' are no longer merely military devices – but now also commercial and even leisure devices – some remnants of their military genesis can be discerned in the discourses that surround them. Looking at a particular class of UAS, we trace back how incumbent conceptions of security, and adjacent notions of safety and privacy, inherit from this military history a tendency to 'externalize' human values from the design of UAS.

Under the umbrella term of UAS, a wide range of airborne devices is captured which, in one way or another, fly without a human pilot on board. Well known are the military devices used by, amongst others, the United States to assassinate alleged terrorists in areas outside its sphere of military control (Syed, 2013). Less prominent is the use of similar devices for mere reconnaissance and espionage purposes. At the same time, unmanned aircraft carrying a payload are increasingly used for civilian purposes such as infrastructure monitoring (Woody, 2014) and crowd control (Heise, 2013) and even for leisure by private persons – for example to take photos and footage of themselves from above. Compared to the much longer history of military uses, leisure and civilian

purposes that do not focus on the aspect of flying have only appeared fairly recently.

The proliferation of UAS applications naturally raises issues of privacy: aerial observation becomes less costly and less risky, and thereby more affordable. We show that privacy is not some abstract value that is either respected or violated by a technology such as UAS. Instead, we consider it as multiple, situated and contingent (Gutwirth, 2002; Finn et al., 2013). What privacy consists of in this particular case is itself defined in the process of developing an operational UAS. In this development, or so we will argue, military narratives have seemed to be able to persist, even though the practice has moved beyond the military context.

We aim to shed new light on the tensions around privacy when pursuing regulation of UAS by looking particularly at the concept of security. Much like privacy, the concept of security in the drone context lacks an *ex ante* definition – for example, as to what is to be secured, and how. Rather, such notions emerge in the many negotiations – which include social, economic, political, technical and cultural aspects – that take place in the process of development. Since UAS have a substantial history of applications in (national) security, particular notions of security and particular configurations of UAS are fundamentally co-produced.

At the same time, transferring UAS – or elements thereof – from military to civilian contexts, will generally modify or *translate* both the technological design and the specific notions of security. Thus, we find ourselves confronted with a double set of questions. On the one hand, it merits further scrutiny whether, and how, narratives with a military origin persist into practices of non-military UAS application – in other words, which 'hinterlands' (Law, 2009) they carry with them. On the other hand, we should investigate how these narratives are modified and translated in their new habitus, and how they lead to particular 'enactments' of the concepts of privacy and security (Law, 2004).

The Case: Unmanned Aircraft Systems (UAS)

The empirical base of our argument is a case study on Unmanned Aircraft Systems used for surveillance purposes. UAS are also referred to as Unmanned Aerial Vehicles (UAVs), Remotely Piloted Aircraft Systems (RPAS) or simply as drones. UAS have been defined more systematically as 'powered, aerial vehicles that do not carry a human operator' and that 'can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or non lethal payload' (Bone & Bolkcom, 2003: 1). Systems typically comprise a ground station and a data communication link (see figure 1). Depending on the payload, UAS can be deployed in various military and civilian scenarios. In this case study, military scenarios will be acknowledged, but the focus will be on non-military governmental and commercial applications. We intend to explain how the meanings of privacy and security emerge in this context, as opposed to considering how UAS are, or are not, ethically problematic.[1]

In this paper, we will engage with one particular class of UAS, namely the fixed-wing type suitable for both civilian and military purposes. Historically, most military UAS have been of the fixed-wing or 'aeroplane-like' type, quite different from the multi-rotor type that flies much more like a helicopter. The history of the latter is much more tied to civilian applications. Hence, if there is one site to spot military discourses riding piggyback on technology transfer, it should be with the fixed-wing type.

