MSc Thesis | December 2015

THE ETHICS of **DOMESTIC DRONES**

An Ethical Evaluation of the Use of Surveillance-Capable Unmanned Aerial Systems in Civil Contexts

by Philip Jansen

THE ETHICS of DOMESTIC DRONES

An Ethical Evaluation of the Use of Surveillance-Capable Unmanned Aerial Systems in Civil Contexts

---

by Philip Jansen

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in
Philosophy of Science, Technology and Society

University of Twente,
December 2015

Supervisor:
Prof. P.A.E. Brey

Second reader:
Dr. A.L. van Wynsberghe

Summary

This study is a contribution to the ethical understanding of the civil use of surveillance-capable *unmanned aerial systems*, also known as "drones". It focuses on analyzing the present and potential future capabilities and applications of such drones, the ethical issues they bring up, and their ethical admissibility. In all these areas, there has been little in the way of systematic and comprehensive research. Since the use of drones with aerial observation and surveillance capabilities is variously argued to present great benefits but also significant ethical concerns, such research was deemed in order. Specifically, this study was aimed at providing answers to the following questions:

1. To what extent is the civil use of drones that are capable of public surveillance ethically justified in light of its potential effects on privacy and other ethical values?
2. What ethical issues need to be considered in efforts to improve the ethical justifiability of the civil use of drones that are capable of public surveillance?

Among the methods that I have used to answer these questions are the *anticipatory technology ethics* approach by Philip Brey (2012); the *seven types of privacy* approach by Finn, Wright & Friedewald (2013); the *contextual integrity* approach by Helen Nissenbaum (2010); and the *proportional balancing* approach by Aharon Barak (2010). The anticipatory technology ethics (ATE) approach has formed the overarching methodology for this study. This is a relatively new approach for the ethical study of *emerging technologies*, which uses *forecasting* and *futures studies* to deal with the problem of uncertainty about a technology's future devices, applications, and societal consequences. Thus, in accordance with the ATE approach, I have conducted an analysis of the future capabilities and applications of surveillance-capable drones, the results of which have formed the input for ethical analysis in this study. Another prominent feature of the ATE approach is that it employs three separate levels of ethical analysis: the *technology level*, the *artifact level* and the *application level*. Thus, I have analyzed surveillance-capable drones in terms of *surveillance-capable drone technology at large*, various *types of surveillance-capable drones*, and various *applications* of such drones. These separate levels have allowed for a very comprehensive ethical analysis of civil drone use that includes the study of fundamental ethical issues pertaining to drone technology at large, and the study of more specific and contingent issues that depend on specific types of drone and specific drone applications. Finally, there are a few ways in which I have expanded the ATE approach or adapted it to the specifics of the case at hand. Most importantly, I have expanded it by presenting (1) an extensive account of how to resolve value conflicts during an ethical evaluation, and (2) a method to determine the ethical permissibility of a technology or technological artifact.

With regard to *surveillance-capable drone technology*, I have concluded in this study that its use in civil contexts is, in principle, ethically justified since the marginal benefits offered by its present and future use in such contexts significantly outweigh the marginal harms. Nevertheless, I found that there are many important ethical issues inherent in drone technology, which deserve careful consideration in any effort to improve the technology's ethical acceptability. Firstly, it was argued that the privacy concerns relating to *behavioral privacy*, *privacy of location and* space, *privacy of association*, *privacy of property*, and *privacy of data and image* are of a very high societal importance. Of particular importance, perhaps, is the impact on *behavioral privacy*, as it contributes very significantly to a "chilling effect" on society in outdoor space—

one that involves serious harms to values such as freedom, autonomy and democracy. As for the other ethical issues at this level of analysis, the issues of *function creep*, *discriminatory targeting and profiling*, and *abuse, error and accountability* were judged to be very important; and the issues of *unequal burden of surveillance* and *shifting of ethical norms* were deemed to be of moderate importance.

In the analysis of *drone artifacts*, I distinguished between three broad categories of surveillance-capable drones: *large wide-area persistent surveillance* (WAPS) *drones*, *small general-purpose drones*, and an anticipated class of *biomimetic spy drones*—which are defined as small and stealthy insect-like or bird-like surveillance drones. As regards the ethical justifiability of these three types, I concluded that there should not be categorical bans on the civil use of large WAPS drones and small general-purpose drones; on the other hand, I argued that, unless there can be adequate safeguards against the threat of *function creep*, a ban ought to be placed on the civil use of biomimetic spy drones—a ban that should at least cover those biomimetic drones that are highly imperceptible and easily mistaken for the animals they are intended to mimic. All three types of drone were found to bring about important ethical issues that should be considered in efforts to mitigate their ethical consequences. For large wide-area persistent surveillance drones, the issues of *increased moral distance to surveillance subjects* and *safety of flight* are respectively of high importance and of moderate importance; for small general-purpose drones, the issues of *concerns about privacy of the person* and *safety of flight* were both judged to be of high importance; and for biomimetic spy drones, the issue of *increased potential for various privacy harms* as a result of their imperceptibility was judged to be of critical importance, and the issues of *concerns about privacy of the person* and *potential harm to (the experience of) wildlife* were considered to be of high importance.

Finally, with regard to *applications of surveillance-capable drones* in civil contexts, I concluded that, while there are great concerns about such applications in general, by far not all of them are morally unacceptable. Given the right circumstances and parameters, even persistent surveillance applications for policing purposes can be ethically justified. In particular, under the conditions set by four very specific but realistic application scenarios, I judged as *ethically justified* the use of small drones for journalistic coverage of socially important news events, and the use of WAPS drones to prevent terrorism during a high-profile public event; and I judged as *not ethically justified* the use of a WAPS drone in a moderately important criminal investigation, and the use of WAPS drones to offer a real-time public mapping service. I further concluded that the justifiability of drone applications is generally highly dependent on whether the goals and values of the broad social contexts of everyday life in *outdoor public space* and *outdoor private space* are served, since these contexts have an overwhelming presence in drone applications. Hence, any impacts of drone use on outdoor physical mobility, informal social life and community cohesiveness, and the associated values of freedom, autonomy and sociality, can be expected to be of high ethical importance and need to be considered in efforts to improve the overall ethical acceptability of civil drone use.

The general conclusion of my research is that the civil use of surveillance-capable drones is, *in principle*, largely justified. Only the civil use of *biomimetic spy drones* was judged to be categorically unethical. In terms of applications, the ethical acceptability of drones appeared to be something of a mixed bag. These conclusions on ethical acceptability, however, are not to understate the severity of the ethical issues, which was found to be very considerable at all three levels of ethical analysis.

Preface

I first became interested in the ethics of domestic drones through my thesis supervisor, Professor Philip Brey, who had steered me towards it from an earlier interest in the ethics of military-type drones. In contrast to the military variants, not much research had been done on the ethics of using civil drones, which in recent years have become a fast-growing and impactful technology. Because of their capabilities for observation and surveillance, these civil drones present a whole new range of ethical issues, which are quite urgent and prominently include concerns relating to privacy. Of course, there are other important issues relating to other aspects of civil drone technology, such as their potential weapons capabilities; however, it was these surveillance-related issues that interested me the most and therefore became the focus of my research. In the end, my decision proved to be a good one, as I feel that with this study I have made a meaningful contribution the ethical understanding of the use of surveillance-capable drones in a civil context. I sincerely hope that my findings will be of value in the societal discussion on the ethical acceptability and future direction of drone technology.

It deserves to be mentioned that a lot of effort went into writing this thesis, which took well over a year to complete. The fact that it took so long was in part due to my obligations for the SATORI ethics project at my university. My perfectionism may also be to blame. Although it generally serves me well, I sometimes wonder whether I may have bit too much of it.

There are a few persons whose supportive efforts I would like to acknowledge. First, I wish to thank my supervisor, Prof. Philip Brey, for his insightful comments on various early drafts (of chapters) of this thesis and for his words of encouragement along the way. I also wish to thank my second reader, Dr. Aimee van Wynsberghe, for really dissecting the final draft of this thesis at the very end and providing me with a lot of helpful and encouraging comments. Finally, I would like to thank Mr. Pieter Elands at TNO for sharing his knowledge and insights, through various personal communications, about the present and future state of development of civil surveillance-capable drone technology. In addition, I want to thank Mr. Elands for the book on miniature drones he so kindly sent me.

Philip Jansen
December 2015

Contents

1 Introduction

Unmanned aerial systems (UASs), or "drones" as they are colloquially called, are expected to dominate the future of aviation as thoroughly as manned aircraft have dominated its past. They have long been deployed for military applications, and are now increasingly also being used for civil applications. According to the European Commission, there are currently more than 400 projects across 20 European countries to develop civil UASs (Reuters, 2013). Furthermore, according to the Association for Unmanned Vehicle Systems International, U.S. sales of civil UASs are expected to top $82 billion in the period from 2015 to 2025, generating about 100.000 jobs (Jenkins & Vasigh, 2013). Typically, these civil UASs are about the size of a large bird, and remotely operated by a pilot on the ground. They can be furnished with a great variety of sensors, actuators, and data processing equipment, which includes high-resolution video and still cameras, thermal imaging cameras, night vision cameras, radiation detectors, mobile-phone jammers, and air sampling devices. Thus, being highly versatile, civil UASs are used in such fields as aerial photography, geo-mapping, agriculture, infrastructure monitoring, wildlife monitoring, firefighting, meteorology and climatology, search and rescue, and policing. They are often preferred for missions that are "dull, dirty or dangerous", as they protect human pilots from fatigue and environmental hazards (Finn & Wright, 2012). Moreover, they are often significantly cheaper to procure, operate, and maintain than manned aircraft. Thus, clearly, there are great incentives for the development of civil UASs technology and applications.

The use of UAS technology, in its various guises, has given rise to a range of ethical concerns. Most prominently, the ethical debate about UAS use has revolved around their military applications, which have been a focal point for the high-profile Campaign to Stop Killer Robots[1] and the International Committee for Robot Arms Control.[2] In recent years, however, there has also been a steady rise in attention for the ethics of civil UASs and their applications. This may have been driven, at least in part, by the increasing number of curious as well as serious incidents involving civil UASs. For example, UASs have been used to smuggle drugs to prison inmates by dropping them on the prison yard (Boyle, 2015); a U.S. citizen has recently shot down a UAS flying over his property, which he alleged was violating his privacy (Cummings, 2015); and the U.S. Federal Aviation Administration has reported it has recorded almost 700 near-collisions in the U.S. between airplanes and UASs over the first nine months of 2015 (Whitlock, 2015). The focus of this study, however, is not on assorted events like these, but on one particular aspect of civil UASs that is going to have significant ethical implications and has thus far received rather scarce scholarly attention—namely, their capacity for *public observation and surveillance*.

In the future, drones (as I will call them from here on out[3]) will increasingly be deployed in civil contexts for aerial observation purposes. Police forces around the world are already starting to use them to monitor large crowds, prevent or detect crime, and assist in incident responses. Within two decades, drones could

[1] See: http://www.stopkillerrobots.org/

[2] See: http://icrac.net/

[3] I am aware that from a technical standpoint the term "drones" may not strictly refer to unmanned aerial systems or vehicles, since, for example, unmanned underwater vehicles may also be called "drones". Nonetheless, I have chosen to use this term from here on out because it is the simplest and most widely understood way of referring to unmanned aerial systems.

be used for jobs such as perimeter patrols around prisons, capturing of license plate numbers of speeding drivers, and detection of cannabis plantations in roof lofts (Bowcott & Lewis, 2011). Besides law enforcement, other institutions, commercial organizations and private citizens could use drones to conduct observation in public for their own varied purposes. For example, a company such as Google may be interested in using drones to create a real-time electronic mapping application, and journalists could use drones for reporting news. It seems as if the number of potential applications of drones involving at least some element of public observation or surveillance is limited only by the imagination.

The British Surveillance Studies Network (2008) has identified deployments of drones for surveillance purposes as forms of "new surveillance". According to Gary Marx (2002), this "new surveillance" is characterized by gathering of information from categories of interest rather than specific persons, an increase in the amount of data collected, remote operation, less coercive data collection, and a "routinization" of surveillance. Future drone surveillance applications are perfect instances of "new surveillance" since future drones may (1) be almost undetectable to the targets being watched due to their low visual and audial profile, (2) have the ability to (autonomously) gather and analyze large amounts of data about many people at once, and (3) stay aloft for extended periods of time.

Despite their apparent benefits in terms of security, efficiency, and other values and interests, civil drones with surveillance capabilities raise a number of profound ethical concerns. With everyone getting filmed, photographed, tracked, and analyzed, one issue that immediately springs to mind is the effects on privacy. What level of privacy should people expect when they are out in public? Often, the law says that there is no reasonable expectation of privacy in public spaces. A U.S. Supreme Court Justice has argued that "a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited" (Dunlap, 2009, p. 185). European Court of Human Rights, somewhat differently, holds that "the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life" (Williams, 2008). This makes any form of public observation lawful, at least as long as data is not being recorded. Nevertheless, there may be something unnerving about the idea of a large-scale use of drones with visual and other sensory surveillance capabilities. As an FAA spokesman once stated, "[i]t smacks of Big Brother if every time you look up there's a bug looking at you" (The Economist, 2007). Perhaps we need a new conception of privacy that better accords to our intuitions in this case—one that does grant to people a right to a certain level of privacy when they are in public spaces. What is clear, though, is that the issue of privacy here is an important one that deserves careful analysis—analysis that has been lacking up till now.

Privacy may not be the only right or ethical value that is impacted by drone observation. The right of non-discrimination, for example, may also be impacted. Finn and Wright (2012) have argued that already marginalized populations—the poor, people of color, and anti-government protesters—receive disproportionate attention from drone deployments, as a result of the specific applications that drones are used for, as well as, perhaps, a so-called "distantiation effect" of drone use. In sharp contrast to this, Myers Morrison (2014) has argued that drone surveillance could supplant profiling and other police practices that make members of these populations feel singled out and humiliated. Another right that may be impacted by drone surveillance is the right of freedom of expression. It has been argued that the mass deployment of surveillance drones that are imperceptible from the ground "could lead to an environment

where individuals believe that a UAS is watching them even when no UASs are in operation" (McBride, 2009, p. 659). This could have a self-disciplining effect, as described by the philosophers Jeremy Bentham and Michel Foucault, where people adjust their behavior to the ever-present possibility that they are being watched (McBride, 2009). Further rights that are be impacted by future drone surveillance may include freedom of assembly, autonomy, and security. The impacts of drone use on all these rights may, too, warrant careful analysis.

Research objectives

Although it is clear that there are serious potential ethical issues with the large-scale use of drones for purposes with public surveillance aspects, and even though academics, civil society organizations and journalists have already voiced their concerns about these issues, there has been comparatively little research done on them. Since there are big incentives for the development of drones and their deployment for aerial observation and surveillance purposes by public and private sector organizations, and even by private citizens, an investigation into the ethics of drone use for public observation may be in order.

My primary aims in this analysis are twofold: firstly, I wish to determine the extent to which the present and projected use of surveillance-capable drones is ethically justified in civil contexts; and secondly—and more constructively—I wish to determine the importance of the ethical issues that would need to be considered in any effort to improve the ethical justifiability of the use of such drones in civil contexts. The second aim is of course very much related to the first. These aims translate into the following main research questions:

1. To what extent is the civil use of drones that are capable of public surveillance ethically justified in light of its potential effects on privacy and other ethical values?
2. What ethical issues need to be considered in efforts to improve the ethical justifiability of the civil use of drones that are capable of public surveillance?

Let us briefly clarify some terms here. First of all, throughout this study, I will often use the term "surveillance" in a loose sense to mean surveillance as well as simple observation. *Surveillance* can be defined as the close and sustained monitoring of people—their behavior or other changing information—for the purpose of influencing or protecting them (Lyon, 2007).[4] Although I include in this analysis the ethical impacts of all forms of observation, many of the most severe ethical impacts result from drones' capabilities for surveillance, which is why I give preference to this term rather than the term "observation". Secondly, as regards "*public* surveillance", this is usually defined as surveillance in *public spaces*, which are social spaces that are generally open and accessible to people. Roads, public squares, parks and beaches are typically considered public spaces. To a limited extent, buildings that are open to the public, such as train stations and public libraries, are also public spaces. Interestingly, drones can be seen as widening the definition of public surveillance to include surveillance from public airspace, which, crucially, adds many non-public outdoor spaces to the publicly visible landscape. It is this enhanced definition that will be used in this study. Thirdly, I define "drones that are capable of public surveillance" as unmanned, non-tethered aircraft, including supporting systems on the ground, that can fly using an onboard means of propulsion; are remotely controlled by human pilots or self-controlled by onboard computers; and contain onboard

[4] It is distinct from casual yet focused people-watching to the extent that it is sustained over time. Furthermore, to conduct surveillance is not to pay attention to just anyone, but to pay attention to a *particular* person or group and for a *particular* reason.

sensor systems consisting of at least a visual-spectrum camera. I will not focus on any weapons capabilities of such drones.[5] Fourthly and finally, the "civil use" of drones refers to all of their *non-military* applications.

With regard to scope, let me make one more clarification. Since drones are an *emerging technology* that has yet to yield many of its devices, applications and societal consequences, it is helpful to focus on present *and potential future* developments and ethical issues in answering the research questions. Doing so prevents the analysis from quickly becoming outdated. I will therefore take potential future developments in drone technology and applications into consideration, with a time horizon set at the year 2030. In my view, this is neither a point in time too far into the future, which may raise reliability issues, nor is it a point that is too close to the present, which may decrease the predictive and prescriptive value of the study.

In addition to answering the above research questions, there is a set of secondary objectives to this study, which are to construct a proper methodology for the ethical evaluation of drone use through selecting, combining, critically evaluating, and possibly improving upon, existing ethical methods, and, where necessary, creating new methods. Among the methods that I include in my analysis are the *anticipatory technology ethics* approach by Philip Brey (2012); the *seven types of privacy* approach by Finn, Wright & Friedewald (2013); the *contextual integrity* approach by Helen Nissenbaum (2010); and the *proportional balancing* approach by Aharon Barak (2010).

This study can be seen as an exercise in *emerging technology ethics*, and also, to the extent that civil drones are and will increasingly become autonomous or semi-autonomous, as an exercise in the *ethics of robotics*. With regard to the nascent field of robot ethics, my analysis is mostly concerned with the question of whether, and to what extent, society at large should allow the use of autonomous civil drones. My focus in evaluating the use such drones is on weighing the general advantages and disadvantages of the *social-technical system* (involving the autonomous drones, their manufacturers, their users, policy makers, etc.) taken as a whole. I will not delve into the question of how *moral responsibility* for autonomous drone behavior should be distributed in the socio-technical context among manufacturers, users, policy makers, and perhaps even the drones themselves. Let me say, however, that as drones will become more autonomous this issue will become increasingly prominent and deserving of further analysis.

Finally, let me emphasize that since this study concerns ethical evaluations of an emerging technology, it has, by necessity, a rather large speculative and subjective component. Although the ethical evaluations in this study are performed in a conscientious manner and largely based on what I take to be generally accepted moral intuitions, others may hold somewhat different views and may arrive at conclusions that are equally valid but different from mine. At any rate, I believe my analysis contains some important insights that are crucial for a societal discussion on the ethical acceptability and future direction of drone technology.

[5] Civil drones for law enforcement purposes could incorporate weapons to incapacitate individuals and control crowds, such as long range acoustic devices that send out piercing sounds, high-intensity strobe lights that can cause disorientation, tasers that administer electric shocks, tear gas, and rubber rounds (Whitehead, 2010). Besides law enforcement, criminals and terrorists could also weaponize drones by (for example) using them to deliver an explosive charge. A proper ethical analysis of potential weapons capabilities and applications of civil drones would require an extensive study of its own.

Thesis outline

To conclude this introduction, let me offer a brief outline of what I will do in this study. To begin, in chapter 2, I will present an approach that I will use as an overarching methodology to identify and evaluate the potential ethical issues of surveillance-capable drones. In chapter 3, I will describe the present and potential future capabilities and civil applications of such drones so that these can be subjected to ethical analysis in later chapters. In chapter 4, I will describe and adapt two approaches to analyze the privacy issues of drone use, which will be used chapters 5 and 6, respectively. In chapter 5, I will *identify* all ethical issues for both *drone technology at large* and *specific types of drone*. In chapter 6, I will make general ethical *evaluations* for a small number of future *drone applications* upon identifying and evaluating the various ethical issues presented by these applications. In chapter 7, I will *evaluate* the ethical admissibility and importance of the ethical issues of both drone technology at large and specific types of drone. Finally, in the conclusion I will summarize my main arguments, evaluate the methods used in this study, and offer a number of policy recommendations as a way to start a discussion about the governance implications of my findings.