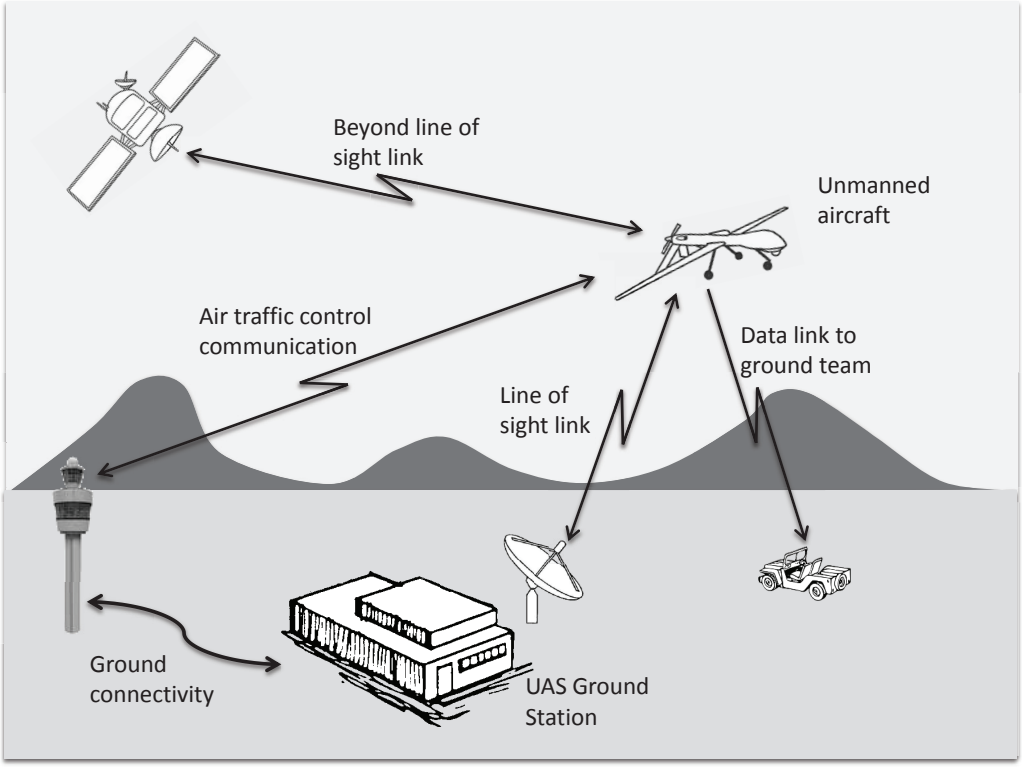

Figure 1. Communication links between ground station, airport, satellite and unmanned aerial vehicle

History

UAS have been around since the First World War. As soon as the technology emerged, it was immediately adopted by the military. While initially used for training anti-aircraft crews, transport of weaponry and for remotely launching bombs, their usage as reconnaissance aircraft began with the Vietnam War (Fahlstrom & Gleason, 2012). Throughout history, UAS have been most commonly associated with the military, only to appear in civilian applications more recently. They have been extensively used in armed conflicts for intelligence gathering and so-called targeted killing missions, e.g. in Kosovo (1999), Iraq (2003), Afghanistan and Pakistan (since 2001) to name a few recent examples (McBride, 2009; Gregory, 2011). Except for small scale UAS, unmanned aircraft are currently only allowed to fly in dedicated zones. A worldwide legislative process aimed at the integration of UAS into the civil airspace is currently underway, which would ultimately enable manned and unmanned aircraft to share the same airspace. In the European Union, this integration depends on initiatives at both member state level and at Union level. In the United States, the aim is to achieve full integration by 2015 – although this is considered very ambitious (Kornmeier, 2012: 8). Pilot applications for UAS may be possible by 2015, but

not general integration. Furthermore, a global coordination of national airspace regulation by the International Civil Aviation Organisation (ICAO) is planned to be complete by 2025. Only after this coordination will integration be complete (according to developer D3 involved in the regulation process; interviewee codes are explained below). This process depends not only on legal issues, but also on technological developments, e.g. on the improvement of sensor and collision avoidance systems and other as yet underdeveloped mechanisms to guarantee sufficient operational dependability and safety. Small-scale UAS can already be operated without major restrictions, whereas large UAS have a lengthy application process in most countries (European RPAS Steering Group, 2013).[2]

Despite the regulatory barriers, the number of users of unmanned aircraft has been growing slowly but steadily (Kornmeier, 2012: 8). It is expected that once the integration of UAS into civil airspace is complete, it will open the market for unmanned aviation.

Current Technology

In the last few years, UAS have received considerable media coverage in relation to targeted killing at war – not least the 'war on terror'.[3] Requirements for UAS to successfully execute combat, surveillance and reconnaissance missions are: the ability to fly at high altitude, long flight endurance time, long range and sometimes also undetectability. In addition to the flight requirements, the payload is expected to deliver high quality sensor data. In the ground station, the data must then efficiently be interpreted automatically or manually. According to multiple interviewees (D3–D5; interviewee codes will be explained below) who are working on large-scale military products, all these technical requirements are reflected in the technical design and thus in the resulting systems themselves.

UAS are systems consisting of a flying unit, usually equipped with some kind of payload. Those units require a ground station and a communication and data link (see figure 1). They can be as small as an insect or as large as an airliner (Eick, 2009). Often UAS are classified by weight (from less than 100 grams to 5 tons), range (from 1 to over 2000 kilometres), altitude (from less than 250 metres to 20 kilometres and above) and endurance (from less than 20 minutes to 48 hours of permanent flight). Shapes also vary considerably: airplane-like fixed wing designs and multi-rotor systems that can vertically take off and land are currently prevalent, UAS with other aerodynamic shapes are in development (Kornmeier, 2012: 13).

Usually systems are remotely operated and monitored by human flight operators (pilots) and additional evaluator(s) for interpreting payload data – all normally located at the ground station. The number of operators depends on the size of the system. Only one person is needed to operate very small UAS, while huge fixed-wing models, such as the MQ-9 Reaper by Northrup Grumman, requires more than 180 people (The Economist, 2011). However, not all systems require human operators in real time. There are aircraft that can fly (semi-) autonomously, e.g. on the basis of GPS and other sensor data, and, for example, supported by a collision avoidance system. Coordinates and/or routes are calculated on the basis of data obtained through sensors in real time during flight (Hing & Oh, 2009: 6). Additionally, some UAS also have the capability to operate in 'swarms', where units communicate with each other and are able to perform complex tasks together.

In most civilian applications, payload will typically consist of an attached video, infrared or thermal camera to get a bird's eye view. Surveillance missions often require additional signal intelligence hardware. Armed UAS for law-enforcement purposes are envisioned (Homeland Security News Wire, 2011; Brumfield, 2014), but to the best of our knowledge not in use yet. Sometimes the data captured by the payload is processed on-board, e.g. to calculate the flight path. However, it is more common for the payload to transfer data to the ground station. There, it can be processed directly – for example, using pattern-recognition algorithms, or by human operators – or it can be stored for future analysis.

In terms of operational advantages, unmanned aircraft are ideal for use due to the possibility of deploying small-scale systems on demand and due to the high range and altitude capabilities and, most important, the endurance of larger systems. In addition, UAS are argued to be more economically efficient than manned aircraft. However, this applies mainly to small-scale systems (Kornmeier, 2012: 8).[4] These characteristics can be taken advantage of in different mission scenarios, including border protection, law enforcement and surveillance, airborne sea patrol, search and rescue operations or scientific data collection (e.g. in hurricanes or forest fires). In general – at least in comparison to manned aircraft – UAS are typically deployed in dull, dirty or dangerous missions.[5]

Civilian Technologies, Military Narratives

Within *science and technology* studies, it is commonly understood that concepts by which people understand and take control of their life worlds cannot be separated from the technologies through which they shape that life world. This implies that translating a technology from one practice to another may offer particular concepts and the discourses organized around them the opportunity to ride piggyback on the technology. While the intrinsic political qualities attributed to technologies – as in Winner's famous discussion of the allegedly racist bridges on Long Island (Winner, 1988) – have long been questioned, postulating a connection between discourses and artifacts does allow us to see how incumbent discourses come to appear as poorly applicable to the practice they relate to.

While there are no such things as, *the* military realm and *the* civilian realm, we do observe certain elements in debates concerning the civilian use of drones that are surprising in light of existing moral and political discourses. These would, at the same time, be less surprising in a military context. Notably the low relative importance attributed to privacy by particular players in the development of drones, to be discussed shortly, seems unacceptable once programmes such as *Privacy by Design* (Cavoukian, 2009) have seen the light of day. Additionally, the fact that privacy has become a leading principle in the development of other surveillance technologies such as *automated license plate recognition* and the *body scanners* (van Lieshout et al., 2015) that are nowadays omnipresent at international airports, clearly dismisses as overly simplistic the explanation that technologists in general would be unreceptive to moral arguments. Also, it is highly unlikely that there is something exceptional to UAS in some technological sense that hampers privacy-friendly implementations. That would be a rather substantive, even deterministic, understanding of technology (cf. Feenberg, 1995) and the argument would be particularly unconvincing in regards of the other aforementioned privacy-

sensitive technologies. In fact, a rejection of such determinism provides an important ontological foundation for a doctrine such as *Privacy by Design* to be deemed feasible in the first place.

Rather, if politics are understood as a struggle for discursive hegemony (Hajer, 2005), then this is one way artifacts have politics. As will be articulated, the conceptual frameworks that travel with UAS technology are successfully displacing the aforementioned privacy-sensitive frameworks. That they are indeed discourses travelling with the technology (Harris, 2010), and not some category of essential properties belonging to the technology itself, is revealed when researchers and developers are invited to reflect on the possibilities of implementing privacy-friendly features on UASs. A considerable number of times they argue that such things would be possible, yet not the primary concern of UAS developers. Interviewee D1 (interviewee codes will be explained below) stated clearly what the primary concern is: '*In our development process, privacy plays no role in the first instance. Because when you develop technology, you try to solve a technical problem.*'

In the following empirical sections, we will present examples of such discourses, and explicate the clashes between those discourses that come with the technologies and those discourses that come from the purportedly 'more civilian' spheres of society.

When looking systematically at reasons for privacy not to be considered a technical problem, strong parallels appear with six rhetoric patterns articulated by Langheinrich (2003) in discourses concerning the potential privacy implications of ubiquitous computing:[6]

- Langheinrich's first pattern is that researchers do not feel morally responsible for privacy, either because privacy problems would not be applicable to their field of expertise, or because other social processes were felt to be more adequate to regulate such issues.
- The second rhetoric pattern is that privacy does not need to be paid any heed, since existing security mechanisms sufficiently safeguard it.
- Third, privacy as such appears as a premature issue or even a non-issue in many cases, since researchers thought that privacy could only be properly addressed after initial prototypes had been built.
- The fourth pattern is based on the third, namely that privacy would be no problem for prototypes, since privacy is not part of the context in which the early development takes place.
- Fifth, some researchers thought of privacy as too abstract of a problem to offer any sensible input to a technical design process.
- Finally, privacy is often not part of specifications and requirements, which entails that it is also not included in deliverables.