2 An approach to the ethical assessment of emerging technologies

As one ponders the main research questions of this thesis, the basic question arises: How exactly would one go about making an ethical evaluation of drones? More generally, one could ask: What is the most suitable approach for dealing with the ethics of a technology that is still *emerging*? Drone technology for civil use is currently at an early stage of development and use, and has yet to yield many of its devices, applications and societal consequences. The central problem with ethical assessment of technologies at the research and development (R&D) and introduction stages is that ethical issues relating to the use of these technologies cannot be identified or analyzed reliably, as their impact on society lies in the uncertain future: since an emerging technology is a technology *in the making*, we may not know all of its future applications, its precise character, and the ethical issues that will play out once it is fully developed and entrenched in society. We may speculate about these things, but as history has shown, speculations about future technology are often way off the mark, meaning that we may end up exploring a misguided or irrelevant set of ethical issues.

Nevertheless, there exist a few approaches that attempt to grapple with this epistemological problem of emerging technology ethics. The *anticipatory technology ethics* (ATE) approach by philosopher Philip Brey (2012) is one such approach. It is, as I will show, a conceptually and methodologically rich approach for making broad ethical assessments of emerging technologies, incorporating a large variety of ethical principles, issues, objects and levels of analysis, and research aims. In this study, I will use the ATE approach as an overarching methodology to identify and evaluate the potential ethical issues of surveillance-capable drone technology in a civil context.

This chapter has two sections. In the first section, I will describe Brey's ATE approach. Then, in the second section, I will briefly outline my motivations for choosing this approach, and I will explain how the approach is used as an overarching methodology to answer the main research questions of this study.

2.1 Brey's Anticipatory Technology Ethics

In a 2012 article, Philip Brey has presented anticipatory technology ethics (ATE) as a new approach for the ethical study of emerging technology (Brey, 2012). His approach is a type of *forecasting* approach that attempts to overcome the problem of future uncertainty through methodologically sound *forecasting* and *futures studies*, so as to better anticipate an emerging technology's future devices, applications, and social consequences. Brey has based his approach on a critical study of three contemporary approaches to the ethics of emerging technologies that use forecasting: *ethical technology assessment* (Palm & Hansson, 2006), the *techno-ethical scenarios* approach (Boenink, Swierstra & Stemerding, 2010), and the *ETICA* approach (Stahl, Heersmink, Goujon, et al., 2010). In constructing his own approach, Brey has built mostly on the ETICA approach. Let us consider the central features of Brey's approach.

One of the most important features of the ATE approach is that it employs three levels of ethical analysis: the *technology level*, the *artifact level* and the *application level*. At each of these levels, various *objects of*

ethical analysis are defined: things, properties or processes that raise ethical issues. Let us briefly explore these levels.

First, the *technology level*, according to Brey (2012), is the level at which a particular technology is defined, independently of any artifacts or applications that may result from it. A *technology* is "a collection of techniques that are related to each other because of a common purpose, domain, or formal or functional features" (p. 7). A *technique* is "a procedure to accomplish a specific activity or task" (p. 7). At the technology level, Brey argues, ethical analysis focuses on features of the technology at large, particular subclasses of it, or techniques within it. It considers generic ethical issues that are attached to these features. These can be ethical issues inherent to the character of the technology; issues that pertain to consequences that are likely to manifest themselves in any or nearly any artifact or application of the technology; or issues pertaining to risks that the technology will result in artifacts or applications that are morally problematic. As an example, Brey mentions a generic issue in genetic engineering, which involves the manipulation of DNA in cells and organisms; at the technology level, he argues, a generic ethical issue could be whether such manipulation violates the natural order things or the dignity of life.

Second, the *artifact level* is the level at which we focus on the functional artifacts, systems and procedures that are developed on the basis of a technology. Brey (2012) offers the example of nuclear technology, which has yielded artifacts like nuclear reactors, nuclear bombs, x-ray imaging systems and ionization smoke detectors. An *artifact* is defined as "a physical configuration that, when operated in the proper manner and in the proper environment, produces a desired result" (p. 8). A *procedure* is "a sequence of actions that, when performed in the proper manner in the proper environment using the proper tools, produces a desired result" (p. 8). At the artifact level, Brey argues, ethical analysis focuses on types of artifacts and processes that have resulted or are likely to result from a particular technology. Ethical analysis considers features of these artifacts and processes that present moral issues. As was the case at the technology level, such moral issues may present themselves for three reasons: because of the inherent character of the artifact, because the artifact has certain unavoidable consequences in most or all of its uses, or because certain potential applications of the artifact are so risky or morally controversial that the artifact warrants reflection on the ethical justification of its manufacture.

The *application level*, finally, is the level at which ethical analysis focuses on particular ways of using an artifact or procedure, or on particular ways of configuring it for use. An *application*, as Brey (2012) defines it, is "the concrete use of a technological artifact or procedure for a particular purpose or in a particular context, or a specific configuration of an artifact to enable it to be used in a certain way" (p. 8). At the application level, Brey (2012) argues, ethical analysis focuses on three groups of ethical issues. A first group consists of moral issues relating to the intended use of the artifact. They concern the morality of certain *purposes* for which an artifact or procedure may be used. An example here would be the use of morphine for mercy killing. A second group consists of moral issues concerning side-effects or unintended consequences for *users* that arise in certain uses, in certain contexts of use, or for certain user groups. A third group, finally, consists of moral issues pertaining the rights and interests of *non-user stakeholders* who may be affected by a particular use of an artifact.

Brey (2012) argues that at all three of these levels knowledge of the objects of ethical analysis is acquired through technological forecasting. Such forecasting includes the use of existing forecasting studies, expert panels and surveys, and self-performed futures studies. At the technology level, engineers may be the best positioned to inform the ethicist on likely future developments; at the artifact and application levels,

ethicists are generally better off analyzing existing studies in forecasting and technology assessment, as well as conducting expert surveys and roundtable discussions with experts.

Technological forecasting will result in descriptions of present and anticipated technologies, artifacts and applications, which constitute the input for ethical analysis. According to Brey (2012), there are two stages to such ethical analysis: a first one in which ethical issues are identified (the *identification stage*), and a second one in which they are evaluated (the *evaluation stage*). Optionally, at a third stage the results of ethical analysis may be used to make ethical recommendations for technology development or for governance.

At the *identification stage*, moral values and principles are *operationalized* and *cross-referenced* with technology descriptions resulting from the forecasting stage. The operationalization of moral values and principles is necessary to properly determine whether a particular technology, artifact or application may negatively impact on these values and principles. To operationalize a value or principle is to provide a description of this value or principle that specifies real-world conditions for its realization or frustration. The values and principles that are to be cross-referenced with the technology descriptions are derived from *ethical checklists* that include values that are widely accepted in society, as well as from the technology ethics literature and form bottom-up analyses. In his essay, Brey offers a checklist that includes *harms and risks* (health and bodily harms, pain and suffering, psychological harm, harm to human capabilities, environmental harm, harms to society), *rights* (freedom of movement, speech and assembly, autonomy, human dignity, privacy, property, as well as other basic human rights as specified in human rights declarations), *distributive justice* (including intergenerational justice), and *wellbeing and the common good* (e.g., supportive of democracy, culture and cultural diversity, happiness, desire-fulfillment, and so on).

At the *evaluation stage*, the potential importance of ethical issues that emerged at the identification stage is assessed, the likelihood of these issues becoming a significant issue in society, as well as their relation to each other, including potential value conflicts. Brey (2012) does not elaborate on how exactly such evaluations should be conducted. For example, he does not explain how the (relative) importance of ethical issues should be determined.

After the evaluation stage, there are, according to Brey (2012), various optional stages in which the results of evaluation are applied for various purposes. These may include a *design feedback stage*, a *responsibility assignment stage* (where moral responsibilities are assigned to different relevant actors), or a *governance stage* (where governance recommendations are made for policy makers on how to deal with the outcomes of the evaluation stage). This part of Brey's account, too, remains a little ambiguous.

2.2 Justifying the use of the ATE approach

As we have seen, Brey's (2012) ATE approach is a conceptually and methodologically rich approach for the ethical analysis of emerging technologies, which incorporates a large variety of ethical principles, issues, objects and levels of analysis, and research aims. Furthermore, it is ready to be applied to contemporary and future emerging technologies. I therefore consider it useful as an overarching methodology to answer the main research questions of this thesis.

The ATE approach offers several advantages over the other three main contemporary approaches to the ethics of emerging technologies (mentioned in the previous section)—*ethical technology assessment*, the

techno-ethical scenarios approach and the *ETICA* approach.[6] This is not the place to make a comprehensive comparative assessment of these approaches and the ATE approach, so let me suffice by briefly listing, without much elaboration, the main weaknesses of the other approaches in comparison to the ATE approach. Firstly, I support Brey (2012) in his assessment that the ethical technology assessment approach is somewhat vague in its methodology (in terms of how forecasting knowledge is acquired and how ethical analysis is performed on the basis of this knowledge) and that it offers an ethical checklist that is rather limited and not supplemented by further methods to identify ethical issues. Secondly, I also share his critique of the techno-ethical scenarios approach, which identifies ethical issues primarily though analysis of public moral controversies, rather than though thorough independent ethical assessments in which the identification of issues is not dictated by public debate. Finally, I agree with Brey that the ETICA approach—which has served as a model of Brey's own approach—is somewhat lacking in terms of its technological forecasting provisions, as its reliance on actual scientific methods of futures research is limited.

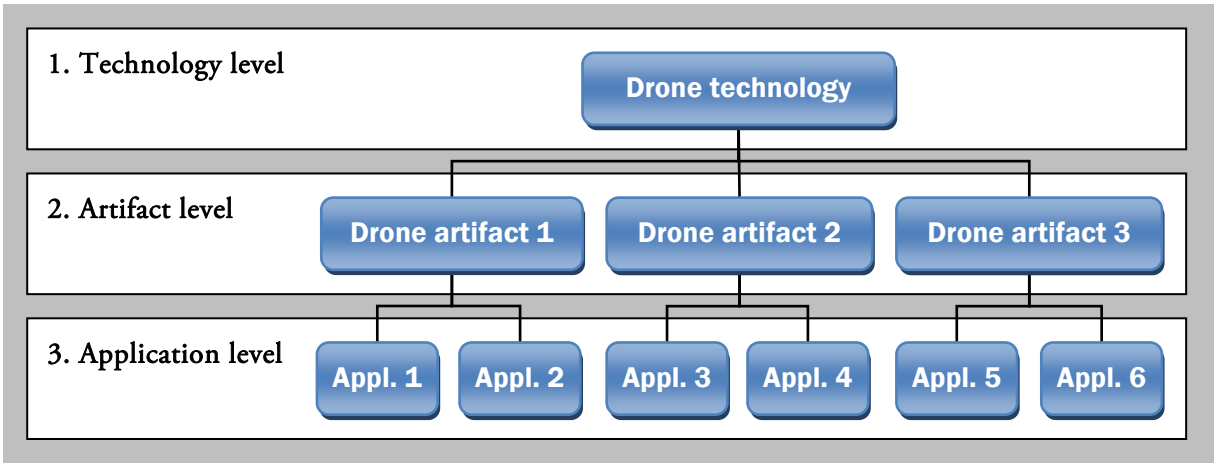

Figure 1: The three levels of ethical analysis of this study (adapted from Brey [2012])

On the basis of all this, I have decided to employ the ATE approach in this thesis. This means that I will analyze the civil use of surveillance-capable drones at three levels of ethical analysis: at the technology level, I will study *drone technology capable of public surveillance*; at the artifact level, I will consider *drone artifacts capable of public surveillance*; and at the application level, I will focus on *drone applications with public surveillance aspects* (see Figure 1). These levels allow for a very comprehensive analysis of civil drone use that includes the study of fundamental ethical issues pertaining to drone technology at large, as well as the study of more specific and contingent issues that depend on specific types of drone and specific applications. In an evaluation spanning all three levels of analysis, these levels can also be interpreted as a series of *substages* within the main stages of analysis (i.e., the forecasting, identification and evaluation stages) in which, starting from the technology level, specificity and contingency gradually increase.

There are a few ways in which I will expand the ATE approach and adapt it to the specifics of the case at hand. Firstly, at all levels of ethical analysis, my aims are to evaluate the importance of the ethical issues concerning surveillance-capable drone technology, artifacts and applications, as well as their ethical

[6] To be sure, there exist various other approaches to the ethics of (emerging) technology; however, none of these other approaches has a focus on anticipating a technology's future devices, applications, and social consequences through futures studies and forecasting methods. I believe such a focus is essential to conduct a proper ethical analysis of an emerging technology such as drones.

admissibility in civil contexts. However, it is not indicated in the ATE approach *how* such evaluations should generally be conducted. For example, it is not specified if and how we should "balance" conflicting ethical values during an evaluation. Therefore, in the course of this analysis, I will supplement the ATE approach with (elements of) other evaluative approaches, including one of my own. Secondly, to evaluate civil drone use at the *application level*, I will use one of these supplementary approaches (namely, Nissenbaum's [2010] privacy-centered "contextual integrity" decision heuristic) to both *identify* and *evaluate* ethical issues in one go. This means that, at the application level, I will depart from the basic structure of the ATE approach by combining the ATE approach's *identification stage* and its *evaluation stage* of ethical analysis. Doing so offers a number of advantages, as I will later explain. Finally, I should mention that I will not, in a meaningful way, conduct any of the optional stages in the ATE approach (i.e., a design feedback stage, a responsibility assignment stage, or a governance stage). Rather, I will offer some very brief and provisional policy recommendations in the conclusion of this study, mainly as a way to jumpstart a comprehensive future discussion about policy implications.

To conclude this chapter, let me offer a brief overview of how the ATE approach is used in this thesis from this point onwards. To begin, in chapter 3, I will conduct the technological forecasting stage with respect to future surveillance-capable drone capabilities and applications. The forecasting and futures methods that are used include environmental scanning, trend analysis, and expert interviewing. In chapter 4, I will operationalize the value of privacy, thus beginning the identification stage of the ATE approach. Privacy is very important in any ethical analysis of civil drone use and the concept has proven notoriously difficult to grasp, which is why an entire chapter is devoted to its operationalization. In chapter 5, I will identify the important ethical issues with regard to civil drone use at the *technology level* and the *artifact level* of ethical analysis by cross-referencing the forecasting information of chapter 2 with the operationalized value of privacy and other values and principles. In chapter 6, I will deviate from the ATE approach *at the application level* by using Nissenbaum's (2010) "contextual integrity" approach to conduct the *identification stage* and *evaluation stage* in one go. Here, the ethical admissibility is evaluated of a number of carefully selected drone applications from a set of application scenarios created for this study. Creating scenarios is not strictly part of the ATE approach, but is done to explain the context of some of the more ethically charged applications of civil drones. In chapter 7, I will conduct the evaluation stage at the technology and artifact levels. This means that the *importance* of the ethical issues concerning surveillance-capable drone technology at large and drone artifacts is evaluated, as well as the ethical *admissibility* in a civil context of the technology and the artifacts. Finally, in the conclusion, I will offer a number of policy recommendations, as well as a short evaluation on the use of the Brey's ATE approach in this thesis.

3 Present and future drone surveillance capabilities and applications

In order to ethically evaluate the use of drones that are capable of public surveillance, it is necessary to have information about the varied capabilities and applications of these systems. Since drones are an emerging technology that has yet to yield many of its devices, applications and societal consequences, it is not sufficient to look only at the *present* in this regard; potential *future* developments require attention as well. Therefore, in this chapter, I will conduct the technological forecasting stage of Brey's (2012) anticipatory technology ethics (ATE) approach. I will offer descriptions of present and anticipated civil drone surveillance capabilities and applications. These descriptions constitute the input for ethical analysis in the subsequent chapters. Anticipating the importance of the topic of privacy in this study, particular attention will be paid to the types of information that could be collected through drone surveillance, to the groups of people who could have access to the information, and to the purposes for which the information could be used.

As indicated in the previous chapter, to obtain the most reliable and diverse predictions of the future capabilities and applications of surveillance-capable drones, it is helpful to employ methods from the interdisciplinary field of *futures studies* or *futurology*. Futures studies are the systematic study of postulating *possible*, *probable*, and *preferable* futures and the assumptions that underlie these futures (Groff & Smoker, n.d.). The first section of this chapter will provide a brief description of the futures methods that have been used in this study.

In the three subsequent sections, I will describe the present and possible future capabilities and applications of surveillance-capable drones. In the descriptions, I will make an important distinction at the level of artifacts between three main categories of surveillance-capable drones: *large wide-area persistent surveillance drones*, *small general-purpose drones*, and *biomimetic spy drones*. This categorization is based on the similarities and differences among drones in terms of their surveillance capabilities. Each of the three sections focuses on the present and future capabilities and applications of a particular type of drone in a civil context. Section 3.2 focuses on persistent wide-area surveillance drones; section 3.3 centers on small general-purpose drones; and section 3.3 is about biomimetic spy drones.

This chapter ends with a short concluding section that summarizes the main findings of the forecasting stage. An overview of the capabilities and applications of the three categories surveillance-capable drones is offered in appendix B of this study.

3.1 Futures methodology

Drones are an emerging technology, which means that the technology is undergoing changes, often very rapidly. In the context of this study, it is essential to know about these changes; and the proper way to explore them is to engage in *futures studies* or *futurology*. Future studies are an increasingly important field of study. People will be living in a future world that promises to be different from today in very significant ways, and change—driven by technological development, globalization, and local decentralization—is happening at an ever faster rate. This has made it necessary for governments, corporations, militaries, and

other organizations to better understand the future, so as to have more influence over it. In the next three sections (sections 3.2, 3.3 and 3.4), futures studies methods have been used to map the future capabilities and applications of surveillance-capable drones.

Futures studies are about postulating *possible*, *probable*, and *preferable* futures and the assumptions underlying these futures (Groff & Smoker, n.d.). The aim of futures studies is not to know the future, but to generate *orientational knowledge* to manage the uncertainties that are inherent to future development (G&S, n.d.). In this study, the focus is on probable futures and *possible* futures (i.e., futures of which the occurrence is somewhat less likely), since in order to conduct a proper ethical evaluation of an emerging technology it is necessary to anticipate anything that has a reasonable likelihood of occurring. The typical time horizon of futures studies is five to fifty years; futures studies usually start at the point where the short-range disciplinary planning and forecasting tools end. The time horizon for this study is set loosely at 2030, or 15 years from now. In my view, this is neither a point in time too far into the future, which may raise reliability issues, nor is it a point that is too close to the present, which may decrease the predictive and prescriptive value of the study.

There are many different futures techniques.[7] According to prominent futurologist Raphael Popper (2008), there is no "ideal" methodological framework providing the "best" combination of methods. Popper merely offers a classification of futures methods based on their degree of reliance on four "sources of knowledge" about the future: *expertise*, *interaction*, *creativity*, and *evidence* (Popper, 2008). In order to obtain the most accurate and widest range of predictions, it would thus seem helpful to combine methods that complement one another in terms of these sources of knowledge. Other important considerations in the selection of futures methods are the investments in terms of time and effort (including knowledge and experience) that are required to properly apply them, which for some future methods would be prohibitively large in the case of this analysis.

On the basis of these considerations, three futures methods have been selected and used at the forecasting stage of this study. They are *environmental scanning*, *trend analysis*, and *expert interviewing*. Environmental scanning refers to the process of scanning the media across a wide range of sources to identify emerging developments, trends, and issues that enable organizations or individuals to anticipate and respond to changes in the external environment (Goertzel, n.d.). The sources of knowledge relied on in the application of this method mainly include *evidence* and *expertise*. I have used environmental scanning to analyze policy documents, defense reports, journalistic articles, company forecasts, and academic studies in forecasting and assessment of the potential future capabilities and applications of drone surveillance technology, as well as those of related surveillance technologies (such as CCTV). The information gained though environmental scanning has formed the backbone of the futures study in this chapter.

Trend analysis is an *evidence*-based futures method that projects past trends into the future for some given period of time. The technique is fairly straight-forward: first, something important is identified in the present; then, its historical development is traced back; and finally, the historic rate of development is cast ahead into the future to see what this reveals. One important trend in computing relevant to the analysis of domestic drones is *Moore's law*, which is the observation that chip performance doubles roughly every 18 months. Trend analysis assumes that the future will be an extension of past trends, which of course is

[7] For a comprehensive overview of different futures methods, see Popper (2008).

not always the case; trends will always come to an end. Moore's law, for example, is said to hold true only until 2022 (Hruska, 2013).