Variants of these patterns or story lines can be recognized clearly in the interviews that we conducted with UAS developers (D1–D5) and one researcher (R1). We understand these patterns as particular ways of 'externalizing' privacy concerns from the technology development discourse. This is an important constitutive element of the relevant discourse coalition, i.e. the group of actors across practices that share this discourse and its meaning (Hajer, 2005): by tapping into this repertoire of story lines, the actors *enact* drones as something

fundamentally distinct from discussing privacy. They thus reproduce and sustain a practice of UAS development that is devoid of privacy concerns, and uphold their legitimacy to do so.

Empirical Base

This case study is based on an analysis of relevant literature and ten qualitative interviews with UAS operators, developers, manufacturers and researchers in German-speaking countries, conducted in August/September 2013. Two users and two potential users of UAS were interviewed, five industrial developers and/or manufacturers, and one academic researcher in the field of unmanned aerial systems (see table 2).

In addition, *freedom of information* requests regarding privacy impact assessments related to UAS were sent to police forces in Essex, Merseyside, Staffordshire and Derbyshire in the United Kingdom and to the police in the German state of North Rhine-Westphalia as well as the German Federal Police. The aim was to understand which UAS privacy impacts police forces had identified and how they had dealt with them.

Civilizing Drones

Moving UAS from military uses into civilian uses, their 'civilising' if you like, involves their *translation* (Latour, 1987): not only are they to be moved physically to different spaces and sociotechnical practices, they also have to undergo qualitative changes in order to be fit to, and function in their new context. Likewise, the discourses that we presume travel with them, will undergo translation. Like any translation, this is a negotiation in which various discourse coalitions strive for hegemony. Translation of both the technology and the accompanying discourses requires work, as with new contexts come new demands.

If translation is the case, it is not self-evident for any element of either technology or discourse to survive or to decease: it requires explanation why some elements change while others don't.

We focus on a particular element of the military discourse that seems to survive this translation: a low priority assigned to concerns of privacy. Even though our analysis does not warrant an explanation of the low priority of privacy concerns merely in terms of the military origin of fixed-wing drones, it is worth pointing out that this prioritization appears both in the military

Table 1. Overview of interviewees

Identifier	Role	Description
R1	Researcher	In public research and technology organization
D1	Developer	In medium-sized aerospace company
D2	Developer	In small company specialized in mini UAS
D3	Developer	In big aerospace and defence company
D4	Developer	In medium-sized company specialized in UAS
D5	Developer	In big aerospace and defence company
U1	Potential user	Use in commercial environment
U2	User	Use for law-enforcement, part of the management
U3	Potential user	Use for law-enforcement, part of the management
U4	User	Use in commercial environment, sometimes in cooperation with law-enforcement

context and in the civilian contexts of UAV deployment. This is especially noteworthy, as privacy is among the primary concerns when technologies with a potential information impact are considered for application in non-military contexts. The discourses enacting this prioritization resemble the story lines identified in an abstract sense above by means of Langheinrich's (2003) conceptual inventory. Also, we see that it is not only a discourse with low priority for privacy, but also a further enactment and institutionalization of the externalization of privacy issues: those are literally delegated to sites outside the design practice.

In the first place, many of the narratives held up by people involved in drones reproduce an externalization of considerations of privacy. Those considerations are not reckoned part of the design space in which drone development takes place. This is atypical, as privacy considerations are amongst the primary hurdles that may be expected to appear if a technology is to be deployed with potential public impact. Notably, within the same population of experts, awareness is reflected of the existence of approaches such as *Privacy By Design* (Cavoukian, 2009), which explicitly pursue the implementation of privacy through (amongst other means) technological design. Also, in the light of their own expertise and position, interviewees recognize that much more is technically possible to implement privacy than is currently done in the development of civil-purpose UAS. It is in the ambiguity of whether or not privacy is external to technology design that, at least apparently, military styles of inference seem to retain dominance.

In addition, the externalisation of privacy issues appears clearly as an institutional distribution of responsibilities. Both users and engineers see the issue primarily as the duty of the competent supervisory authority: they must supervise the privacy compliant application of UAS. The interviewees mentioned the aeronautical authorities and the authorities that grant flight clearances as a potential source of compliance monitoring. A certain displacement is visible: if the problem of privacy is predominantly enacted as external to design practice, it is indeed likely to re-emerge somewhere else.

Interestingly, interviewees did not mention data protection authorities in this regard, which is again an interesting parallel with military practices, as data-protection authorities concern situations of peace rather than war.

Interviewed user U2 assumed that if there were any privacy impacts in the technology, they would have been addressed in the procurement procedure. The *freedom of information* requests we sent to police forces asking for privacy impact assessments made in the context of UAS procurements, showed that no such impact assessments had been made prior to any procurement. Therefore we assume that privacy considerations were not part of procurement procedures. All explanations provided boiled down to the idea that 'there is no legal requirement for us to do so.'[7] Alternatively, user U3 lists a number of privacy measures such as non-retention policies and compliance with data processing laws as protection mechanisms, which relate to operation rather than design – technical measures and early-phase design adaptations being notably absent.