Expert interviewing, finally, is an *expertise*-based method that is frequently and variously employed in future studies. I have conducted a (mostly) qualitative interview with Pieter Elands, who is the program manager of the Unmanned Systems division at the Netherlands Organization for Applied Scientific Research (TNO; http://www.tno.nl/en/). The areas of expertise of Mr. Elands include "unmanned systems, integration and C[4]ISR"[8] (P. Elands, personal communication, December 1, 2014). The interview questions are provided in appendix A of this study. The results of the interview were used to verify, support and add to the findings of the environmental scanning and trend analysis activities.

It should be noted that the futures methodology used for this chapter is somewhat deficient in terms of its reliance on *interaction* and *creativity* as sources of knowledge about the future. Given the limited resources I had at my disposal for this study, I found it difficult to incorporate interaction-based and creativity-based methods (e.g., *expert panels*, *Delphi*, *scenario writing*), some of which are rather time-consuming and organizationally demanding. In addition, evidence-focused and expert-focused methods were given a slight priority over methods of other types, since methods that are grounded in evidence and expertise offer, in my view, the soundest basis for thinking about the future.

The integrated results of using of the above three methods to envision the future of surveillance-capable drones are presented in the "future capabilities" and "future applications" subsections of the next three sections of this chapter.

3.2 Drones category 1: Large wide-area persistent surveillance drones

Let us now turn to these results. *Large wide-area persistent surveillance drones* (large WAPS drones) are the first category of drones to be distinguished. These are large (vehicle weights of at least 20 kilograms), technologically advanced systems that have great endurance and offer so-called *persistent surveillance* capabilities over an extensive ground area. They share a military origin and their precursors have a long military history. Currently, these drones are mainly being deployed by military forces in conflict areas around the world, but they also have great potential for surveillance applications on the domestic front.

The term "persistent surveillance" is used by the U.S. Department of Defense (2005) to denote "a collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in near or real-time" (Dictionary of Military and Associated Terms, n.d.). The main advantage of persistent surveillance drones over manned aircraft includes this long-duration, loitering surveillance ability. In addition, they (potentially) also have lower procurement, operation and maintenance costs.

Currently, most large WAPS drones are powered, fixed-wing aircraft, such as the drone depicted in Figure 1 (on the next page). However, I also include in the present category large unmanned aircraft with WAPS capabilities that utilize other ways to generate lift and movement through the air, such as unmanned airships (which are a type of *aerostats*) and helicopters. As stated in the introduction of this chapter, the categorization of drones is based mainly on similarities in terms of their surveillance characteristics. In a more comprehensive study, however, these aircraft may be analyzed as separate artifacts to account for the

[8] C[4]ISR is the concept of *command*, *control*, *communications*, *computers*, *intelligence*, *surveillance* and *reconnaissance*.

effects of different methods of flight on the surveillance. Such a study may also distinguish between different size categories among large drones: a 20 kilogram Boeing Insitu ScanEagle, for example, has surveillance capabilities that differ considerably from those of a Northrop Grumman RQ-4 Global Hawk that weighs nearly 7000 kilograms—although the ScanEagle has persistent surveillance capabilities nonetheless. Still, I am confident that this crude grouping does not have an excessively negative effect on the ethical analysis conducted later on in this study.

In what follows, the present and future capabilities and applications of large WAPS drones will be discussed. Since these drones are (as yet) a largely military technology that is entering (or can easily enter) the domestic domain, much of the focus in terms of their present and future capabilities will be on military-type WAPS drones.

3.2.1 Present capabilities

One of the most significant recent developments leading up to the emergence of *wide-area persistent surveillance* (WASP) capabilities has been the introduction of large, medium- to high-altitude, long-endurance military reconnaissance and surveillance drones. The use of such systems as the MQ-1 Predator (depicted in Figure 2), the RQ-4 Global Hawk, and the MQ-9 Reaper in the U.S.-led wars in Afghanistan (2001) and Iraq (2003) has garnered a lot of attention. These sophisticated systems are being used to remotely conduct ground surveillance operations from altitudes of up to 20 kilometers, and, in the case of the Predator and the Reaper, neutralize ground targets with onboard precision-guided munitions. They have proven to be very successful on the battlefield in terms of completing missions against insurgents, and reducing casualties among U.S. military personnel. Their use in so-called "signature strikes", however, has sparked great controversy over the last few years, as these strikes have cost the lives of a considerable number of civilians mistakenly identified as insurgents.

Figure 2: An MQ-1 Predator.

These large military surveillance drones are controlled by pilots in so-called *ground control stations* (GCSs; see Figure 3). Satellite communication systems make it possible for a GCS to be located far away from a theater of operations. Furthermore, drones such as the Reaper can stay aloft for about 30 hours at altitudes of up to 15 km and cruise at speeds of about 300 km/h. Their sensor payloads may include high-

resolution video cameras and radar and infrared sensors. Data from these sensors can be distributed in real-time to locations around the world.

Figure 3: An MQ-1 Predator ground control station.

A key technology that is carried these days by some large military surveillance drones is the *wide-area motion imagery* (WAMI) sensor, which can capture extremely detailed footage of very large areas. As a key enabler of wide-area persistent surveillance (WASP), this technology greatly contributes to the ability of drones to conduct military reconnaissance and surveillance missions as well as surveillance operations in a civil context. The WAMI sensor consists of one or more large lenses and a spherical array of numerous small image sensors. The imagery produced by the individual sensors is automatically stitched together by powerful computers so as to form one big image, enabling users to have a "big picture" view instead of multiple "soda straw" views.

One WAMI system used in drones by the U.S. military is named *Gorgon Stare*. Its latest iteration features the *Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System* (ARGUS-IS). ARGUS-IS is a highly advanced camera and imagery analysis system that can capture and broadcast wide-area, ultra-high-resolution motion imagery, with each frame covering of an area 7,2 kilometers across (Heller, 2011). Reportedly, it can also track within this footage, automatically and for many hours at a time, a large number of individual moving objects, such as vehicles and pedestrians (see Figure 4, next page) (Heller, 2011). The system has four main components: a video sensor system, an airborne processing system, a ground processing system, and a data storage system. The video sensor system utilizes four lenses and 368 five-megapixel cell phone image sensors placed in a large mosaic. With this, it is able to capture very large 1,8 Gigapixel images at a rate of twelve frames a second (Heller, 2011).

Data processing capabilities become truly impressive when the ARGUS-IS is coupled with a computational system called *Persistics*. This system, which consists of sophisticated algorithms and novel computer architectures, is being developed for the U.S. military in response to some fundamental problems that exist with utilizing data generated by high-data-output video sensors (Heller, 2011). Currently, there is insufficient human and computer capacity to promptly and properly categorize, index,

annotate, and draw conclusions from the *petabytes*[9] of data that are collected daily by reconnaissance and surveillance drones. In addition, the communication bandwidth supporting data transmission from the drone to the ground and the archive storage capability are much too slow or too small to support fast-turnaround data analyses. Persistics is a data-processing "pipeline" that tries to tackle these overload issues. The system compresses motion imagery about a thousand-fold, while retaining the level of detail necessary for detecting anomalies (Heller, 2011).[10] Providing a means of compressing motion imagery so it can be efficiently transported is not all Persistics does, however. The system also offers advanced anomaly detection and behavioral analysis to differentiate between normal and abnormal patterns of behavior in traffic. Furthermore, it can detect and track, for hours at a time, thousands of objects simultaneously in the ARGUS-IS coverage area (Heller, 2011). Finally, the system can store all of the processed video footage for after-the-fact analysis.

Figure 4: An MQ-9 Reaper drone with the ARGUS-IS system and automated object tracking within the footage.

Analysts at ground stations can work with the transmitted imagery data in a variety of ways. Persistics has been integrated with a surveillance footage viewing application to allow analysts to pan, zoom, rewind, query, and overlay maps and other metadata. With the application, analysts can use Persistics to detect and track objects in real-time and engage in forensic analysis of past events—making such requests as "give me the trace data of this vehicle from one till two o'clock this afternoon", or "show me all the vehicles that stop at this location today". Persistics thus enables analysts to determine relationships between vehicles, people, buildings, and events.

ARGUS-IS and Persistics are just one example of a drone-mountable system enabling wide-area persistent surveillance; there exist a number of other WAPS imagery systems, of which a few are already being used for domestic law enforcement purposes in the U.S. The HawkEye II, by Persistent Surveillance Systems LLC, is one such domestically-used system. It features an aircraft-mountable pod containing an array of 12

[9] One petabyte is the equivalent of 1.000 terabytes or 1.000.000 gigabytes.
[10] By comparison, standard video compression techniques can at best achieve a 30-fold reduction (Heller, 2011).

commercially available cameras which together are capable of taking color images of 192 Megapixels—which are about a tenth the size of images taken by ARGUS-IS. The pod can be mounted on large drones, although for legal reasons it has thus far only been used on manned aircraft.[11] The HawkEye II can cover a 64-square-kilometer area with a resolution of about half a meter. The system takes one picture per second and generates 1,29 Terabytes worth of footage over a flight period of six hours. Figure 5 offers an impression of how the system is used.

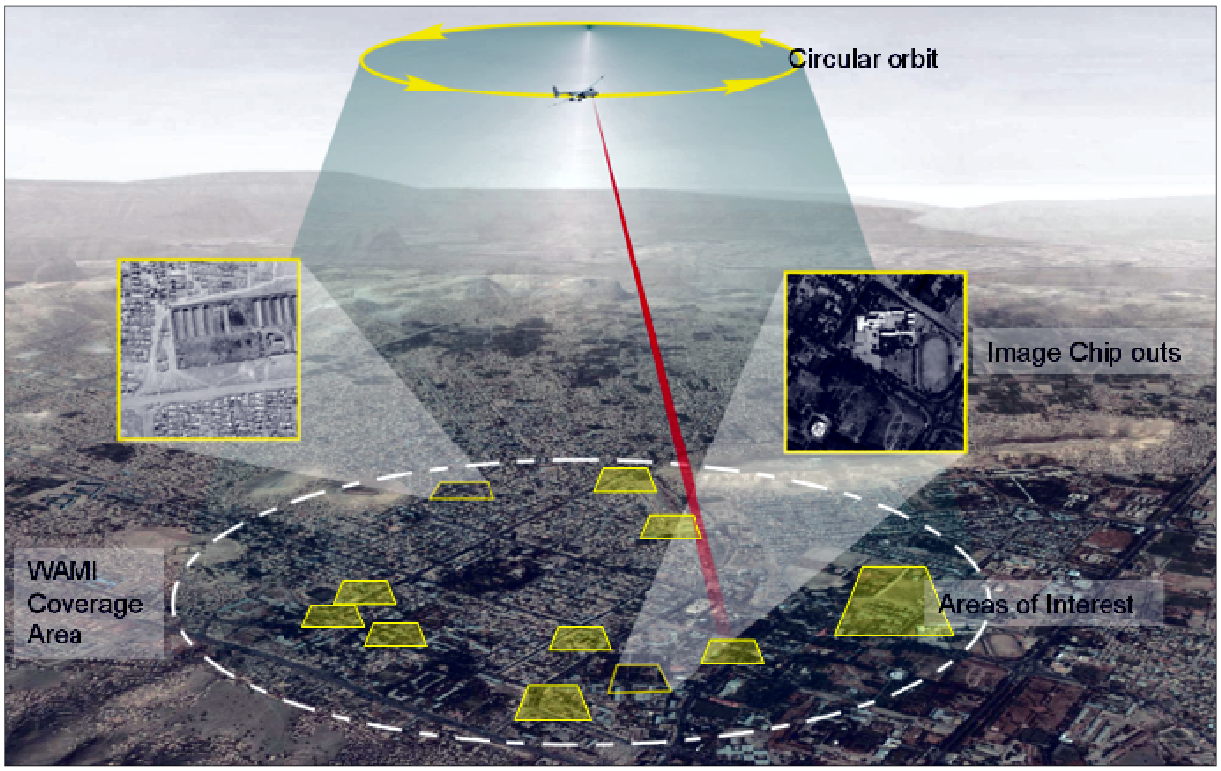

Figure 5: The HawkEye II system being used over a city.

On the images taken by the HawkEye II, each person appears as a single pixel and is, without contextual information, indistinguishable from another. Looking at the imagery, it is also hard to see what it is precisely that people are doing. With the HawkEye II, every person and vehicle across an area the size of a small city can be tracked on live or recorded footage, for many hours at a time. This tracking is to be done manually. Combined with information from other sources, the tracking data can provide a wealth of information that law enforcement and other users can use to identify people and their activities.

3.2.2 Future capabilities

Visible-spectrum WAMI sensors used on drones have shown dramatic improvements over the last decade, going from an image resolution capability of 4 Megapixels in 2003, to 176 Megapixels in 2007, to 800 Megapixels in 2009, and finally to 1,8 Gigapixels in 2013 (Heller, 2011). Developers of these sensors have been exploiting the exponential growth in image resolution capabilities of commercial imaging sensors (Kopp, 2011). Sustained growth in this area combined with the development of sophisticated sensor array designs will enable the trend towards higher-resolution wide-area imaging sensors to continue in the near future. Increases in resolution can be used to increase the area coverage and the precision of the imagery.

[11] The reason for this is that the U.S. Federal Aviation Authority has put severe restrictions on the flying of unmanned aircraft in domestic airspace.

When precision is enhanced, objects such as vehicles are more detailed and thus more easily identifiable. There are limits, however, to the growth of these resolution capabilities. Limiting factors are, for example, the lenses that are used (Kopp, 2011). The sharpness of lenses has not been growing exponentially, and might not be able to keep up indefinitely with the resolution capabilities of the imaging sensors. Moreover, despite the resolution enhancements, identifying people from a single image will remain difficult, as faces are hard to make out from a position that is more or less directly overhead.

In the future, large domestic WAPS drones will have a variety of different sensors. At present, military variants already feature high-resolution visible-spectrum WAMI, night vision and still cameras, as well as thermal imaging and radar sensors. In the future, it may be common for domestic WAPS drones to have *multispectral* and *hyperspectral* sensors, which collect information from across the electromagnetic spectrum for purposes of finding objects, identifying materials, and detecting chemical processes (P. Elands, personal communication, December 1, 2014). Remote airborne hyperspectral imaging may, for example, be used to detect cannabis plantations in gardens. Radar sensors may also be used, which allow vehicles to be tracked at night and in adverse atmospheric conditions (Sánchez-Oro, Fernández-López & Cabido, 2013).

In the future, the sensor data analysis systems of WAPS drones will improve as well. The computational power powering them may increase at the exponential rate described by Moore's Law, which predicts that chip performance will double every 18 months. It has been argued, however, that Moore's Law will only hold true until about the year 2022, after which chip performance gains will slow down considerably (Hruska, 2013). The projected increases in performance will shrink the size, weight, and power (SWaP) requirements of systems such as Persistics and allow them to be mounted onboard WAPS drones in the next couple of years (P. Elands, personal communication, December 1, 2014). The benefit this brings is that it removes network bandwidth as an important limiting factor in data analysis capabilities. Besides improvements in terms of SWaP, there will also be improved capabilities in terms of additional and more robust data analysis algorithms. Tracking algorithms are expected to become "context-aware", which means that they can determine a target's "pattern-of-life" by recognizing specific behaviors through its interactions with its surroundings or network (Gao, Ling, Blasch, et al., 2013).

The flight duration of large WAPS drones will also increase in the future. Large drones in the Zephyr family of solar-electric-powered drones, currently developed for the U.K. military, will be able to fly at high altitudes for up to 82 hours (Airforce-technology.com, n.d.). Some large solar-powered drones might fly for months, or years at a time (Schechter, 2013).

The capabilities of drones to identify, track, and analyze the behavior of people may be enhanced by the creation of connections with other information systems. Improved ICT infrastructures may make it easier to establish such connections. Roadside CCTV systems featuring visual recognition algorithms could identify motorists by the license plates of their vehicles and enable a WAPS drone to persistently track the movements of identified motorists.

Finally, WAPS drones will have a greater degree of autonomy in the future. The field of drone autonomy is an emerging field that is largely going to be driven by the civil domain (P. Elands, personal communication, December 1, 2014). Sensor data analysis and communication will, as has become clear, involve a great deal of autonomy on the part of the drone. Other areas of autonomous behavior development will be vehicle path and motion planning. Important here are sense-and-avoid systems,

which prevent mid-air collisions with other aircraft. Higher level processes, such as task allocation and scheduling, are the hardest to make autonomous, and autonomy in this area will develop more slowly.

3.2.3 Present applications

Domestic public surveillance is an emerging field of drone applications. Large WAPS drones are being used for this purpose because they compare favorably to manned aircraft in terms of flight endurance, stealth and operating costs. Public surveillance applications of WAPS drones and video systems have thus far mainly included border surveillance, crime investigation, and crowd monitoring at large public events.

In the U.S., the Customs and Border Protection agency (CBP) has been using a number of Predator drones to monitor U.S. borders and catch illegal immigrants and drug smugglers (Booth, 2011). North Dakota local police, the Federal Bureau of Investigation, the North Dakota Army National Guard, the Texas Department of Public Safety, and the United States Forest Service, among others, have also fielded the CBP's Predator drones, using them for such things as investigating crimes, searching for missing persons and inspecting levees along the Mississippi River (Sengupta, 2013).

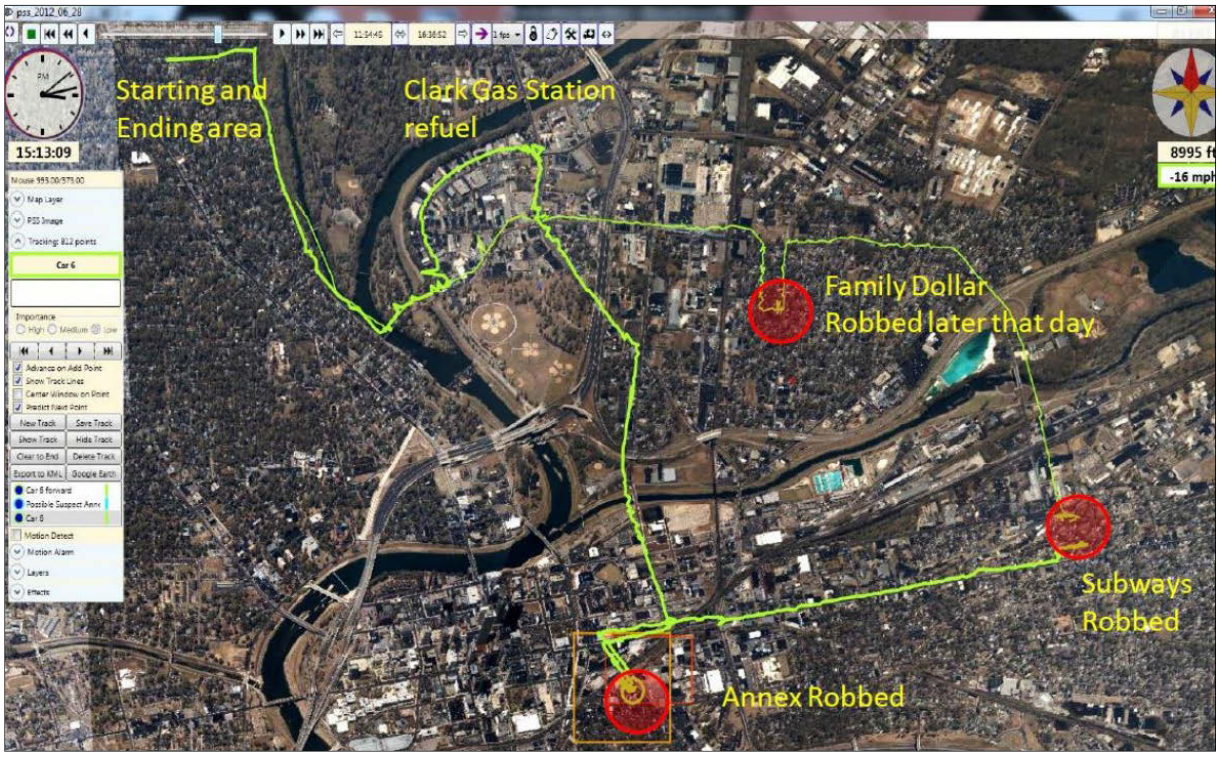

Figure 6: A robbery suspect tracked to robbery locations and area of residence.

The HawkEye II WAPS video system has also been deployed domestically over cities in the U.S. and Mexico. Manned aircraft were used for the deployments, but drones could very well have been used had the FAA's regulations not prohibited this.[12] The system has been used for such things as crime-surveillance and investigation over urban areas, traffic impact studies, and security surveillance at NASCAR races. During operations to assist local law enforcement in the U.S. city of Dayton, Ohio, it has helped in the monitoring and investigation of major crimes and events, and it has reportedly seen some success in that

[12] Although the HawkEye II WAPS video system has only been flown on manned aircraft, the only thing preventing its use on drones in the U.S. is the FAA's restrictions on unmanned flight. I therefore believe it is appropriate to discuss the current applications of this system here.

regard. About the system's effectiveness, Dayton's chief of police has said: "We found their systems and services to be a significant asset to our officers to detect and investigate criminal events. It is my belief that through consistent use, this system will ultimately reduce and deter crime" (Farivar, 2014).