Reasons for privacy not to be part of the design problem also exist in the form of perceived attributions of moral responsibility. Five out of six interviewed developers and the researcher (D1–D5, R1) did not feel morally responsible for protecting privacy. If at all, privacy would become important in later development processes such as system integration and

deployment. It is reflected in the majority of interviews that *'each system operator is responsible for a lawful operation'* (D2), including privacy laws, as the exact privacy relevance of the technology hinges upon its particular application.

All interviewed developers and the researcher (D1–D5, R1) stated that privacy is too abstract of a problem to solve technically. D2 even stated '*that [it] is not possible*' to solve technically. They argued that during the development process, it is not foreseeable how privacy will be situated in the contexts in which the system is to be used. One interviewee stated that privacy is not a problem for prototypes, since these preliminary models will never be used outside the development context. Thus, from their point of view, there is no need to protect privacy in a technical way, as it is not part of the UAS's problem and design description. Five out of six literally confirm that privacy is not part of their deliverables, since customers do not ask explicitly for such features. Also, as manufacturers, they are not obliged to implement privacy protecting features. While we would not go as far as claiming that the developers maintain a purely instrumental view of technology, it is clear that they do maintain a view of technology that attributes much of the meaning of the technology to the context of operation.

In addition, there is yet another institutional arrangement that helps see privacy as not being a design problem. The market for fixed-wing UAS is dominated by manufacturers who supply to both military and non-military customers. Interviewees D2 and D4 stated that they sell their systems only to users who are certified to comply with laws and do not abuse the technology. One interviewee from this group (D4) stated that his company sells exactly the same fixed-wing systems to the military and law enforcement agencies, be it with differently configured payloads. This means that non-military governmental customers in some respects have similar technical possibilities as do military customers. As the market supply of civilian fixed-wing UAS is not very high compared to the military market, purchase options outside military-oriented suppliers are limited. This means that for potential civilian users, a tendency exists towards the purchasing of technologies that have been developed in a context in which privacy was not a primary consideration. Also, D4 argues that military parties are hegemonic in the development of drones. As a consequence, privacy is not likely to be a feature in the 'drone catalogue'. Even if non-military governmental customers have other requirements, it is difficult for them to find alternatives (Rodrigues, 2015).

These institutional and discursive forms of externalization consistently render privacy a retro-fitting problem, to be resolved once the functional design of the UAS is more or less completed. This is where the paradox, that possibilities for implementing privacy in a technological way are both confirmed and denied, becomes even more pressing. Indeed, with *Privacy by Design* in mind, it should be expected that such retrofitting will at best deliver sub-optimal solutions (Cavoukian, 2009).

Remarkably, the interviews do not provide any evidence that the persons involved in the development of UAS think of security as a value that is to be implemented in merely technological terms. Much like the general trend in the story lines mobilized when discussing privacy, security is also not seen as something particularly linked to technology, but rather as something that is the result of a practice in which some technologies happen to be deployed. Both the engineers and the users interviewed agreed that security is something that emerges as a result of how technologies are

used, not as an unmediated consequence of those technologies. Developer D2, for example, mentions that UAS technology *'alone cannot contribute to public security'* but rather adds to an already existing set of tools of governmental users. This view is consistent with the other engineering interviewees who claimed that they provide a tool that is then deployed by someone else. This view was epitomized in one interview, when developer D4, who is only supplying to governmental customers, explicitly rejected the view of UAS as being a security technology. Rather, he described it as platform systems: *'It depends on what you do with this platform, how you equip this platform, which payload will be mounted, and above all, how the [information generated by the] payload will be used in the ground station'* with security being only one of many use cases.

This is again the intricate balance between technological instrumentalism and radical social constructivism: neither technologies nor socio-cultural arrangements determine what privacy and security are, but rather how the technology operates in its proper context. It is vital to recognize here that this shape of the discourse silences contestation of hegemonic perspectives. In particular, it silences privacy issues, and it leaves perspectives on security uncontested. In this very particular arrangement, a strong parallel is reflected with the military deployment of drones, and their appearance as security devices. While the latter may not be the cause of the former, it is worth pointing out that the *de facto* structure of the discourse on civilian UAS is favourable towards patterns already existing around military UAS.

Thus far, we have mainly considered how privacy is thought to be something existing outside the technological design space. Another question is whether or not privacy and security can be realized at the same time. The literature has widely disproved the idea that privacy and security must be mutually exclusive values (Solove, 2008, 2011; van Lieshout et al., 2013; Valkenburg, 2015). Yet, in the discourse coalition of UAS producers and users it seems as if these values cannot be served at the same time: it takes the function of security as the main driver for the development of drones, while putting privacy 'on hold' for a later phase of development.