When a major crime is reported, analysts working for PSS (the company exploiting the HawkEye II) will review the recorded footage of the scene and present police detectives with a detailed incident report (Figure 6 on the previous page provides an illustration). PSS has made rules for itself on how long data can be kept, when images can be accessed, and by whom they can be accessed. The company does not allow the police to conduct fishing expeditions using its system: police personnel are to begin looking at the footage only after a crime has been reported.

3.2.4 Future applications

Of course, these self-imposed restrictions to safeguard privacy may not deter other companies and government agencies from expanding the reach of WAPS applications. With a system such as SkyHawk II, analysts could technically engage in indiscriminate covert surveillance. They could silently track, in real-time, the movements of anyone in the streets and private outdoor areas such as gardens, and make inferences about his or her activities. People who are well-known, either by the analyst or in general, or people who are conducting activities which seem unusual, could become prime targets.

As WAPS drones become cheaper to operate, they could be used in mundane police work and could (partially) supplant other forms of surveillance. In the future, for example, it may not be necessary for police officers to physically patrol the streets of dangerous neighborhoods, thus perhaps saving public funds and reducing the risk of injury for police officers.

With ARGUS-IS and Persistics, domestic applications of WAPS drones would expand further. A system composed of both has a larger coverage area and provides a sharper image than the SkyHawk II does. In addition, it has automated instead of manual object tracking, which makes the analysis of footage much less labor-intensive. It would allow law enforcement agencies to conduct a very efficient and deep-reaching form of "dragnet" surveillance, especially if it is combined with other surveillance systems such as road-side traffic cameras that can read license plates. This type of surveillance could suit basic policing as well as national security purposes.

In addition to forensic analysis and real-time suspect-tracking, there will be significant predictive analysis applications of WAPS systems with behavioral analysis algorithms. These algorithms will automatically alert analysts to potentially suspicious activity in a section of the vast field of view. Suspicious activity could involve nervous loitering, sudden crowding, repeated drive-bys, et cetera. When alerted, the analysts may monitor the scene to figure out what the individuals in it are up to, possibly using other surveillance systems such as nearby CCTV cameras or *small drones* (see the next section) that can provide a more detailed view. If the situation is potentially serious, they may report it to law enforcement.

Finally, WAPS drones may not only be deployed by law enforcement agencies: one can also imagine commercial uses for these systems. For example, a company such as Google Inc. might use them one day to provide a real-time Google Maps service to its customers. Such an application could enable ordinary citizens to track each other's movements in urban public spaces.

3.3 Drones category 2: Small general-purpose drones

Now that the capabilities and applications of the WAPS drones have been described, it is time to discuss the second category of drones. This second category may be called *small general-purpose drones*. With weights in the order of kilograms, these drones are much smaller than the large WAPS drones. In general, they lack the range, the speed, the wide-area perspective, and the sophisticated sensor payload of their larger cousins. They are, however, significantly cheaper and easier to procure, operate, and maintain, and can observe and record scenes in high detail from up close and from many different angles—all of which makes them highly versatile.

Figure 7: A small fixed wing drone.

Two main types of small general-purpose drones can be differentiated: the first has a fixed-wing design (see Figure 7) and the second a rotary blade design (sUAS News, 2013) (see Figure 8, next page). The fixed-wing systems are ideal for such things as undertaking topographic surveys where relatively large areas need to be covered. The rotary blade systems, on the other hand, are suited for such things as detailed inspection of bridges where there are many hard-to-reach spaces. Unlike the fixed-wing models, the rotary drones are able to fly in any direction and hover in a fixed position. Since small drones of the latter type make up the majority of drones that are and will be used in congested urban spaces—where their surveillance capabilities arguably have the most impact—this section will largely focus on this type of small drones.

Before we begin the analysis of the capabilities and applications of small general-purpose drones, it again deserves to be noted that the categorization of drones in this study is based mainly on similarities and differences in terms of their surveillance characteristics. In a more comprehensive study, fixed-wing and rotary blade drones may be analyzed as separate artifacts to account for the effects of different methods of flight on the surveillance. Such a study may also account for small drones that combine elements of a fixed-wing and a rotary blade design, as well as small aerostats.

Figure 8: A small rotary blade drone.

3.3.1 Present capabilities

Rotary blade drones tend to be a little smaller in size than their fixed-wing counterparts. A highly popular rotary blade drone design is the *quadcopter* which is lifted and propelled by four rotor blades (the drone in Figure 8 is a quadcopter). Other popular rotary blade designs are the (often larger) *hexacopters* and *octocopters*. Most quadcopters do not weigh more than a few kilograms and have width, length and height dimensions of that make them very portable. There is much variation among small drones in terms of cost and capabilities. This section will largely focus on the capabilities of drones at the higher end of the capabilities spectrum so as to give a good impression of what will technically be possible, now and in the future.

Since the maximal weight of their sensor payload is limited, small drones have sensor capabilities that are necessarily less impressive than those of their larger relatives. The largest top-of-the-line quadcopters used for surveillance purposes feature cameras that have the same capabilities as powerful hand-portable digital cameras. They can often shoot still images with resolutions upwards of 15 Megapixels and video footage in high-definition (1080p) format or better, both with zoom lenses offering "50x" magnification or more. Provided vibration control systems are of sufficient quality, these drones can be very formidable in terms of observing scenes in high detail over relatively large distances. From a low-observable position one hundred meters away, some are able to capture people's faces with such detail that they are easily identifiable. Besides video and still cameras, quadcopters can feature a host of other sensors, including light-weight multispectral, thermal, and night vision imaging sensors.

Small drones, especially those with rotary blades, are very useful for statically observing things that are better seen from an oblique perspective than from a position overhead. Examples are scenes where structures block an overhead view and scenes where persons need to be visually identified (through facial recognition). Rotary-blade-based drones can continuously view a scene from any vantage point in the air.

Their ability to position themselves in relatively close proximity to their target enables them to record images of a scene that are more detailed than those of WAPS drones.

Just as there is a limited sensor payload that small drones can carry, onboard sensor data analysis systems are also limited due to weight constraints. Computationally demanding tasks such as tracking multiple objects are done by computer systems on the ground.

Small rotary-blade-based drones have excellent flight capabilities. They are inherently unstable aircraft, but sophisticated algorithms controlling the speeds of the four propellers make them very stable, quick and maneuverable nonetheless. Furthermore, they need no runway since they are able to take off and land vertically, and operating them generally does not require much piloting experience. However, since they are powered by Lithium-ion batteries, they are only capable of short duration fight. The largest quadcopters can fly on average for 25 to 40 minutes (The Quad Cops, 2014). Further, most small drones can only be piloted within the line of sight—although high-end systems feature map- and GPS- based navigation systems that allow them to be controlled beyond the line of sight and in low visibility conditions (The Quad Cops, 2014).

When using silent brushless motors, quadcopters are fairly quiet during flight, which enables them to operate with some level of stealth. Camouflage colors and their ability to loiter in low visibility spaces, such as in or behind tree foliage, also contribute to their stealth ability.

Small drones may express a limited degree of autonomous behavior. Some drones are able to follow a programmed flight path or Bluetooth beacons. Some are also self-monitoring and self-adjusting, handling battery levels, in-flight wind speeds, and other system and environmental conditions on their own, and (upon reaching user-configurable limits) returning home and landing automatically.

3.3.2 Future capabilities

Quadcopters, hexacopters, and octocopters will likely remain popular designs for small drones operating in the urban environment. In the future, their basic capabilities will improve while they become ever smaller and cheaper. This is largely because important components of these drones are also used mobile phones and are getting better and cheaper due in part to the enormous scales at which the mobile phone industry operates (Anderson, 2014). From a technical perspective, it is plausible that rotary blade drones will be a very widely accessible technology in the future.

The imaging capabilities of small cameras used in small drones will improve rapidly in the future. As stated in section 3.2, the exponential growth of the image resolution capabilities of commercial imaging sensors is likely to continue. Current micro-electronics manufacturing technology has made sensors with one billion pixels within reach (Cossairt, Miau & Nayar, 2011). In addition, crucial advancements in lens technology have recently been made. Columbia University scientists have presented a proof of concept of a novel optical design for Gigapixel imaging in handheld cameras (Cossairt, Miau & Nayar, 2011), and Duke University researchers have stated that they believe that the first generation of Gigapixel cameras should soon be available to the general public (Woollacott, 2012). For comparison: As of now, professional handheld digital cameras have maximum resolutions of up to 50 Megapixels.

Future small drones will have additional sensor capabilities. They could be equipped with radar-based sensor systems that can “see” through walls (Thomasnet.com, 2013). Such radar-based systems would enable the tracking of individuals in foggy conditions, through foliage, and inside buildings (Research

Group of the Office of the Privacy Commissioner of Canada, 2013). Also, they may use remote hearing systems such as *laser Doppler vibrometers*, which use *laser interferometry* to make faint sounds like human speech interpretable over great distances (Qu, Wang & Zhu, 2009).

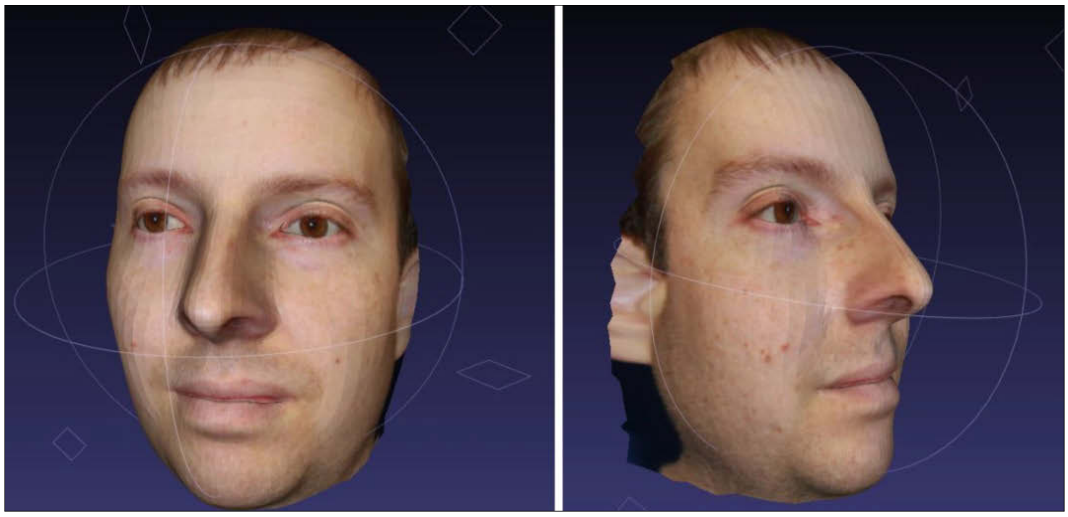

Figure 9: A 3D model made for facial recognition in surveillance footage.

In the future, the sensor data analysis systems of small drones—especially those intended for surveillance purposes—will also continue to improve. Their computational power is likely to follow Moore's Law in the near future and will support advanced computer vision capabilities such as facial recognition. Working on a drone-mounted biometric identification and tracking system, a U.S. company is currently developing algorithms that can construct a 3D model of a person's face from a single high-quality two-dimensional image (Shachtman, 2011; see Figure 9). Using the 3D model, the system can recognize faces in any pose, with any expression, and in any lighting, thus being able to track people persistently across wide areas (Shachtman, 2011). The system also has another way of identifying individuals: using a series of so-called "soft biometrics", such as age, gender, skin color, height and weight, it can keep track of targets at ranges of 225 meters or more. Considering that camera resolutions will keep improving at a fast pace, it is clear that the identification over people over large distances will be a basic capability of small surveillance drones in the future.

Work is also underway on an innovative system for obtaining threat assessments of individuals and groups based on their likely intentions (Shachtman, 2011). The system integrates data from drone footage, informants' tips, and intercepted phone calls and then applies advanced human behavior modeling and simulation algorithms to the combined data.

Another interesting computer vision technique is called Eulerian Video Magnification (Durand & Freeman, 2012). This technique has been developed to amplify small changes in video imagery, such as small movements or changes in color. It has been used to take an individual's pulse by greatly amplifying the rhythmic flushing of the individual's face, and to track an infant's breathing by exaggerating the movement of the infant's chest. It is not a stretch to assume that this technique could one day be used in surveillance systems to determine, for example, whether a suspect person is nervous of not. (To be sure, nervousness by itself is not indicative of malicious intentions.)

A final development in the realm of sensor data analysis systems that deserves mention is the research on a system that can determine, for many individuals simultaneously and from low resolution color surveillance

footage, in which direction they are looking (Reid, 2009) (see Figure 10). Naturally, situations where many people are suddenly gazing at someone or something could be of interest to surveillance operators.

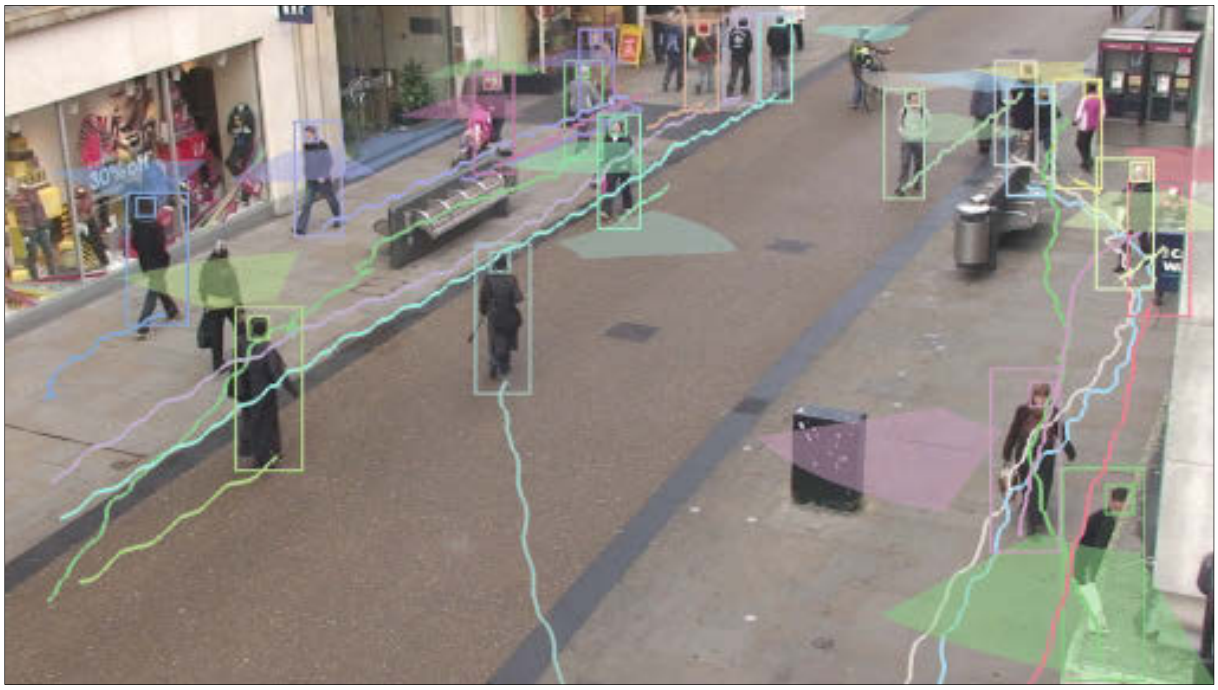

Figure 10: Gaze direction recognition in surveillance footage.

In terms of flight capabilities, too, small drones will continue to improve. Miniaturization and new battery technologies, such as fuel cell battery technology and perhaps laser wireless recharging technology, will greatly lengthen the flying times of small drones. A prototype 17-kilogram fixed-wing drone powered by fuel cells has already managed to stay aloft for almost 24 hours on a single fuel load (Fox, 2009). And tests with a small electrically-powered drone and a long-distance wireless recharging system that uses a high-power laser allude to the theoretical possibility that drones can stay in the air for unlimited periods of time (Brown, 2012). Further, it will become easier to operate small drones as vocal and gesture control technologies are being developed (Thalen, 2013).

Finally, drones will have a greater degree of autonomy in the future. Sensor data analysis will, as has been explained, involve a great deal of autonomy on the part of the drone. Other areas of autonomous behavior development will be vehicle path and motion planning. The majority of drones will have the ability to fly autonomously by GPS waypoints and feature sense-and-avoid systems that perhaps use echolocation and microradar, which will help them to sense obstacles and avoid collision (Insinna, 2014). Work is also underway on intelligent drone swarming. Flocking algorithms have already been created that enable quadcopters to self-organize as they move through the air, tracking targets together while keeping formation and avoiding collisions (Vásárhelyi, Virágh, & Somorjai, et al., 2014). Intelligent swarms of small drones could in the not-too-distant future be used to efficiently and effectively conduct surveillance operations. Furthermore, they could themselves be part of larger, highly interconnected surveillance networks that could include WAPS drones as well.

3.3.3 Present applications

Small drones have numerous domestic applications. They are used professionally by public and private sector users in such fields as aerial photography, geo-mapping, agriculture, industrial infrastructure monitoring, wildlife monitoring, firefighting, meteorology and climatology, search and rescue, and policing. To be sure, this is only a small selection of the ever-growing list of application areas. Their deployment is often preferred because it is significantly cheaper, faster, easier and safer than many alternative practices. In various countries, however, their non-recreational use is currently severely restricted for public safety reasons by order of national aviation authorities. Applications of small drones that have significant public surveillance aspects will now be discussed for public sector, private sector, and recreational use categories.

In the public sector, applications of small drones with significant public surveillance aspects are primarily by law enforcement agencies. Police forces around the world have varyingly been using them for purposes such as traffic accident investigations, forensic investigations, search and rescue, tactical operations, emergency and disaster response, crowd monitoring, and hazardous materials management.

Although drone use in the private sector has significant restrictions imposed on it by many national aviation authorities, there currently are various commercial users of small drones with applications that have surveillance aspects. Many drone operators are offering "surveillance" services and list infrastructure firms, insurance companies and council planning departments among their clients (Merrill & Troen, 2014); private investigators have used small drones to locate property hidden in a person's backyard (Surveillance Specialist Group, n.d.); some news agencies have used them for investigative reporting (Corcoran, 2012); paparazzi journalists have used them to spy on the rich and the famous (Evans, 2014); several real-estate firms have used them to photograph properties from an aerial perspective (Wingfield & Sengupta, 2012); and German logistics company Deutsche Post AG is starting to use them for the delivery of supplies to a small island in the North Sea (AFP, 2014).

Small drones are also being used non-commercially for recreational and hobbyist purposes. Recreational use is fairly extensive compared to public and private sector use due to the affordability of entry-level camera-equipped drones and the fact that laws applying to recreational drone use are very lenient in many countries. Recreationally, small drones may be used for outright spying, or purposes that at least violate a person's rights such as privacy to a degree. A neighborhood snoop can instruct a small drone to hover in front of a 10th-floor apartment window and take pictures of someone's private dwelling. Such a drone may further be used by a film and photography enthusiast to capture footage of a public recreational area, all the while recording many unsuspecting people in the area without their consent. Finally, a political activist or citizen journalist may fly a drone low over riot police lines to record clear bird's-eye-view images of a violent demonstration (ABC, 2012).

3.3.4 Future applications

In the future, the use of drones is likely to grow rapidly. The FAA estimates that in the skies over the U.S. as many as 30.000 drones could be flying by 2020 (Federal Aviation Administration, 2014). The majority of these would qualify as small drones. With the rise in numbers, new applications will emerge that will likely have a significant impact on society. The following is a discussion of the potential future public

surveillance-type applications of small drones for public sector, private sector, and recreational use categories.

For the public sector, one can imagine applications by government agencies, which may include police departments, national security agencies, taxation offices, and waste management offices. In the future, these users may be allowed to deploy small drones in the urban environment once sense-and-avoid technology has improved enough. Law enforcement agencies may deploy swarms of small semi-autonomous drones that act as a mobile CCTV system of sorts. Small drones may be able to perch on rooftop edges to secretly monitor crowds, and pursue targets through the air, which powerful facial recognition systems identify for them. Law enforcement can also be imagined using drones to patrol stretches of highway and to monitor environmentally protected lands. Furthermore, they might use small drones for targeted intelligence gathering during criminal investigations, perhaps by secretly peeking through the windows of a suspect's residence from a convenient vantage point in the air. Also within the public sector, tax agencies may use small drones to look for such things as undocumented property improvements, which would indicate tax fraud. Finally, environmental protection offices may use drones for such purposes as flying over residential neighborhoods to see if environmental laws are being broken by residents.