The idea that privacy is not a moral obligation for designers and producers to implement into their UASs, is of course closely related to what they think privacy is. All five engineers (D1–D5) and the researcher (R1) interviewed reproduce a legalistic understanding of privacy in the context of UAS development, namely that *'what is meant here by privacy is enshrined in law'* (D3). It became clear that this view hinges heavily on the principle of informational self-determination and on existing data protection laws. When talking about privacy, most interviewees did not distinguish between the protection of personal data and the protection of privacy and the private sphere in a wider sense. Thus, the ontology predominantly maintained in practice constitutes a relatively narrow definition of privacy. This results in a low likelihood for privacy to become an integral part of the design process.

This is again a salient similarity between the military discourse and the *de facto* discourse on civilian UAS. In war and combat situations, military operations are a matter of life and death. The life of a soldier is valued highly, even when national security is at stake. This means that even if national security ultimately outweighs the soldier's security, the two are at least commensurate in the sense that it is considered that both should be considered and weighed against each other. To deliver these two forms of

security, the highest possible quality of data is needed, without any limitations, or so it is argued in the military discourses that we observed in multiple interviews. In such situations, privacy is not much of a concern, and certainly ranks below national security and soldier life. Thus, if indeed a military perspective is assumed, it is at least understandable that privacy becomes excluded from the discourse, and by consequence fails to become part of technical requirements for military UAS.

Interviewee D5, who is working for the governmental as well as for the commercial market, reported that his company's business model is not just to sell UAS, but also to offer services based on unmanned aviation, e.g. monitoring of critical infrastructure such as gas pipelines. In this case an interesting situation emerges: the manufacturer is also the user who has to comply with all regulations. Consequently, this interviewee has a general interest in technological designs that implement and guarantee privacy and, at the same time, fulfil the desired mission. These thoughts confirm that privacy could indeed become part of the technical problem description through the shifting and merging roles of manufacturers and users. Hitherto, though, while this opens the door for *Privacy by Design* and similar approaches, the emphasis is yet on operational and post-design solutions, not on the implementation of privacy in the technological design at an early phase.

The interviewed users' and potential users' understanding of privacy concurs with the engineers' understanding of privacy as a post-design issue. An important difference was, though, that the users additionally reflected on the socio-political consequences of UAS deployment and even had personal concerns and fears regarding privacy. This aspect did not come up in interviews with engineers. Oddly enough, only interviewee U1 gave a thought to technical mechanisms to ensure compliance with legal requirements regarding data protection and privacy.

Conclusion

It followed from the interviews that the problem of privacy was largely assigned to users, not to designers. However, as existing discourses show, quite some potential exists for privacy to be pursued in the (arguably technical) design phase, rather than *post-hoc* in the form of regulation. There is no natural or self-evident reason why this potential could not be realized, and in fact interviewees often acknowledged this potential as realistic. We have tried to explain the 'unrealisation' of this potential by reference to the capability of military discourses to travel with the very technologies in question.

Part of the answer, as we argued above, might be in the military history that preceded the current state of affairs in unmanned flying. Privacy simply is not an important concern in military operations. Also, since, even today, the military is still an important client of UAS vendors, it is to some degree understandable that incentives are missing to pay more attention to privacy in the development of UAS. However, this explanation is far from complete: as unmanned flying is currently developing rapidly, especially in the civilian sector, it could be equally self-evident that there is economic potential in creating marketable products that offer innovative solutions to privacy concerns.

It is for this reason that additional research might reveal further reasons why this seemingly military discourse is so attractive outside the military sphere. While it long has been suggested that it is not naturally given for technological design practices to realise other values than

efficiency (Feenberg, 2002), it is also fair to say that considerable attention has been paid to examples of technologies where other human values are yet inscribed, not least the *Privacy By Design* framework mentioned earlier (Cavoukian, 2009). More detailed study of the histories and contexts of involved people might reveal why privacy has yet not become part of their practice. It might have been missing in their education, it might be that tacit parts of the corporate structures they work in are particularly geared against such considerations, it might be that spheres in which procurement takes place are unfavourable to such offers, or other.

Yet, despite the fact that we at least have to be open to such alternative explanations that are neither confirmed nor disproved by our empirical analysis, we can conclude first, that a particular distribution of responsibility is apparently *reproduced* in the practices of UAS development. This reproduction takes both material and discursive shapes. The discursive part has been explained above: as is clearly witnessed in the interviews, people keep *talking* about UAS in the particular frame that renders privacy a non-issue – or at least as a non-issue for technical design. The material part is the fact that change is always costly in the short term: it is not surprising that the cheapest option is simply to recycle military designs (the so called 'lock-in effect'). It is also in the fact that once these UAS are there, they pre-structure how people tend to talk and think about them. Some options are more within reach than others, simply because a particular material configuration already exists.

Second, part of the answer to the question of why respect for privacy is not an internal part of the design process may lie in the fact that 'implementing privacy' is never just that. It also involves redesigning notions of safety and security, it involves redesigning how costs and benefits are defined and how they are distributed, and it involves redefining the notion of privacy itself so as to make it apt for informing technological design *in this particular practice*. That is to say: the problem of privacy will have to be *translated* such that it fits the development process of UAS. In this respect, it is important to realize that the technical potential to develop privacy-friendly solutions is not something that sits on a shelf to be picked up, but requires further adjustment and fine-tuning towards the very design of UAS. In consequence, making privacy respecting UAS takes more than simply discussing what privacy could be in this particular context. It also requires discussing how the development process of UAS must itself be revised, and how discourses and institutional structures must be devised that resemble less the military context and discourses that externalize the issue of privacy.

If the argument of this paper cuts ice, any normative program pursuing a more privacy-friendly design for UAS should start not at the level of normative ideas, but at the meta-level of how discourses are arranged. This should include an idea of how this meta-level depends itself on the technologies it discusses and of how technologies and discourses are closely knit together. Only then can the more conceptual avenue, of discussing how privacy can be internalized such that it becomes commercially interesting, be explored and hence made part of the (technical) design specifications. This would include an exploration of ways the design of UAS can be better politicized, rather than defining privacy outside the scope of design requirements, thus emptying the design practice of one particularly controversial issue. Bringing it in will likely generate the friction that is needed to come to creative solutions and connect the radically different

discursive universes of the military and the civilian realms (cf. Tsing, 2005).

Acknowledgment

This paper draws on research carried out in the EC-funded FP7 project PRISMS: The Privacy and Security Mirrors: Towards a European framework for integrated decision making (FP7-SEC-2010-285399). The comments and suggestions of Dara Hallinan, Marc van Lieshout and the reviewers on earlier versions of this manuscript are highly appreciated.

References

Bone E & Bolkcom C (2003) *Unmanned Aerial Vehicles: Background and Issues for Congress*. Washington, D.C.: Library of Congress.

Brumfield E (2014) Armed Drones for Law Enforcement: Why it Might Be Time to Re-Examine the Current Use of Force Standard, *McGeorge Law Review* 46: 2014–2015.

Cavoukian A (2009) *Privacy by Design … Take the Challenge*. Toronto: Information and Privacy Commissioner of Ontario.

The Economist (2011) Flight of the drones: Why the future of air power belongs to unmanned systems. 8 October. Available at: http://www.economist.com/node/21531433 (accessed 29.01.2015).

Eick V (2009) Das Dröhnen der Drohnen: Technisierung von Überwachung und Kontrolle, *Bürgerrechte und Polizei/CILIP* 94: 28–40.

European Commission (2012) *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)*. COM(2012) 11 final. Brussels.

European RPAS Steering Group (2013) *Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System*. Brussels: European Commission.

Fahlstrom, PG & Gleason TJ (2012) *Introduction to UAV Systems*. Chichester: Wiley.

Feenberg A (1995) *Alternative Modernity*. Berkeley, Los Angeles and London: University of California Press.

Feenberg A (2002) *Transforming technology: A critical theory revisited.* Oxford; New York: Oxford University Press.

Finn, RL & Wright D (2012) Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications, *Computer Law & Security Review* 28(2): 184–194.

Finn RL, Wright D & Friedewald M (2013) Seven types of privacy. In: Gutwirth S, Leenes R, De Hert P & Poullet Y (eds) *European Data Protection: Coming of Age*. Dordrecht: Springer, 3–32.

Gregory D (2011) From a View to a Kill: Drones and Late Modern War, *Theory, Culture & Society* 28(7–8): 188–215.

Gutwirth S (2002) *Privacy and the Information Age*. Lanham, Boulder, New York, Oxford: Rowman & Littlefield.

Hajer MA (2005) Coalitions, Practices, and Meaning in Environmental Politics: From Acid Rain to BSE. In: Howarth D & Torfing J (eds) *Discourse Theory in European Politics. Identity, Policy and Governance.* Basingstoke: Palgrave Macmillan, 297–315.

Harris CV (2010) Technology and Transparency as Realist Narrative, *Science, Technology & Human Values* 36(1): 82–107.

Heise K (2013) Drohnen sollen Menschenmassen überwachen. *Die Welt*, 07 Januar, Available at: http://www.welt.de/wissenschaft/article112471009/Drohnen-sollen-Menschenmassen-ueberwachen.html (accessed 30.04.2014).

Hing JT & Oh PY (2009) Development of an Unmanned Aerial Vehicle Piloting System with Integrated Motion Cueing for Training and Pilot Evaluation. In: Valavanis KP, Oh P & Piegl LA (eds) *Unmanned Aircraft Systems.* Dordrecht: Springer, 3–19.

Homeland Security News Wire (2011) Texas county police buys drone that can carry weapons. 31 October. Available at: http://www.homelandsecuritynewswire.com/texas-county-police-buys-drone-can-carry-weapons (accessed 29.01.2015).

Kornmeier C (2012) *Der Einsatz von Drohnen zur Bildaufnahme: Eine luftverkehrsrechtliche und datenschutzrechtliche Betrachtung*. Münster: Lit Verlag.