It is conceivable that there will be a high degree of integration between small public surveillance drones and other security and information systems. Connections could be established with national biometric and social networking databases, enabling small drone systems to identify almost anyone within their field of view. Also, with algorithms designed to identify unusual behavior, there will be a shift from forensic analysis towards predictive analysis, or before-the-fact policing (Iannotta, 2013).

Commercial drone use is expected to expand rapidly from the moment national aviation authorities integrate drones into national airspaces. The U.S. Federal Aviation Authority seeks integration in U.S. airspace by late 2016 or early 2017 (Hughes, 2015). Existing commercial applications will evolve and many new ones can be expected to emerge. Among the many future applications, there are a few that may harbor significant surveillance aspects. An increase in the use of drones for journalistic purposes has been predicted (Flock, 2012). Also, skies may soon be teeming with camera-equipped delivery drones, as companies such as Deutsche Post AG, Google Inc. and Amazon.com Inc. are eagerly exploring the drone courier concept (Weiss, 2014). Furthermore, security companies may largely switch to drones for their patrolling and crowd monitoring activities; insurance agencies may deploy drones to help them evaluate property damage on-site (Johnson, 2014); and television and film industries may use them to shoot and broadcast breath-taking aerial footage for television shows, advertisements, and movies. Finally, small drones could be used for a few rather pernicious purposes such as industrial espionage.

Future recreational and hobbyist uses may include applications that already exist, which may evolve and grow more popular, as well as new applications. Current practices, such as snooping, amateur filmmaking, and journalistic reporting, are likely to expand in the future. It is speculated that inexpensive small camera-equipped drones may generate a power shift between governments and civilians, hence becoming a "civic equalizer", as they are giving ordinary citizens new means to expose deceptive and illicit behaviors by governments, corporations, and other powerful entities (Greenwood, 2014). Also, they may become a powerful tool for civilians to document civilian-on-civilian crime (Greenwood, 2014).

Finally, one new reality that may emerge as the skies fill up with small drones is the hacking of these systems. The aircraft have a fundamental weakness in that hackers can hijack them through their wireless communication links and their GPS signal receivers (Moskvitch, 2014). Malicious individuals could hack delivery drones to steal their cargo, the expensive machine itself, or even to engage in black-market activities, such as transporting narcotics (Moskvitch, 2014).

3.4 Drones category 3: Biomimetic spy drones

Now let us move to the third and final drone category, which may be called *biomimetic spy drones*. Drones of this kind are very small and inconspicuous and perfectly exemplify the trend of miniaturization. Moreover, they answer the U.S. military's demand for very small drones that can "hide in plain sight" through mimicking the size and behavior of insects and birds (Kelley, 2013). The ability to go unnoticed will greatly help in their use for covert surveillance applications. Not only will the use of biomimetics lead to benefits in terms of stealth, however; it will also lead to better overall designs, for example in terms of energy efficiency.

Currently, biomimetic drones do not have practical uses outside the laboratory environment. Many are still at the prototype stage, their real-life application being hampered by design challenges that will take some time overcome. Biomimetic robots, however, have a bright future, according to future-warfare expert Peter Singer (2009): "The robots you know tomorrow are going to look like nothing you know today. More likely, they will look like the animals around you."

3.4.1 Future capabilities

The biomimetic spy drones that are currently in development are being designed to look like, have the size of, and replicate the flight mechanics of birds and insects such as moths, dragonflies, herring gulls, and hummingbirds, but also even of such creatures as jellyfish (BBC, 2014). One difficulty in creating these drones lies in developing "flapping wing" technology, or recreating the flight mechanics of natural winged flight (Lee, 2014). A bigger problem is the limitation imposed by current battery technology on their flight duration, which is often only a few minutes (P. Elands, personal communication, December 1, 2014). It will likely still take many years before small biomimetic drones have achieved a level of development that will allow them to serve real-world purposes.

One of the most sophisticated biomimetic drones that is currently in development and has been prototyped is the Nano Hummingbird by U.S. defense contractor AeroVironment Inc. (see Figure 11 on the next page). This drone is modeled after a hummingbird. It has a 16,5-centimeter wingspan and weighs only 19 grams. It can fly vertically and horizontally, hover in place against gusting wind, and perch on a windowsill. In spite of its small size, it carries a low resolution color video camera, wireless communications systems, and a power source (Piore, 2014), which gives it a flight time of about eight minutes (Hennigan, 2011). Another biomimetic drone that is being developed is the Dragonfly, by the company TechJect (see Figure 12 on the next page). This drone, which has yet to be fully prototyped, looks much like a real dragonfly and will feature high-definition video and wireless communication (Hennigan, 2011).

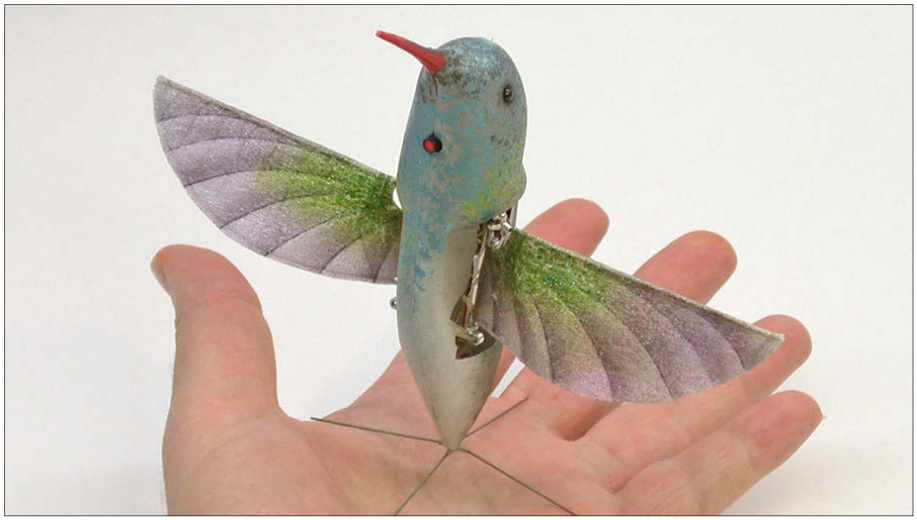

Figure 11: AeroVironment's Nano Hummingbird.

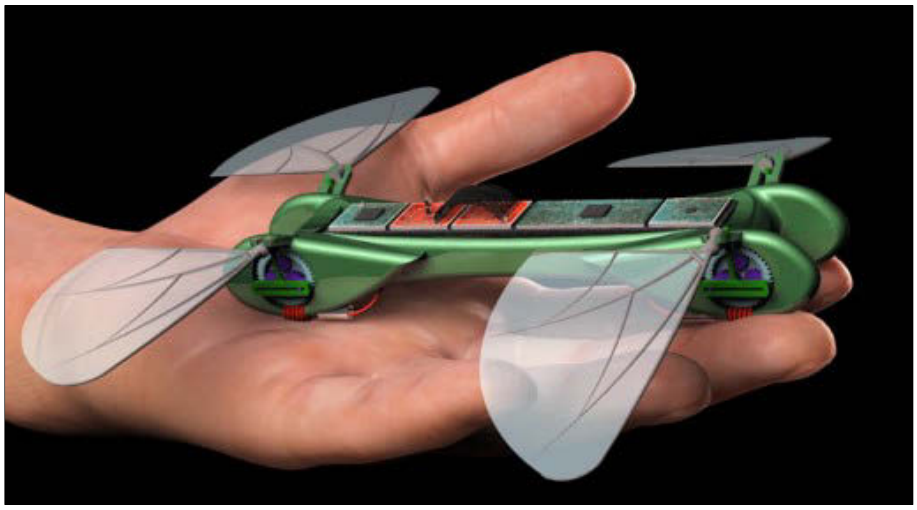

Figure 12: TechJect's Dragonfly.

Figure 13: Festo's SmartBird.

A final drone worth mentioning is the SmartBird (see Figure 13), which has been designed and prototyped by the German company Festo. This mechanical bird has been modeled on the herring gull. Its design emphasizes good aerodynamics and maneuverability. With a weight of about 450 grams and a wingspan of 1,96 meters, the SmartBird is somewhat larger than Nano Hummingbird and the Dragonfly (Lai, 2011).

It is capable of taking off and landing on its own, but it can also be controlled and monitored from afar (Lai, 2011).

For all but the largest of biomimetic drones, power consumption remains a problem that hinders their practical application. Fashioning insect-sized drones that can stay aloft for more than a few minutes will require great advances in battery technology. One drone engineer expects it to take more than a decade (Horgan, 2013). Technologies currently being pursued that could help insect-sized drones sustain flight for longer periods include miniature fuel cells, and small-scale infrared laser systems and inductive charging systems, both of which can transfer power wirelessly (Piore, 2014).

Given the current trend towards technological miniaturization, the current state of research on biomimetic flight technology, and the potential developments in terms of battery technology, I think it is likely that in the future small biomimetic drones are going to possess much of the capabilities that larger regular small drones have today. They will have excellent flight mechanics, decent sensor systems and endurance, and they will be able to function autonomously in swarms.

3.4.2 Future applications

The future applications of biomimetic drones may include many of the applications that currently exist for regular small drones. Biomimetic drones will, however, add an important extra dimension to all these uses in that they will be able to come very close to their targets while going largely unnoticed. This capability will make them very formidable spying tools. Eventually, they may be capable of swarming through alleys, crawling across windowsills, and perching on power lines, all the while capturing decent quality audio and video while their targets would be none the wiser (Hennigan, 2011). The company behind the Nano hummingbird has stated in 2011 that it sees biomimetic drones carrying out detailed reconnaissance missions ten years on (Hennigan, 2011).

In the future, the spying capabilities of biomimetic drones could be used by law enforcement agencies for covert surveillance of, for example, criminal or terrorist suspects and political demonstrators. Many drones could be used to track multiple individuals at once. Other relevant public sector uses include security surveillance, search and rescue, traffic monitoring, and environmental monitoring (with sensors for pollution monitoring) (Piore, 2014). For all these uses, they could be deployed in swarms.

Commercial applications of biomimetic drones may include workplace security, private investigations, inner-city courier services, outdoor event documenting, and athlete tracking at sports events (Science Learning, 2014). Privately, these small-scale bird- or insect-like aircraft may be used for home security, amateur photography and filmmaking (documenting recreational activities such as a day of skiing or hiking), citizen journalism, and advanced gaming (Science Learning, 2014). More sinister ways of using them may include snooping on other people and transporting narcotics.

The widespread use of stealthy biomimetic drones in all these ways might have a profound social effect in that it might make the public wary of everything that looks like an insect or a bird, for anyone from a law enforcement agent to the next-door neighbor could be secretly watching. This potential effect and other effects and their ethical implications will be discussed in the next chapters.

3.5 Conclusion

In this chapter, I have carried out the *forecasting stage* of Brey's (2012) anticipatory technology ethics (ATE) approach. I described the present and possible future capabilities and applications of surveillance-capable drones in civil contexts. To obtain the most reliable and diverse set of predictions of the technology's future capabilities and applications, I used methods from the interdisciplinary field of *futures studies* or *futurology*, which included environmental scanning, trend analysis, and expert interviewing. This combination of methods has a strong focus on *evidence* and *expertise* as sources of knowledge about the future and as a result of resource limitations is somewhat deficient in terms of its reliance on *interaction* and *creativity* as sources of knowledge.

In the descriptions of present and future capabilities and applications, I have made a distinction at the level of artifacts between three main categories of surveillance-capable drones, namely, large wide-area persistent surveillance drones, small general-purpose drones, and biomimetic spy drones. This categorization is largely based on the similarities among drones in terms of their surveillance capabilities. In future analyses, using a more detailed categorization may be helpful.

First, I have defined large wide-area persistent surveillance (WAPS) drones as large (> 20 kg), expensive, technologically advanced systems that have great endurance and offer so-called *persistent surveillance* capabilities over an extensive ground area. Persistent surveillance may be defined as the close, sustained monitoring of an area enabling the detection, location, identification, and tracking of any individuals or objects within this area. Large WAPS drones can be almost unnoticeable when flying at high altitudes. In the future, their wide-area motion imagery (WAMI) capabilities will continue to expand, with increases in area coverage and image resolution. Large WAPS drones will also be capable of carrying any of a wide variety of sensors, including thermal, night vision, radar, multispectral, and hyperspectral sensors. The tracking algorithms that may be utilized by these systems are expected to become "context-aware", meaning that they can determine a person's "pattern-of-life" by recognizing specific behaviors through her interactions with her surroundings or network. Their capabilities to identify, track, and analyze the behavior of people may be further enhanced by the creation of connections with other information systems. Finally, WAPS drones will have a greater degree of autonomy in the future. Sensor data analysis and communication will involve a great deal of autonomy on the part of the drone. Other areas of autonomous behavior development will include vehicle path and motion planning.

The use of WAPS drones will largely be restricted to well-funded public sector and private sector organizations. Applications of these drones may include: border surveillance, crime surveillance over urban areas, criminal investigation in urban areas, security monitoring of large crowds, search and rescue, and emergency and disaster response.

Secondly, I have defined small general-purpose drones as small (< 20 kg) systems that mostly lack the range, the speed, the wide-area perspective, and the sophisticated sensor payload of large WAPS drones, but are much cheaper and easier to procure, operate, and maintain. These drones can be used to observe and record scenes in high detail from up close and from many different angles, thus making them highly versatile. There is much variation among small drones in terms of cost and capabilities. Currently, two main types of small general-purpose drones can be differentiated: fixed-wing drones and rotary blade drones. The largest small drones used for surveillance purposes may feature cameras that have the same capabilities as powerful hand-portable digital cameras. These drones can be very formidable in terms of

observing scenes in high detail over relatively large distances. Besides video and still cameras, small drones can carry a host of other sensors, including light-weight multispectral, thermal, and night vision imaging sensors. The systems tend to be fairly quiet during flight, which enables them to operate with some level of stealth. In the future, their basic capabilities will improve while they become ever smaller and cheaper. The imaging capabilities of small cameras used on these systems will likely improve rapidly, with Gigapixel resolutions soon entering the realm of the possible. Their computational power will support advanced computer vision capabilities such as facial identification, "soft biometrics" identification, gaze detection, et cetera. Given these developments, it is likely that the identification over people over large distances will be a basic capability of small drones used in surveillance applications. Miniaturization and new battery technologies, such as fuel cell battery technology and perhaps laser wireless recharging technology, may significantly increase the currently rather short flying times (< 2 hours) of small drones. Finally, small drones will have a greater degree of autonomy in the future. Sensor data analysis and vehicle path and motion planning will involve a great deal of autonomy, and some drones may be able to swarm using sophisticated flocking algorithms.

Small general-purpose drones will have a plethora of applications for public and private sector organizations, as well as for private individuals. Applications of these drones may include: border surveillance, traffic accident investigations, criminal investigation in urban areas, search and rescue, tactical operations, tax investigation, environmental protection monitoring, security monitoring, infrastructure monitoring, investigation by private investigators, parcel and grocery delivery, property damage evaluation by insurers, photography and filmmaking, industrial espionage, (paparazzi) journalism, real estate advertising, snooping on other persons, amateur filmmaking, amateur journalistic reporting, and drone usage through hacking.

Thirdly and finally, I have defined biomimetic spy drones as small to very small systems that mimic the size, appearance and behavior of insects and birds and are thus able to hide in plain sight. Inherently, these drones have great potential for covert surveillance applications. Currently, biomimetic drones do not have practical uses outside the laboratory environment. Many are still at the prototype stage, their real-life application being hampered by design challenges relating to flight mechanics and power supply that will take some time overcome. I believe it is possible, however, that in the future small biomimetic drones are going to possess much of the capabilities that larger regular small drones have today. They will have excellent flight mechanics, decent sensor systems and endurance, and they will be able to function autonomously in swarms.

Biomimetic spy drones will have numerous applications for public and private sector organizations, and private individuals. Applications of these drones may include: criminal investigation in urban areas, search and rescue, tactical operations, tax investigation, environmental protection monitoring, traffic monitoring, workplace security monitoring, private investigation, inner-city courier services, outdoor event documenting, athlete tracking at sports events, home security monitoring, amateur photography and filmmaking, citizen journalism, and advanced gaming. Biomimetic drones add an important extra dimension to all these uses in that they will be able to come very close to their targets while going largely unnoticed. This capability will make them very formidable spying tools.

A full summary of all drone capabilities and applications that have been described in this chapter is provided in table form in appendix B of this study.

4 Conceptualizing privacy

Now that the capabilities and applications of surveillance-capable drone technology have been adequately described, we can almost start the ethical analysis of the technology. One of the core arguments against modern surveillance technologies is that they pose a threat to privacy (Lyon, 2003), which is a concept that is generally considered important to the extent that it is a necessary part of human existence (Newell, 1995).[13] The concept of privacy, however, has proven notoriously difficult to grasp, which is why this chapter is devoted to its conceptualization and operationalization.

The term "privacy" is used frequently in ordinary language as well as in philosophical, political and legal discourse. Although the concept has a rich history in terms of discussions about the extent to which it is valued and preserved, a universally accepted definition of privacy has remained elusive. At present, there is significant disagreement among theorists over its meaning, value and scope. Accounts of privacy can generally be classified according to whether they are normative or descriptive; whether they define privacy in terms of "access" or "control"; and whether they see privacy as a means to achieve other values or as a way to protect a specific, private realm (Nissenbaum, 2010). In particular, there has been significant debate on whether privacy is to be understood in terms of the *access* that others—the state, corporations, or other people—have to an individual's body or personal information, or in terms of the *control* that the individual has over what happens to her body or personal information. It is also worth noting that many of the older approaches to privacy, as well as some contemporary approaches, maintain a distinction between a public and a private sphere, which has increasingly attracted criticism. Contemporary theorists such as Helen Nissenbaum (1997, 1998) argue that this distinction cannot serve as a basis of a privacy theory. (More on this in section 4.3.)

In an effort to move out of the deadlock of disagreement in privacy theory, recent scholarship recognizes that privacy comprises multiple, fundamentally different, *dimensions*. Some theorists have therefore attempted to create taxonomies of privacy problems, intrusions or categories (Kaspar, 2005; Solove, 2008; Finn, Wright, & Friedewald, 2013). Moreover, Daniel Solove (2008), a prominent legal theorist, has advocated moving away from defining privacy and towards addressing *contextual* privacy problems, which means that how we are to approach privacy is dependent on the specific context of the privacy problem.

In light of these facts, it is clear that we must be careful to select an approach to privacy that is suitable for the ethical analysis at hand. Now what would be the requirements for such an approach? First of all, the approach should enable us to assess the impacts of an emerging (surveillance) technology on privacy. Specifically, it should be able to be used at the *technology level*, the *artifact level* and the *application level* of the ethical analysis carried out in this thesis. Consequently, it must be capable of producing coarse as well as fine-grained analyses of a technology's impacts. Furthermore, since drones are most often being used in

[13] Over the years various justifications have been offered for a right to privacy, which include individual psychological needs (such as the need for autonomy and individuality; a space to develop one's identity and personhood; not being gazed at; not being de-contextualized against one's will), philosophical understanding of human beings (dignity); privacy as constitutive of intimate relationships, of professional relationships (attorney-client; physician-patient), and ultimately, as a social good, constituting a healthy and functioning community and the democratic state at large (Birnhack, 2011).

public spaces, the approach should be able to deal, in a meaningful way, with issues of *privacy in public*. Finally, it should be able to recognize a wide range of intuitively sensed privacy issues in a wide range of situations. Considering this last requirement and a general lack of consensus in the field of privacy theory, it may help us to stay clear of "partisan" approaches, such as the "access" and "control" theories, in favor of more pragmatic ones that are contextual and do not have privacy definitions that are too restrictive. Such practical, contextual approaches would cast a wider scope for the identification of privacy issues and would perhaps also lead to greater acceptance among theorists of the privacy analysis at hand.

I have selected two privacy approaches that, taken together, best meet the above requirements. I apply both of these approaches, separately, in chapter 5 and chapter 6. The first approach is a well-received and comprehensive approach to addressing privacy "in context" by privacy theorist Helen Nissenbaum (1997, 1998, 2004, 2010). Nissenbaum proposes a construct called "contextual integrity" as a benchmark for privacy in public surveillance contexts. She stresses that she does not offer a philosophical definition of privacy, but a practical approach that nonetheless *explains*, *predicts* and *prescribes* in relation to privacy impacts. Her approach ties adequate protection of privacy to the *informational norms of specific contexts*, demanding that the gathering of personal information is appropriate to the context in which it is taking place, and that its dissemination obeys the governing norms of distribution within this context. The contextual integrity approach is used to make evaluations at the *application level* of ethical analysis for a number of specific applications in chapter 6, as it is well-equipped for this kind of "micro-level" analysis.