Langheinrich M (2003) The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects. Paper presented at the *Designing for Privacy Workshop. Conference on the Tales of Disappearing Computers*. Santorini, Greece. Available at: http://www.vs.inf.ethz.ch/publ/papers/dctales-privacy.pdf (accessed 29.01.2015).

Latour B (1987) *Science in Action: How to Follow Scientists and Engineers Through Society*. Cambridge, Mass.: Harvard University Press.

Law J (2004) Enacting Naturecultures: a Note from STS. Available at http://www.lancaster.ac.uk/fass/sociology/research/publications/papers/law-enacting-naturecultures.pdf (accessed 29.01.2015).

Law J (2009) Seeing like a survey, *Cultural Sociology* 3(2): 239–256.

McBride P (2009) Beyond Orwell: The Application of Unmanned Aircarft Systems in Domestic Surveillance Operations, *Journal of Air Law and Commerce* 74(3): 627–662.

Rodrigues R (2015) The Surveillance Industry in Europe. In: Wright D and Kreissl R (eds) *Surveillance in Europe.* London, New York: Routledge, 101–49.

Solove DJ (2008) 'I've got nothing to hide' and Other Misunderstandings of Privacy, *St. Diego Law Review* 44: 745–772.

Solove DJ (2011) *Nothing to Hide: The False Tradeoff between Privacy and Security*. London, New Haven: Yale University Press.

Syed BS (2013) 2,160 terrorists, 67 civilians killed by drones. *Dawn (Islamabad, Pakistan)*, 31 October. Available at: http://www.dawn.com/news/1053069/2160-terrorists67-civilians-killed-by-drones (accessed 30.04.2015).

Tsing AL (2005) *Friction. An ethnography of global connection.* Princeton and Oxford: Princeton University Press.

U.S. Government Accountability Office (2013) *Defence Acquisitions: Assessment of Selected Weapon Programs*. Washington: Government Printing Office.

Valkenburg G (2015) Privacy versus security: problems and possibilities for the trade-off model. In: Gutwirth S, Leenes R & De Hert P (eds) *Reforming Data Protection: The Global Perspective.* Dordrecht: Springer, 253–269.

van Lieshout M, Friedewald M, Wright D & Gutwirth S (2013) Reconciling privacy and security, *Innovation: The European Journal of Social Science Research* 26(1–2): 119–132.

van Lieshout M, van Schoonhoven B, Roosendaal A, Valkenburg G, Huijboom N, van Veenstra AF, Braun S & Friedewald M (2015), *Security and privacy technologies: understanding trends and developments*, PRISMS Deliverable 2.3, Available at: http://prismsproject.eu (accessed 25.06.2015).

Winner L (1988) Do artifacts have politics?, *Daedalus* 109(1): 121–136.

Woody T (2014) Drones Are Becoming Energy's New Roustabouts. *The New York Times*, 21 April. Available at: http://www.nytimes.com/2014/04/22/business/energy-environment/drones-are-

becoming-energys-new-roustabouts.html?_r=0 (accessed 30.04.2015).

Notes

1 For a recent analysis of the privacy and ethical aspects of UAS surveillance see (Finn & Wright, 2012).

2 In Europe discussions are going on whether small scale UAS should be brought under the umbrella of European Civilian Aircraft Authorities as well; this also deals with the private use of UAS for sport and leisure.

3 Even though it is questionable whether the war on terror is formally a war, we believe this distinction is not relevant to the current argument.

4 Accordingly, small-scale systems mostly have low range, altitude and endurance. Large and mostly fixed-wing UAS having a high range, altitude and endurance are mostly very expensive. For example, the Global Hawk by Northrop Grumman, which is not yet in use for civil applications, costs about $ 222 million without maintenance costs. In addition, interviewee R1 stated that due to personnel and infrastructure costs an unmanned flight is generally more expensive than manned flights, except for systems that can be operated by few persons. See (U.S. Government Accountability Office, 2013: 113)

5 In the context of UAS `dull' means long-endurance missions requiring very long flight times. `Dirty' means missions with a risk of human exposure to nuclear, biological and chemical agent concentrations. `Dangerous' missions are those with a risk of human exposure to air defence and counter-air defences.

6 Ubiquitous computing is the concept to invisibly embed computing and communication hardware in all kinds of object and in the environment with the goal to make computing capabilities available everywhere and anywhere.

7 In Europe, privacy impact assessments are a relatively new instrument and not required by law. As 'data protection impact assessment' a variant is proposed in Art. 33 of the draft General Data Protection Regulation. See (European Commission, 2012)

Sven Braun
Technical University of Darmstadt
64289 Darmstadt, Germany
sb@devbraun.de

Michael Friedewald
Fraunhofer Institute Systems and Innovation Research
Breslauer Strasse 48
76139 Karlsruhe, Germany
michael.friedewald@isi.fraunhofer.de

Govert Valkenburg
Maastricht University
Faculty of Arts and Social Sciences
Maastricht, The Netherlands
g.valkenburg@maastrichtuniversity.nl