The contextual integrity approach is, however, less well suited for use at the *technology level* and the *artifact level* in chapter 5. Because of its inherent focus on specific, well-defined contexts of use, it is less fruitful to use the approach to analyze drone surveillance technology and artifacts in more general terms. Therefore, a second approach is used in the identification of privacy risks and impacts at the technology and artifact levels, which is the "seven types of privacy" approach by Finn, Wright & Friedewald (2013). This complementary approach is a categorization of *types of privacy* that are relevant to emerging technologies, which can serve as a checklist to identify general privacy issues. Although the two approaches are different from each other in important ways, they are philosophically compatible since they both lack a strict philosophical definition of privacy.

In the four sections that now follow, I offer a description and an assessment of the "contextual integrity" approach and the "seven types of privacy" approach. The chapter ends with a short concluding section. I will start off with a description of Nissenbaum's contextual integrity.

4.1 Nissenbaum's "contextual integrity"

Over the last two decades, privacy theorist Helen Nissenbaum (1997, 1998, 2004, 2010) has worked to develop a framework for informational privacy in the public realm, called "contextual integrity". Nissenbaum argues that informational privacy is neither a right to secrecy nor a right to control information about oneself, but a *right to an appropriate flow of information*, and that what is appropriate varies from context to context. In this section I will explain what she means by this.

4.1.1 Nissenbaum's criticism of traditional privacy approaches

Nissenbaum (1997, 1998, 2004, 2010) has argued that traditional approaches to privacy often yield unsatisfactory conclusions when they are used to study the privacy effects of new information technologies

that harvest information in the public realm. In a 1997 article, she has voiced opposition to two "misleading assumptions" that are common in these theories. The first assumption is that there is a realm of public information about persons to which no privacy norms apply. The second is that an aggregation of information does not violate privacy if its parts, taken individually, do not.

In response to the first assumption, Nissenbaum (1997) argues that even quintessential public spaces, such as public parks and sidewalks, are governed by some norms of privacy; information collected from those spaces is never completely public. For instance, it would be within one's rights to reply "none of your business" to a stranger who asks about one's name. Moreover, she points out that an individual has a right to control the dissemination of personal information even if it happened in a public area. For example, if a rape occurred in public, the victim still deserves some measure of privacy as to her identity.

With regard to the second assumption, Nissenbaum (1997) points out that combining seemingly worthless pieces of information of an individual can be invasive of her privacy, because those pieces of information can together be transformed into a rich portrait of her. Through technology, large amounts of personal information can be collected in a short period of time, from which meaningful inferences can be drawn that can embarrass and hurt a person. Nissenbaum adds that the act of compiling almost always involves shifting information from one context to another, which often means using information in a way that was not explicitly announced when the information was initially collected. When users have not explicitly granted permission to move their information around, they have effectively lost control over it.

4.1.2 Contextual norms of information flow

Nissenbaum (1997, 1998, 2004, 2010) has argued that privacy issues presented by new information technologies are seldom acknowledged by philosophical accounts of privacy and she refers to them as the "problem of privacy in public" or the "problem of public surveillance". To solve this problem Nissenbaum created a new construct, which she calls *contextual integrity* (CI), as a model of people's intuitive judgments and a normative benchmark for informational privacy. She first presented her theory in 2004 in an influential essay titled "Privacy as Contextual Integrity" and later, in 2010, wrote a detailed account of it her book called *Privacy in Context: Technology, Policy, and the integrity of Social Life*. CI focuses on the notion of context to analyze whether or not a *flow of personal information*—that is, the gathering or the dissemination of *any* information about a person—is appropriate given the informational norms embedded in a particular context. It is based on two principles, namely that (1) the activities people engage in take place in a plurality of contexts, and that (2) each context has a distinct set of entrenched norms governing the flow of personal information that shape people's roles, behavior, and expectations within this context.

According to Nissenbaum (2010), contexts refer to "structured social settings with characteristics that have evolved over time (sometimes long periods of time) and are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more" (p. 130). Nissenbaum argues that almost everything people do happens in contexts and people navigate across different contexts throughout the day. The different contexts one could be in on a single day could, for example, include working at the office, consulting a doctor for a medical problem, watching television with one's partner, and attending a birthday party. Contexts, she says, incorporate assemblages of *roles*; are partly constituted by canonical *activities* that are oriented around *values*; and are governed by behavior-guiding *norms* that prescribe and proscribe acceptable actions and practices. In an effort to explain these constructs, Kanha Sar & Al-Saggaf

(2013) offer the following useful example: "[I]n the context of education, Jane's *role* is a PhD candidate or student at the School of Computing and Mathematics at Charles Sturt University, where some of her *activities* include conducting interviews for her research, analyzing the data and writing up the reports. The *value* of the education or her role as a PhD candidate is to create new knowledge and contribute to the literature. The *norms* prescribe that Jane as well as other PhD candidates submit progress reports to the Research Office every six months." (p. 19).

Norms, according to Nissenbaum (2010), define duties, prerogatives, obligation, and privileges associated with particular roles, as well as acceptable and unacceptable behaviors. Among the norms present in most contexts are those that govern the flow of personal information in the contexts. There are two types of such informational norms in Nissenbaum's theory: (1) *norms of appropriateness*, and (2) *norms of distribution*. The first set of norms determines whether it is appropriate, expected or allowable for personal information of a particular kind to be revealed within a certain context. In the example of Kanha Sar & Al-Saggaf "it is appropriate [within the context of education] that the Research Office at Jane's university know her PhD progress, but it is not appropriate that they also know her medical condition details" (p. 19). The second set of norms regulates the flow of information within and across contexts. For instance, "within a health care context, it is appropriate that Jane's General Practitioner (GP) access her medical records, and divulge those details with other GPs or specialists if needed, but it is not appropriate that he provide these details to Jane's employer" (Kanha Sar & Al-Saggaf, 2013, p. 19). Contextual integrity of the information flow is maintained when both the norms of appropriateness and the norms of distribution are respected. When either of them is breached, a "violation of privacy" occurs.

Nissenbaum (2010) further explains that informational norms are characterized by four key parameters: *contexts*, *actors*, *attributes*, and *transmission principles*. Contexts are the "backdrop of informational norms" (p. 141); actors can be understood in terms of three components: "senders of information, recipients of information, and information subjects" (p. 141); attributes can be understood as a "*type* or *nature* of information" (p. 143, italics in original); and transmission principles serve as a "constraint on the flow of […] information from party to party in a context" (p. 145) and expresses terms and conditions, such as *confidentiality* and *reciprocity*, under which such transfers occur.

According to Nissenabum (2010), the CI framework can "guide an assessment" of a "problematic new practice resulting from the development of a novel technical device or system" by asking the question: "Does the practice in question violate any context-relative informational norms?" (p. 148). In Nissenbaum's view, her CI approach does a much better job than the traditional approaches at analyzing and evaluating the privacy issues relating to new information technologies, such as consumer profiling and data mining technologies. For example, unlike many other approaches, it would in many instances consider it a privacy violation when publicly available information gathered from a variety of sources was combined to build detailed personal profiles of individuals. Such judgments bring the CI approach in line with the intuitive judgments of most people.

4.1.3 A "decision heuristic"

Insofar as the CI framework is used as an approach to normatively evaluate the privacy impacts of new information technology-based systems and practices, it has been criticized for being too conservative in that it always favors the entrenched norms of information flow, and (relatedly) for not being easily adaptable to those new information technologies for which there are no clearly articulated pre-existing

practices, expectations, or norms that govern the flow of personal information (Nissenbaum, 2010). While defending the general conservative nature of her approach, Nissenbaum (2010) has acknowledged that there are two problems with CI as described thus far, which are both rooted in conservativism. They are the problems of "opportunity cost" and "tyranny of the normal" (p. 160): firstly, the approach flags as problematic *any* departure from entrenched practice, even if the new practice seems very much preferable, and secondly, it "appears to provide no buffer against insidious shifts in practice that ultimately gain acceptance as 'normal'" (p. 161).

Addressing these problems, Nissenbaum (2010) has augmented her approach with a normative component, which holds that entrenched informational norms do not merely indicate when novel practices contravene traditional practices, but also possess moral justification insofar as they support the attainment of general as well as context-dependent *values*, *ends*, and *purposes*. For example, important values of an airport context will likely include safety, security, and efficiency of movement. This adaptation of the CI framework, she argues, opens up the way for challenges to an entrenched practice by nonconforming practices, when the latter are shown to be more effective in supporting or promoting the values, ends, and purposes. In evaluating a challenge, a presumption in favor of entrenched norms recognizes that these norms are likely to reflect the *settled rationale* of a given context. However, Nissenbaum embraces the possibility that challenges might outperform entrenched practices; in this event, entrenched norms legitimately give way to new norms.

Based on the augmented framework, Nissenbaum (2010) has outlined a "decision heuristic" that is intended as an "approach to understanding the source or sources of trouble as well as an approach to evaluating the system or practice in question" (p. 181). This decision heuristic takes the form of guidelines that are articulated in a series of nine steps:

1. "Describe the new practice in terms of information flows.
2. Identify the prevailing context. Establish context at a familiar level of generality (e.g., 'health care') and identify potential impacts from contexts nested within it, such as 'teaching hospital.'
3. Identify information subjects, senders, and recipients.
4. Identify transmission principles.
5. Locate applicable entrenched informational norms and identify significant points of departure.
6. Prima facie assessment: […] A breach of informational norms yields a prima facie judgment that contextual integrity has been violated because presumption favors the entrenched practice.
7. Evaluation I: Consider moral and political factors affected by the practice in question. What might be the harms, the threats to autonomy and freedom? What might be the effects on power structures, implications for justice, fairness, equality, social hierarchy, democracy, and so on? […]
8. Evaluation II: Ask how the system or practices directly impinge on values, goals, and ends of the context. In addition, consider the meaning or significance of moral and political factors in light of contextual values, ends, purposes, and goals. In other words, what do harms, or threats to autonomy and freedom, or perturbations in power structures and justice mean in relation to this context?
9. On the basis of these findings, contextual integrity recommends in favor of or against systems or practices under study. […]" (p. 182-183).

The first five steps or components in this model are descriptive; they help us to gain a clear understanding of the features in a new technology that may have implications for privacy. Steps six through nine, on the

contrary, are essentially normative in nature since they guide us in evaluating the features and practices associated with the new technology. The exact significance of each of these steps will become clear as we apply the heuristic in chapter 6.

4.2 Justifying the contextual integrity approach

An adapted version of Nissenbaum's (2010) contextual integrity approach is used in chapter 6 at the application level of ethical analysis. It is used because it performs well in terms of satisfying the three main conditions specified in the introduction of this chapter. First of all, the approach can be used to study the effects of an emerging technology on informational privacy. It is a forward-looking approach, especially its latest iteration containing the decision heuristic, which is specifically designed to be able to deal with new technologies, such as unmanned aerial vehicles, that may challenge entrenched practices. The approach is particularly useful for a privacy analysis of an emerging technology *at the application level*, as it has a rich conceptual toolkit that allows for a comprehensive analysis of the specific contexts of a technology's applications, thus generating very detailed privacy analyses of these applications.

Now, although the approach is well suited for analysis at the application level, it is not the most efficient approach at the *technology level* and the *artifact level*. In fact, it would be rather cumbersome to use Nissenbaum's approach at these levels of analysis, as this would lead one to make unnecessarily detailed analyses of a number of different drone application contexts that are encompassed by the technology.[14] Ultimately, it is not essential to have such a detailed look at the contexts if the aim is simply to identify potential privacy issues in a more general sense with respect to a technology or an artifact. For these reasons, a simpler, more efficient, approach is used in chapter 5 at the technology and artifact levels of the ethical analysis at hand. The "seven types of privacy" approach by Finn et al. (2013) is thus described in the next section.

In response to the second requirement, it can be argued that the approach takes seriously the issues relating to privacy in public spaces. One of its main virtues that sets it apart from many traditional privacy theories is that it justifies protecting "public" personal information (PPI) in certain situations. Many traditional privacy theories divide personal information into two exclusive realms—the private and the public—and only protect non-public personal information (NPI). As we have seen, Nissenbaum (2010) has convincingly shown that viewing personal information merely in terms of this dichotomy is problematic, arguing that one's PPI can also warrant normative protection, even if that PPI does not qualify as personal information that is confidential, sensitive, or intimate. According to the CI approach, it is always the contexts in which and across which one's personal information flows, and not the type of personal information itself, that determine whether the information in question deserves normative privacy protection within these contexts.

Finally, with regard to the third requirement, we can say that the approach is capable of recognizing a wide range of intuitively sensed privacy issues, since it is not loyal to just one particular philosophical definition of privacy. Like the "seven types of privacy" approach (as we will see), it avoids a major tension that is

[14] The contextual integrity approach is best suited for analysis of specific, well-defined contexts. Alternatively, one can broaden the scope of the contexts under consideration (for example, taking "public space" as a context, instead of the more specific "catching terror suspects at the Olympic park" context), but then the contextual integrity approach will quickly lose much of its analytical strength and will not offer much of an advantage over the "seven types of privacy" approach.

found in much of the traditional privacy discourse (as stated in the introduction), where the concept of privacy tends to be viewed in terms of either restricting *access* to or having *control* over one's personal information. Arguably, authors who view privacy in terms of information control often tend to ignore the role that restricting access to personal information also plays, and authors who defend the restricted access view of privacy tend to underestimate the insights offered by theories that emphasize the importance of one's having at least some control over one's personal information (Tavani, 2012). Nissenbaum (2010) explains that her CI framework "[...] reveals why we do not need to choose between them; instead, it recognizes a place for each. The idea that privacy implies a limitation of access by others overlaps, generally, with the idea of an informational norm. [...] Control, too, remains important in the framework as one of the transmission principles" (pp. 147-148).

Now, in spite of all these virtues, the CI framework has faced criticism. It has been argued that the approach insufficiently takes into account individual differences in people's personal attitudes towards privacy in particular contexts (Friedewald, Gutwirth, Wright, Mordini, et al., 2011). However, as has been pointed out by Solove (2008), it would quite impractical to devise a set of practical rules around an array of individuals' idiosyncrasies.

Other, perhaps more serious, concerns have been raised by Michael Birnhack (2011). This author argues that the CI approach remains too conservative in its reliance on the *status quo ante* of informational norms, which he notes does not even exist sometimes. Many contexts, he says, are dynamic, unsettled and unstable and are the result of power relations instead of moral considerations. In his view, contexts are dynamic social constructions which should be given the freedom to develop and change, in terms of informational norms *and* in terms of their underlying values, goals and ends. Moreover, he argues that although CI results in a seemingly "neutral" decision heuristic, many of the steps in this heuristic require its user to make normative judgments. Such normative judgments would, for example, be needed in determining the context in cases where contexts are unclear or unsettled. They would also be necessary in determining the informational norms, as CI does not fully account for who determines what the informational norms are, how their validity should be determined and what the process is in which these norms become norms. CI does not offer guidance for making these normative judgments.

Nevertheless, on balance I think Nissenbaum's contextual approach remains very useful. We will see that the criteria included in the heuristic device are especially helpful in analyzing privacy concerns that arise in civil drone applications in public environments. The framework can, however, be improved a little if some of the above-mentioned problems are addressed.

I agree with Birnhack (2011) that the CI framework is too conservative, even if it allows entrenched norms to be challenged in some cases. My primary concern is not the dynamic, unsettled nature *per se* of some, mostly new, social contexts (such as, perhaps, social media); rather, I think it is most important to recognize that preferring the status quo of informational norms *and their underlying values* within a context might legitimize and reinforce an unfair equilibrium achieved by a powerful party at the expense of relatively powerless other parties. For example, one could argue that in the healthcare context economic values such as efficiency and cost-effectiveness have become increasingly important under the influence of market forces, and that this has come at the expense of patient-centered values such as health and autonomy (a development which is seen by many as unwelcome). Nissenbaum's (2010) defense of the conservative structure of CI by reference to theories of conservatism at large (such as those of Jeremy Bentham and Edmund Burke) does not address this problem. Therefore, I think the goals, values and ends

on which the norms of the context are based should be evaluated by recourse to external moral reasoning. As Birnhack rightly notes, a theory of privacy should ideally explain why people do what they do and offer sufficient reasons to overrule the majority in some cases and impose duties on some actors. I propose to add the following step in Nissenbaum's decision heuristic between step 7 ("Evaluation I") and step 8 ("Evaluation II"):

"Evaluate whether the goals, values and ends of the context, as well as the balance between them, are fair, and amend them if they are not."

Unfortunately, I have no clear and reliable principles on which to base such an evaluation, which means that an evaluation is going to be somewhat subjective. As a suggestion, however, one could aim to settle for goals, values and ends that best support the wellbeing of the widest majority of people who are *by necessity* involved in or affected by the context at hand, without having an exceedingly negative impact on the wellbeing of a minority of those people. The positive consequences of the goals, values and ends for the majority must then far outweigh rather than marginally outweigh any harm to a minority of people. Such a principle would amount to a weak form of *consequentialism* that allows room for *deontological* considerations—one we may call *threshold consequentialism*.[15] I do not wish to advocate a strict moral absolutism, however. Perhaps the principles for evaluating the contextual goals, values and ends should themselves to some extent be dependent on the given context.

Finally, one last issue regarding the CI framework has to do with analyzing a potential state of affairs *in the future*, as is necessary in the case of this study. It is probable that *present* informational norms of various public surveillance contexts are thoroughly contested by the use of drones for mass public surveillance. However, whether public surveillance norms will remain contested in the *future* is not at all clear. What if societal norms gradually shift to adapt to increased privacy incursions by future drone use? Nissenbaum would likely call this an instance of "tyranny of the normal". We could deal with this situation by focusing on how future drone systems and practices directly impinge on fundamental social, political, and moral values (step 8 in the original decision heuristic) and on values, goals, and ends internal to the context (step 9). These will presumably not change quite as quickly as the informational norms will. Moreover, they have been made subject to external moral reasoning in the updated version of the decision heuristic, which means that "the spirit of the time" in terms of values goals and ends is not the only factor to take into account in an evaluation. Nevertheless, useful insights may still be obtained by examining how future drone systems and practices impinge on the present informational norms of particular contexts, which is why step 5 of the original decision heuristic is kept in the adapted version that is used in this thesis.

4.3 Finn, Wright & Friedewald's "seven types of privacy"

Let us now have a look at the privacy approach that I take to be a better, more efficient, alternative to contextual integrity at the technology and artifact levels of ethical analysis. As a part of their research for the Privacy and Emerging Sciences and Technologies project, funded under the European Commission's 7th Framework Programme for Research and Technological Development, Finn, Wright & Friedewald

[15] Consequentialism is the class of normative ethical theories holding that the consequences of an action (or, in this case, the proper goals, values and ends of the context) are the ultimate basis for any judgment about the rightness or wrongness of that action. It stands in opposition to (amongst other theories) deontology, which is the normative ethical position that judges the morality of an action based on the action's adherence to a rule or rules. In this case, such a rule could be that no persons are to be harmed at all by the context's goals, values and ends.

(2013) have developed a contemporary conceptualization of privacy. In their view, privacy is best conceptualized as a categorization of types of privacy. The authors believe that their conceptualization "provides academics and other privacy experts with a useful, logical, well-structured and coherent typology in which to frame their privacy studies" (p. 6).

Privacy, according to Finn et al. (2013), has proven incredibly hard to define philosophically. The authors take it to be a fluid and dynamic concept that develops alongside technological and social change. They agree with Daniel Solove (2008), who asserts that privacy is best understood as a "family of different yet related things" (p. 9). Solove finds that there is no common denominator to all things referred to as "privacy" and that the meaning of privacy depends upon context. He therefore outlines a typology of privacy problems that must be addressed, even as they do not collectively conform to an exact definition of privacy. A typology of privacy intrusions is also offered by Debbie Kaspar (2005).

Finn et al. (2013) agree with Solove and Kaspar that creating typologies is the best way to obtain a usable conceptualization of privacy. However, they contend that the focus of both scholars on the ways in which privacy can be infringed is "largely reactive" (p. 3). Solove and Kaspar wrongly "focus on specific harms which are already occurring and which must be stopped, rather than over-arching protections that should be instituted to prevent harms" (p. 3). Finn et al. argue for a typology of *types of privacy* rather than a typology of *privacy harms*. The difference between a typology of *types of privacy* and one of *privacy harms*, Finn et al. hold, is the pro-active, protective nature of the latter. The authors compare it to the difference between outlawing murder and adopting a right to life. Murder, they say, is only one way in which life can be undermined; a simple prohibition against murder would not prevent the dissolution of safety principles. A positive right to life, on the other hand "forces individuals, governments and other organizations to evaluate how their activities may impact upon a right to life and introduce protective measures" (p. 3).

The authors argue that Roger Clarke's (1997) human-centered approach to defining categories of privacy does assist in outlining what specific elements of privacy are important and must be protected. Clarke lists the following categories: *privacy of the person*, *privacy of personal behavior*, *privacy of personal communication*, and *privacy of personal data*. Taking into account important emerging technologies such as drones, Finn et al. (2013) have adjusted this list and expanded it so it contains seven types of privacy. In their view, privacy encompasses the following aspects:

- *Privacy of the person.* This category refers to the right to keep body functions and body characteristics (such as genetic codes and biometrics) private, which "is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society" (p. 4).
- *Privacy of behavior.* This category refers to the right to behave in public, semi-public or one's private space without having one's actions monitored or controlled by others, which contributes to "the development and exercise of autonomy and freedom in thought and action" (p. 5).
- *Privacy of personal communication.* This category refers to the right to have one's communications—including emails, telephone calls, and SMSs—protected against interception, which "benefits individuals and society because it enables and encourages a free discussion of a wide range of views and options, and enables growth in the communications sector" (p. 5).

- *Privacy of data and image.* This category, also known as data protection, refers to the right to have one's personal data protected and to "exercise a substantial degree of control over that data and its use", which "builds self-confidence and enables individuals to feel empowered", and "has social value in that it addresses the balance of power between the state and the person" (p. 5).
- *Privacy of thoughts and feelings.* This category refers to the right not to share one's thoughts or feelings or to have one's thoughts or feeling revealed, which "benefits society because it relates to the balance of power between the state and the individual" (p. 5).
- *Privacy of location and space.* This category refers to the right of individuals to move about in public or semi-public space without being identified, tracked or monitored, a right to solitude and a right to privacy in spaces such as the home, the car or the office. "When citizens are free to move about public space without fear of identification, monitoring or tracking, they experience a sense of living in a democracy and experiencing freedom. Both these subjective feelings contribute to a healthy, well-adjusted democracy. Furthermore, they encourage dissent and freedom of assembly, both of which are essential to a healthy democracy" (p. 5).
- *Privacy of association (including group privacy).* This category refers to the right of individuals to associate with whomever they wish, without being monitored, which benefits a democratic society as it "fosters freedom of speech, including political speech, freedom worship and other forms of association" (p. 6).

4.4 Justifying the use of the "seven types of privacy" approach

Finn et al.'s (2013) "seven types of privacy" conceptualization is used in the next chapter at the technology and artifact levels of ethical analysis. There are a number of reasons for selecting this approach.

Let us first have a look at how the approach satisfies the three main conditions stated in the introduction. Firstly, the approach enables us to carry out evaluations of the impacts of an emerging technology on privacy. The approach is specifically designed to be able to deal with novel privacy issues that accompany emerging technologies such as unmanned aerial systems, whole body imaging scanners, RFID-enabled travel documents, second-generation DNA sequencing, human enhancement technologies, and second-generation biometrics.[16] Furthermore, it can conceivably be used at each of the three levels of ethical analysis. Secondly, the approach takes seriously issues relating to privacy in public spaces. For example, the sixth category of the approach encompasses the right of individuals to move about in public or semi-public space without being identified, tracked or monitored. Finally, it is capable of recognizing a wide range of intuitively sensed privacy issues, since it is not exclusively loyal to a single philosophical definition of privacy. The approach incorporates various recognized definitions of privacy and builds on a well-received typology established by Clarke (1997), thus casting a wide scope for the identification of privacy issues. Furthermore, by categorizing types of privacy, it adds detail and specificity to the concept of privacy, thus making analysis easier and more accurate; the approach can be used as a check-list.

I propose to expand Finn et al.'s list with one more type of privacy, namely *privacy of property*. The list would then encompass eight types of privacy (henceforth I will still refer to the approach as the "seven

[16] Finn et al. (2013) demonstrate their approach by briefly analyzing the potential impact on privacy of these six emerging technologies. For each technology, they examine what types of privacy the technologies could infringe upon. The result of their short privacy analysis of drones will be used in the next chapter.

types of privacy" approach). Privacy of property is somewhat similar to *privacy of location and space* in that it refers a right of privacy in private spaces such as an individual's house, backyard, or car. However, it is different in that the object of privacy protection in the most direct sense is not an individual or group, but their *personal property*. I believe that many people would find it unsettling if detailed and extended footage of their backyard became available to commercial parties, law enforcement, or the public at large, even if no persons are in the footage. A lot of personal information can be inferred merely by closely monitoring and analyzing a person's belongings in semi-publicly visible private spaces. A right to not have one's property monitored in spaces such as one's house (through the windows) or one's backyard (from above) would likely contribute to an individual's autonomy and various forms of freedom, such as freedom of expression.

The simplicity of Finn et al.'s (2013) approach makes it particularly well suited for use at the technology and artifact levels of ethical analysis. It is to be favored over the contextual integrity approach at the technology and artifact levels because it allows for a more efficient identification of general privacy issues regarding a technology or artifact. As already argued in section 4.2, it would be rather cumbersome to use Nissenbaum's approach at these levels of analysis, since this would lead one to make unnecessarily detailed analyses of many different drone application contexts encompassed by the technology.[17] Ultimately, it is not essential to have such a comprehensive look at the contexts if the aim is simply to identify more general potential privacy issues regarding a technology or artifact.

Then, one may ask, what about using the "seven types of privacy" approach at the application level of analysis? Although the approach can be used at the application level, Nissenbaum's (2010) approach is very much preferred here; contextual integrity is a more suitable approach for identifying privacy issues at the application level for a selected number of applications, since it uses a rich conceptual toolkit that allows for a very structured and comprehensively analysis of the specific contexts of a technology's applications, thus generating very detailed privacy analyses of these applications.

4.5 Conclusion

I have chosen to use two operational approaches to privacy to analyze privacy issues in this thesis. Both of the approaches meet the requirements of being capable of analyzing an emerging technology in terms of privacy issues; dealing with privacy issues in public space; and recognizing a wide range of intuitively sensed privacy issues. The approaches complement each other, as they are best suited for slightly different purposes because of their different strengths and weaknesses. The first approach is the practical and comprehensive "contextual integrity" approach by Helen Nissenbaum (2010), which focuses on contextual norms to produce very detailed evaluations of the impacts of emerging technologies on informational privacy in its broadest sense. This approach is well-equipped for "micro-level" analysis and is therefore used in chapter 6 to make evaluations at the application level of ethical analysis for a limited number of applications. The second approach is the "seven types of privacy" approach by Finn, Wright & Friedewald (2013), which is a straightforward categorization of types of privacy that are relevant in the

[17] The contextual integrity approach is best suited for analysis of specific, well-defined contexts. Alternatively, one can broaden the scope of the contexts under consideration (for example, taking "public space" as a context, instead of the more specific "catching terror suspects at the Olympic park" context), but then the contextual integrity approach will quickly lose much of its analytical strength and will not offer much of an advantage over the "seven types of privacy" approach.

context of emerging technologies. This approach can serve as a convenient checklist for quick and accurate identification of more general privacy issues and is therefore used in chapter 5 to identify general privacy impacts and risks at the technology level and the artifact level of ethical analysis.

Although these two approaches are different from each other in important respects, they are not at odds with each other philosophically since they do not adhere to a strict philosophical definition of privacy. Perhaps the most obvious difference between the approaches is that contextual integrity focuses on analyzing contextual norms, whereas the analysis of contextual norms is not formally a part of the "seven types of privacy" approach, which merely is a categorization of privacy types. I would like to stress, however, that this does not mean that certain general contextual norms cannot, in a more informal way, be taken into account during the identification of privacy impacts and risks using the "seven types of privacy" approach. Ultimately, what binds the two approaches is that they both are pragmatic and contextual, and the decision to combine them is also one that is made on the basis of pragmatism and context.

5 Ethical issues at the technology level and artifact level

In the previous chapter, I have conceptualized and operationalized the concept of privacy. Since I consider it unnecessary to offer extensive conceptualizations of other relevant ethical values,[18] we are now ready to focus our attention on the actual ethical analysis of drone utilization. As explained in chapter 2, the overarching ethics assessment approach used in this study is the anticipatory technology ethics (ATE) approach by Philip Brey (2012). This approach employs three levels of ethical analysis—the *technology level*, the *artifact level*, and the *application level* (see Figure 1 in chapter 2)—which each contain different objects of analysis. In the ethical analysis at hand, these objects are in simple terms, respectively: *drone technology capable of public surveillance*; *drone artifacts capable of public surveillance*; and *drone applications with public surveillance aspects*. In chapter 3, I provided information on the present and future capabilities and applications of three main types of surveillance-capable drones. I will now use this information, and the privacy approaches described in the previous chapter, to carry out the first stage of the ethical analysis of the ATE approach, which is the *identification stage*. In this chapter, various ethical issues concerning surveillance-capable drones are identified that play at the *technology level* and the *artifact level* of analysis. The next chapter focuses on the *application level*. After the identification stage, there is an *evaluation stage* at which the importance of the identified issues is determined and at which the ethical admissibility of drone technology and drone artifacts is evaluated.

I should at this point explain that the general structure of the ethical analysis in this study represents a slight deviation from Brey's (2012) ATE approach. At the technology and artifact levels, things will be done a bit differently than at the application level, which is why this chapter focuses only on the former two levels of analysis and not on all three. Whereas at the technology and artifact levels the identification stage and evaluation stage are conducted separately and thus have separate chapters (for both levels combined), I have found it necessary at the application level to combine both these stages in one chapter. I have also found it necessary to position this latter chapter between the identification stage chapter for the technology and artifact levels (which is this chapter) and the evaluation stage chapter for the technology and artifact levels (which is chapter 7). The reasoning behind these decisions is explained more precisely in the next chapter, but relates to, respectively, the fact that at the application level I will use a single additional approach to conduct at once both the identification stage and the evaluation stage of ethical analysis, and the fact that the results of the evaluation stage at the application level inform the evaluations of drone technology at large and drone artifacts (due to the method I will use to evaluate their ethical admissibility). The general structure of the ethical analysis of this study will thus be as follows:

- Chapter 5: Identification of ethical issues at the technology level and the artifact level
- Chapter 6: Identification of ethical issues and ethical evaluations at the application level
- Chapter 7: Ethical evaluations at the technology level and the artifact level

Now, how exactly should the identification of ethical issues at the technology and artifact levels be conducted in this chapter? As explained in chapter 2, for a comprehensive identification of ethical issues

[18] The meanings of these values, which include equality, security, freedom, etc., are generally more straightforward and less contentious. In addition, these values play a less prominent role in the analysis.

concerning a technology, artifact or application, the ATE approach prescribes that descriptions of the technology's present and future capabilities and applications be cross-referenced with a wide variety of moral values and principles (Brey, 2012). These moral values and principles can be derived from ethical checklists, the technology ethics literature, and bottom-up analyses (Brey, 2012). In this chapter, I use Finn et al.'s (2013) "seven types of privacy" approach as an operationalized checklist for the identification of privacy issues. For the identification of other ethical issues, I rely on a bottom-up approach that draws from the academic and non-academic literature on the societal impacts of civil drone use, as well as from generally accepted moral intuitions.

The next two sections of this chapter respectively present ethical issues inherent in drone technology at large and issues inherent in each of the three main types of drones and some advanced additional features of drones. The chapter ends with a short concluding section that summarizes the ethical issues identified at both levels of analysis.

5.1 Issues at the technology level

Let us first have a look at the ethical issues presented by drones at the technology level. According to the ATE approach, ethical analysis at this level focuses on features of the technology at large, particular subclasses of it, or techniques within it (Brey, 2012). It considers generic ethical issues that are attached to these features. These can be ethical issues inherent to the character of the technology; issues that pertain to consequences that are likely to manifest themselves in any or nearly any artifact or application of the technology; or issues pertaining to risks that the technology will result in artifacts or applications that are morally problematic. In what follows, I will describe the most important of such ethical issues for surveillance-capable drone technology.[19] I have grouped these issues into two subsections, the first subsection focusing on privacy issues and the second focusing on other ethical issues.

Before we begin, let me first clarify and put emphasis on two things. Firstly, "drone technology capable of public surveillance" refers to a collection of the most elemental features of surveillance-capable drones. In the introduction, I have defined surveillance-capable drones as unmanned, non-tethered aircraft, including supporting systems on the ground, that can fly using an onboard means of propulsion; are remotely controlled by human pilots or self-controlled by onboard computers; and contain onboard sensor systems consisting of at least a visual-spectrum camera. In addition, the quintessential drone would have a relatively low visual and audial profile and would send sensor data to the ground via wireless communication.[20] The impacts of non-essential advanced features such as biometric and behavioral analysis systems, which are not present in every drone, are not discussed here, but separately at the artifact level (subsection 5.2.4).

Secondly, it should be stressed that some of the issues listed in this section are "inherent to drone technology" only in the sense that they are likely to occur with all three types of drones in many (if not all) of their applications. Their occurrence is typically difficult to prevent, but can be avoided or mitigated if appropriate (policy) measures are taken.

---

[19] For the sake of convenience, I henceforth refer to these issues collectively as "issues inherent in surveillance-capable drone technology".

[20] To be sure, these two characteristics apply *generally*, in most cases, but not always. However, although they are not part of the (strict) definition of surveillance-capable drones, I do take them as part of the inherent character of the technology.

5.1.1 Privacy issues

This subsection discusses the privacy issues that are inherent in surveillance-capable drone technology. As explained in chapter 4, Finn et al.'s (2013) "seven types of privacy" approach is the most suitable privacy approach for the technology level of ethical analysis. I have used this approach as a checklist to identify privacy issues and I have categorized them according to the type of privacy that is (at risk of being) violated.

The following five groups of privacy concerns are discussed: *issues relating to behavioral privacy*; *issues relating to privacy of location and space*; *issues relating to associational privacy*; *issues relating to privacy of property*; and *issues relating to privacy of data and image*.

Issues relating to behavioral privacy

Let us first discuss issues relating to *behavioral privacy*. As explained in section 5.3, behavioral privacy encompasses the right to behave in public, semi-public or one's private space without having one's actions monitored or controlled by others (Finn et al., 2013). Some aspects of human behavior may be sensitive in nature, such as sexual activities, religious practices and political activities, and people may experience a psychological need for "seclusion", even in public spaces (Clarke, 2014). Protection of behavioral privacy ultimately contributes to the development and exercise of autonomy and freedom in thought and action (Finn et al., 2013).

Surveillance-oriented drones can generally make fairly detailed observations of the activities of many persons within their field of view, and are likely to do so regardless of whether the observations are warranted for most individuals within view. Some behaviors in drone-observable public or private spaces, such as ecstatic behavior in a crowd at a rock concert, could hurt or embarrass the person engaging in them if they became known to others. Moreover, most people do not like it when their behavior is monitored and recorded in spaces where no monitoring and recording is reasonably expected to occur, such a quiet park or a backyard.

The potential for negative impacts is especially significant since drone surveillance is much less overt and can be more persistent than closed-circuit television or helicopter surveillance, to which it is frequently compared. It has been argued that the mass deployment of surveillance drones imperceptible from the ground "could lead to an environment where individuals believe that a UAS is watching them even when no UASs are in operation" (McBride, 2009, p. 659). Participants in a particular social context in outdoor space might have their ability to read the circumstances of this context diminished, becoming less clear on who their actions are accessible to and in what circumstances their actions may be reviewed. This could have a self-disciplining effect, as famously theorized by the philosophers Jeremy Bentham (1984) and Michel Foucault (1979), where people adjust their behavior to the ever-present possibility that they are being watched—in the case of drone use, by *unknown others* in *unknown contexts* (i.e., for law enforcement, commercial, private use, criminal, or other purposes).

The term "chilling effect" is used to refer to a decrease in the legitimate exercise of civil liberties and rights, such as freedom of assembly or freedom of expression, which happens when individuals are discouraged from participating in social movements or public dissent activities for fear of being under surveillance (Clarke, 2014). This "chilling effect" is frequently observed in situations where people are under generalized covert surveillance (Finn et al., 2013). As will be shown in chapter 6, the "chilling effect" of

drone surveillance may even include the deterioration of basic social interaction in outdoor public space. Furthermore, according to Roger Clarke (2014), drone surveillance may generate a sentiment that "they know all about you anyway", which in turn may result in "hypervigilance" or even "paranoia" among people who are at risk of developing these conditions.

A key factor determining the intensity of the "chilling effect" is the level of uncertainty on the part of the public about the specifics of drone surveillance. The less is known about the particular drone that is or could potentially be in the air—the particular type of drone, its payload, its location, its operator, and its purpose—the more pronounced the "chilling effect" is likely to become. Thus, even if a drone that is used by a delivery company does not monitor people, the mere presence of the drone and the inability of the public to identify what its purpose and payload may be, will (given a future state of affairs where drones with excellent surveillance capabilities exist and are frequently used) contribute greatly to a "chilling effect".

Issues relating to privacy of location and space

Another set of privacy concerns relates to *privacy of location and space*, which encompasses the right of individuals to move about in public or semi-public space without being identified, tracked or monitored; the right to solitude; and the right to privacy in spaces such as the home, the car or the office (Finn et al., 2013; see section 5.3). These rights contribute to one's sense of living in a democracy and one's experience of freedom, thus encouraging dissent and freedom of assembly (Finn et al., 2013).

Drone technology capable of public surveillance infringes upon privacy of location and space in that drones are almost unavoidably used to locate and track people, whether intentionally or unintentionally, and undermine their expectations regarding the boundaries of personal space. Drones fitted with cameras are very likely to capture images of a person or a vehicle in outdoor public space, thus placing individuals in particular places at particular times and perhaps revealing their movements through public space if more than one image is captured. A comprehensive record of a person's movements can reveal sensitive personal data such as familial, political, professional, religious and sexual details. In the hands of a stalker, an advertising agency or even the police, drones may thus result in a multitude of privacy breaches, and potentially inflict injury on the surveillance subject.

In addition to breaching privacy of location, drones may also cause intrusion into some spaces historically recognized as private. For example, drones can capture images of backyards and—especially when flying low and making observation from particular angles—reveal information about activities within homes, offices or other apparently private spaces. Thus, individuals who assume that their activities are not being monitored because they occur within the home or within other private spaces may find that this assumption is false. The fact that the capture of information from private spaces can be covert makes it particularly problematic.

Issues relating to associational privacy

A third category of privacy concerns relates to *associational privacy,* which refers to the right of individuals to associate with whomever they wish, without being monitored (Finn et al., 2013). This right benefits a democratic society as it fosters freedom of speech, including political speech, freedom worship and other forms of association (Finn et al., 2013).

Drone technology capable of public surveillance presents a threat to privacy of association through the ability of drones to (covertly) monitor individuals and crowds. Much of the drone footage shot in public may unintentionally contain information about the groups and individuals a person associates with as well as the nature of this person's relations with these groups and individuals. Drone technology may also make it easier to purposely gather information about one's associations. For example, in the commercial sector, a corporate spy could utilize a drone to identify organizations that senior staff members of a competitor company are secretly associating with for a breakthrough future innovation. Such usage of drones would be hard to prevent. Instead of individuals, groups can also be taken as a starting point. For example, at large protests the number and organization of participating individuals can be analyzed from drone footage, and group membership can be inferred.

Issues relating to privacy of property

A fourth category of privacy concerns relates to *privacy of property*, which, as I have proposed in section 5.4, encompasses a tentative right to not have one's property monitored and analyzed in spaces such as one's house or backyard. Such a right would likely contribute to an individual's autonomy and various forms of freedom, such as freedom of expression.

Drones equipped with cameras are able to shoot detailed and extended wide-area footage that is likely to include backyards and some interior areas of people's houses. A lot of sensitive personal information can be inferred merely by monitoring and analyzing a person's belongings in these semi-publicly visible private spaces. For example, a drone enthusiast could use a drone to peer through her neighbor's bedroom window to observe this person's intimate belongings. Provided the drone is fitted with a good camera, she need not even trespass on her neighbor's property in order to do this. Another example would be a situation where a roof insulation company uses a drone equipped with thermal cameras to identify houses that have poor insulation, so it can make targeted offers to potential customers.

Issues relating to privacy of data and image

A fifth and final category of privacy concerns relates to *privacy of data and image*—also known as *data protection*—which refers to the right to have one's personal data protected and to exercise a substantial degree of control over that data and its use (Finn et al., 2013). Having control over one's data builds self-confidence and enables individuals to feel empowered, and has social value in that it addresses the balance of power between the state and the person (Finn et al., 2013).

Surveillance-capable drone technology risks infringing upon privacy of data and image since it is unavoidable that many drone users are going to store and use the personal data they capture with their drones. Now, before we analyze drones in terms of their precise impact on privacy of data and image, it is useful to further operationalize the right to data protection. There exists a very influential set of data protection principles that will help us here, which is the *Guidelines Governing the Protection of Privacy and Transborder Flows of Data* of the Organisation for Economic Co-operation and Development (1980). This was the first internationally agreed-upon set of privacy principles, and formed the basis of the *EU Data Protection Directive* (*Directive 95/46/EC*). It contains the following principles:

- "*Collection limitation principle.* There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- *Data quality principle.* Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, compete and kept up-to-date.
- *Purpose specification principle.* The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- *Use limitation principle.* Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [Principle 3] except: (a) with the consent of the data subject; or (b) by the authority of law.
- *Security safeguards principle.* Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- *Openness principle.* There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- *Individual participation principle.* An individual should have the right:
  a) to obtain from the a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
  b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
  c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and
  d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- *Accountability principle.* A data controller should be accountable for complying with measures which give effect to the principles stated above."

There are three general aspects of surveillance-capable drones that contribute to a risk that some of these principles are violated by the use of such drones. These are (1) the *invisible and distanced collection of data*, (2) the *indiscriminate and mass collection of data*, and (3) the *wireless transmission of data*. They are derived from the definition of surveillance-capable drones and additional general characteristics provided in the introduction of this section.

Let us first have a look at the impact of invisible and distanced collection of data. Specialized, high-resolution cameras with telephoto lenses enable drones to shoot film and take photographs from distances at which the relatively small aircraft are hardly noticeable by the people they observe. Furthermore, drone operators themselves are usually also far removed from, and thus invisible to, the data subjects. This capacity for invisible and distanced data collection adds significantly to the risk of violating several of the abovementioned data protection principles. Firstly, there is an increased risk of infringement of the *openness principle*, since it is easy for drone operators to covertly record and process personal data. Secondly, the *collection limitation principle* and the *use limitation principle* are at a greater risk of being

violated. This is because some personal data collected by drones may be of such sensitive nature that its collection requires data subjects' knowledge or consent, which, as a result of the invisible and distanced collection of data, is likely not always guaranteed. Finally, the *purpose specification principle* is at risk of being breached, since the purposes of the personal data collection may frequently not be communicated to the data subjects.

Let us now turn to the effect of indiscriminate and mass collection of data. Owing to their mobility and wide-area viewing capability, drones can record massive amounts of personal data in an indiscriminate way. Such mass collection of personal data way may cause several breaches of the above data protection principles. Firstly, it is likely to violate the *collection limitation principle* and the *data quality principle*, since much of the personal data collected may frequently be irrelevant and sometimes excessive to the goal that is pursued. For example, a commercial drone fitted with a high-definition camera for inspecting 100-meter high power lines in a rural area, captures and records images of those power lines, as well as residential gardens visible in the background (Finn & Wright, 2012). It is clear that in many situations—especially in densely populated urban areas—non-trivial amounts of irrelevant personal data are incidentally collected by drones. Secondly, indiscriminate and mass collection of personal data risks breaching the *use limitation principle*, since with great amounts of personal data captured and stored, individuals in charge of its use may at some time in the future be tempted to use the data for purposes that go beyond its stated purpose, and do so without the data subjects' knowledge or consent. An example of this is the police deploying a drone to take high-resolution footage of a road accident in dangerous conditions and sometime later using the footage to identify drivers who have violated traffic rules (Finn & Wright, 2012).

Finally, there is the impact of wireless data transmission. The wireless transmission of collected data from a drone to a data controller poses security risks to this data. Those with some degree of knowledge of wireless communication protocols may be able to secretly intercept sensitive personal data that is send out by drones. Wireless data communication is inherently less secure than wired communication. Recently, a team of developers of the company Groupon hacked a drone at the "Drone Games" and used it to take photographs of the public (Geffray, 2013). They then applied a facial recognition algorithm to the footage, added in the names of the persons who were identified, and finally posted it on Twitter. Wireless data transmission by drones may thus harm the *security safeguards principle* if the security of wireless transmission of sensor data can easily be breached.

Besides violations of the OECD's data protection principles by these three aspects of drones, it might also be fitting here to mention the risk of *combining data sources*, which seems to be an almost inevitable part of many new information and communication technologies. Drone data may be combined with closed-circuit television (CCTV) footage, road-side license plate scanners, and so forth (see chapter 3). As explained in chapter 4, combining seemingly worthless pieces of information of an individual from various contexts can constitute a privacy invasion since those pieces of information can together be transformed into a rich portrait of the individual (Nissenbaum, 1997). *Profiling* and *data mining* are techniques that allow sensitive personal information to be synergized from seemingly innocuous pieces of data across different data sources (more on profiling in subsection 5.1.2). These techniques may reveal personal or private information about an individual's behavior and preferences that the individual might not even be aware of herself (Hildebrandt & Gutwirth, 2008). The combination of drone data and other sources of data may thus worsen the impact of drones on various types of privacy.

5.1.2 Other ethical issues

We have now discussed all issues relating to privacy that are inherent in surveillance-capable drone technology. Beyond issues relating to privacy, there are a few other ethical issues inherent in this technology. The non-privacy issues that I have identified from the drone literature and my own reasoning are: *function creep*; *unequal burden of surveillance*; *discrimination*; *abuse, errors and accountability*; and *shifting ethical norms*. I will now discuss these in turn.

Function creep

Various authors, such as Roger Clarke (2014) and Joseph Nevins (2011), have warned about the risk of *function creep* in the case of drones. Function creep is the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended. Since surveillance-capable drone technology has a wide array of potential applications, drones may be purchased for specific, restricted operational uses, but used for wider, more controversial purposes. An example of this would be the situation mentioned earlier where the police deploy a drone to take high-resolution footage of a road accident in dangerous conditions and later use the footage to identify drivers who were violating traffic rules (Finn & Wright, 2012). Another example could be a situation where a law enforcement agency purchases drones to help with search and rescue missions in remote areas, but ends up using them primarily to find drug plantations and to follow potential drug traffickers in these territories. Function creep can have a profound impact on various types of privacy (as well as on the values supported by these types of privacy, such as freedom and autonomy) and on other values, such as equality (see next item) and health/safety.

Unequal burden of surveillance

Even before considering discrimination issues, which I will do shortly, it can be argued that surveillance-capable drone technology is likely to affect some groups of people more than others. Notably, people who, sometimes of necessity, spend a lot of their time outdoors in public spaces bear more than their fair share of the negative impacts of drone surveillance. Waste collectors, gardeners, couriers, and police patrolmen, among other groups, are likely to suffer unwarranted privacy incursions at an increased rate by the simple fact that drones are likely to collect more sensitive personal data on them through their ability to collect massive amounts of data in a dragnet-like fashion.

Discrimination issues (especially for surveillance applications)

As just mentioned, there are also discrimination issues concerning drones. To the extent that surveillance-capable drone technology will unavoidably (legally or illegally) be used for security surveillance applications by organizations and private individuals alike, an inherent risk of such technology is *discriminatory targeting*.[21] Discriminatory targeting in surveillance practices increases social alienation and distrust among affected individuals and groups, and undermines social cohesion (Finn & Wright, 2012). The risk of discriminatory targeting is tied to the inevitable human component in the functioning of the technology. In the United Kingdom, security closed-circuit television (CCTV) operators have been found to focus disproportionately on people of color; according to Norris & Armstrong (1997), "[b]lack people

[21] This concern could perhaps be seen as fitting best at the application level of analysis under "surveillance applications". However, considering the fact that such applications are such a prominent and likely outcome of the technology, I think it is worth mentioning the issue here.

were between one and a half and two and a half times more likely to be monitored than one would expect from their presence in the population." Such focus on people of color is likely due to CCTV operators acting on their prejudices and biases (Stanley & Crump, 2011). More generally, Coleman & McCahill (2011) have argued that "'new' surveillance technologies reinforce 'old' social divisions—particularly along the lines of class, race, gender and age." Drones fitted with cameras can act as mobile CCTV cameras, so it is not unreasonable to expect that discriminatory behaviors also correlate with the use of these systems. It can even be argued that these behaviors are likely to be more pronounced in the case of drones, since the mobility of drones may give operators the freedom to monitor locations of their own choosing (thus giving them more opportunity to express their prejudices and biases). Surveillance would not necessarily be bound to specific pre-determined locations, as in the case of CCTV systems.

Another, more sophisticated source of unfair discrimination could be *profiling*. In the information sciences, profiling can be defined as "[t]he process of 'discovering' correlations between data in data bases that can be used to identify and represent a human or nonhuman subject (individual or group), and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category" (Geradts & Sommer 2006, p. 41). Profiling can be applied in a variety of different domains and for a variety of purposes, and larger collections of data increase its usefulness. Profiling practices are by their very nature discriminatory. They generate unparalleled levels of social sorting and segmentation which could have unfair consequences. For example, law enforcement agencies and private security companies could have their drones focus on people whose appearances and behaviors ("young; male; person of color; baggy jeans; loitering on a street corner") seem to correlate with criminal behavior on the basis of profiling techniques. We could also imagine a situation where insurance companies adjust the rates of their clients after identifying their "lifestyle profile" on the basis of drone footage of their homes and the surrounding neighborhoods. To be sure, unfair discrimination is not the only impact of profiling practices using drones. Other impacts could include impacts on privacy (as stated in section 5.1.1), due process, security and liability.

Abuses, errors and accountability

There is a significant potential for abuse, error and accountability issues inherent in surveillance-capable drone technology. These concerns are related in that they result in part from the ability of drones to operate in a covert manner, which contributes to a lack of transparency and consequently a lack of accountability.

There is a significant risk that drone technology will be abused by government agencies, commercial companies and private users. For government agencies and private security companies, drones may appear to be a perfect candidate for blanket surveillance activities. Drones can be used covertly and offer an extensive range of surveillance capabilities. Recent revelations about secret government surveillance programs, such as PRISM, show that government agencies in some countries possess an eagerness to take the use of surveillance technologies to the limits of their capabilities for the sake of national security, even if there is no democratic mandate and no widely acceptable moral justification for doing so. Drone technology may, too, become a tool for institutional abuse.

Abuse may also be committed at a wider level, by government agencies, commercial companies and private individuals, for personal and sometimes criminal purposes. As Clarke (2014) explains: "[D]rone pilots and operators of onboard facilities are remote from their target, and operate in the virtual reality created by

their data-feeds. Their detachment from the physical reality of the individual in their sights tends to weaken the constraints of conscience, and loosens at least some of the psychological and social controls that apply 'in meatspace' [sic[22]]. This gives rise to a risk of operators engaging in voyeurism, harassment, stalking, and even acts of gratuitous violence." For the same reasons, corporate espionage may also flourish, since corporate spies do not have to be on-site when they are utilizing a drone.

The lack of transparency in drone use also increases the risk of *errors* committed by law enforcement and other users, since there are fewer people to pick up on and prevent such errors. In addition, drones themselves and the software they run can be prone to causing errors. The risk of human errors is compounded by the fact that a single drone offers only one perspective on a situation. Clark (2014) argues that as a result of such a limited view "[m]any cases of mistaken identity arise, fuelling rumours and innuendo." Furthermore, he states that "[i]mages and video recordings, particularly when taken from above the object being observed, and especially when presented by government agencies, are invested with importance that it may or may not merit." In turn, "[r]efutation of unjustified accusations is very challenging in the 'court of public opinion' and even in courts of law."

Finally, the lack of transparency also raises issues in terms of accountability, which in turn contribute significantly to the problems of abuse and errors just described. As drone surveillance can be covert and carried out by virtually anyone, the ability to detect those responsible for the surveillance is diminished. The European RPAS Steering Group (2013) has stated that the "low cost of operation [of drones] and their small size, together with the difficulty of controlling their use through licensing or registration systems, could make it very difficult to ensure that they are used in a lawful and legitimate way" (p. 27). The accountability problem is compounded by the fact that drones will be able to function autonomously to some degree, and that they can be hacked and taken over in flight (Clarke, 2014).

Shifting ethical norms

In chapter 4, the following question was raised: What if societal norms gradually shift to adapt to increased privacy incursions by future drone use? It is quite possible that some policy makers and drone operators will aim to let privacy issues and other ethical issues resolve themselves by waiting for the norms to adapt to the new drone practices. However, any shift in ethical norms as a result of drone use may be unethical if the new norms are conducive of practices that violate fundamental civil and human rights such as those outlined in the United Nation's Universal Declaration of Human Rights and the Council of Europe's European Convention on Human Rights. These time-tested and widely-accepted fundamental rights ought to be our ultimate moral guide stone—not the fleeting societal norms that could potentially be highly unfair if they are a reflection of power inequities in society.

It is worth noting that privacy laws and policies that are based solely on public norms or expectations, such as privacy laws in the U.S., may not offer adequate protection of a supposed fundamental right to privacy in the face increased drone use. Ryan Calo (2009), for example, has remarked that surveillance robots could "operate to dampen constitutional privacy guarantees by shifting citizen expectation" (p. 2).

[22] Meatspace is an informal term used to refer to the physical world. It stands opposed to and should not be confused with the term *metaspace*, which refers to cyberspace or a virtual environment.

5.2 Issues inherent in specific drone categories

Now that we have discussed all ethical issues at the technology level, we can have a look at the issues presented by drones at the artifact level, which are specific to particular types of drone. According to the ATE approach, ethical analysis at this level focuses on types of artifacts and processes that have resulted or are likely to result from a particular technology (Brey, 2012). The analysis considers features of them that present moral issues. As was the case at the technology level, such moral issues may present themselves for three reasons: because of the inherent character of the artifact, because the artifact has certain unavoidable consequences in most or all of its uses, or because certain potential applications of the artifact are so risky or morally controversial that the artifact warrants reflection on the ethical justification of its manufacture. I will now describe the most important of these ethical issues for the three types of surveillance-capable drones that I have identified in chapter 3, which are the *large wide-area persistent surveillance drones*, the *small general-purpose drones*, and the *biomimetic spy drones*. Furthermore, I will describe the ethical issues presented by various advanced sensor systems and onboard data analysis systems that may be present in some of these types of drones but are not considered essential features of any of these types.

Before we begin, it deserves to be emphasized that all of the ethical issues at the technology level apply to each of the three types of surveillance-capable drones. So, the issues that are now presented can be considered an extension to the issues of section 5.1 *for each type of drone individually*. Furthermore, whereas none of following issues is present in all three categories at once (*ergo*, in drone technology at large), some of them still present themselves in more than one category of drone.

5.2.1 Large wide-area persistent surveillance drones

Let us first consider the ethical issues that are inherent in large wide-area persistent surveillance (WAPS) drones. In chapter 3, these drones were defined as large, technologically advanced systems that have great endurance and offer so-called *persistent surveillance* capabilities over an extensive ground area. Automated person tracking systems are considered an essential future feature of these drones. Two issues are inherent in large WAPS drones, which are *increased moral distance to surveillance subjects* and *safety of flight*.

Increased moral distance to surveillance subjects

In subsection 5.1.2, I mentioned Roger Clark's (2014) argument that the remoteness of drone pilots from their targets might cause in these pilots a detachment from the physical reality of the individuals who are in their sights, which may weaken the pilots' constraints of conscience and increase the risk of their committing abuse. The tem "moral distance" is sometimes used in relation to the general observation that one's moral behavior toward another person is negatively affected by increased (perceived) physical or temporal distance, and thus psychological distance, to this person.[23] Although I think Clark's argument applies to drones in general, I believe that this "moral distance" effect on the relation of drone pilots with their surveillance subjects will be especially pronounced in the case of *large wide-area persistent surveillance drones*.

[23] Physical distance tends to increase moral distance. For example, it is known in military psychology that, in general, killing from a distance is easier than killing at close proximity (Grossman, 1996). This is in part due to the fact that with increasing distance there is decreasing knowledge of the suffering one causes, and therefore decreasing empathy for one's victims. A natural moral-psychological barrier to killing is thus being removed.

Large wide-area persistent surveillance drones tend to operate at a much greater distance from their targets than do small general-purpose drones and biomimetic spy drones. This means that even with the best high-resolutions cameras they cannot capture images with the same level of detail in a particular situation as images captured by general-purpose drones and biomimetic drones. In addition, they are generally taking footage from angles that are worse, as their options to maneuver to optimal vantage positions are more limited. Consequently, the images they capture are less clear and vivid representations of a particular situation, which has the effect that the drone operators experience less intimacy with their targets. These intimacy-reducing effects are mitigated to an extent by the fact that the operators of large wide-area persistent surveillance drones have the opportunity to become familiar with their targets through extremely long periods of observation. This opportunity depends on the level of automation of the surveillance and the level of attention paid to individual targets, among other factors. Nevertheless, I think it is safe to say that usage of these large drones will still engender less intimacy during surveillance than usage of general-purpose drones and biomimetic spy drones. Thus, moral distance is increased, which may increase the incidence of abuse and neglect of surveillance subjects' rights.

Safety of flight

The use of *large wide-area persistent surveillance drones* may carry safety risks, although arguably not to the extent of small drone use. As they are primarily used by law enforcement organizations and private security companies, large drones are likely to be operated and maintained in a more responsible way and thus likely to be more reliable. Furthermore, since they are larger and inevitably much more expensive, they may be designed and manufactured with higher safety standards in mind. Finally, there are likely to be far fewer of them in sky at any one time—although when they are involved in accidents, these accidents are likely to be worse than accidents involving smaller drones.

For the near future, however, it can still be expected that large wide-area persistent surveillance drones are not going to be as safe as traditional manned aircraft. This can be inferred from the safety record of their military equivalents, which is not nearly as good as that of manned aircraft. Manufacturers of large military surveillance drones have yet to overcome significant safety hurdles, which include: a limited ability to detect and avoid trouble; pilot error; persistent mechanical defects; and unreliable communications links (Whitlock, 2014). All of these problems increase the risks for other (passenger) aircraft and people on the ground. Only one of these—the unreliability of communications links—may be a permanent issue with large wide-area persistent surveillance drones, due to the fact that wireless communication makes drones inherently vulnerable to hacking.

5.2.2 Small general-purpose drones

Let us now consider the ethical issues that are inherent in small general-purpose drones. In chapter 3, these drones were defined as systems that lack the range, the speed, the wide-area perspective, and the sophisticated sensor payload of WAPS drones, but are much cheaper and easier to procure, operate, and maintain, and can observe and record scenes in high detail from up close and from many different angles, thus making them highly versatile. In terms of their sensor capabilities, only visual-spectrum cameras are considered here. Two ethical issues are found to be inherent in small general-purpose drones, which are *concerns about privacy of the person* and *safety of flight*.

Concerns about privacy of the person

There is a set of privacy concerns specific to small general-purpose drones that relates to *privacy of the person*, which refers to the right to keep one's body functions and body characteristics (such as genetic codes and biometrics) private (Finn et al., 2013; see section 5.3). This right is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society (Finn et al., 2013).

Small general-purpose drones may infringe upon privacy of the person if they are fitted with high-resolution photo cameras, or other types of sensors and data analysis systems, such as integrated facial, voice, or "soft-biometric" recognition systems (see chapter 3 and subsection 5.2.4), which allow various biometric properties of a surveillance subject to be recorded and analyzed. With many small drones in the very least being equipped with powerful camera systems, there is a substantial inherent risk of such an infringement on privacy. This risk is also present in biomimetic spy drones, but not in large WAPS drones, which is why it is listed here and not at the technology level. In spite of their high-resolution sensors, large WAPS drones generally operate from too far a distance to capture detailed biometric data of individuals.

The threat to privacy becomes even greater if connections are established with biometric databases and other surveillance systems, since this would enable small drone systems to identify almost anyone within their field of view and track individuals much more persistently. These capabilities may be enticing to law enforcement agencies and private security companies. They would compound the impacts on other types of privacy, such as behavioral privacy, privacy of location and space, and associational privacy. Furthermore, reductions in bodily privacy could also further increase the risk of discrimination, since the increased access to various kinds of biometric data offers a greater potential for profiling.

Safety of flight

Large-scale deployment of *small general-purpose drones* carries significant flight safety risks. Small drones are cheap and available to anyone—law enforcement, commercial companies, private citizens, et cetera. This means that they are likely to be less well built, less well maintained, and less well piloted than manned aircraft. Moreover, massive numbers of them could be zipping through the skies in the future. Also, like large wide-area persistent surveillance drones, they are inherently vulnerable to cyber-attacks. Even with proper standards and regulations in place, the risks other (passenger) aircraft and people on the ground could be significant. It has been reported that the current accident rate for drones is a hundred times that of manned aircraft (King, Bertapelle & Moses, 2005).

5.2.3 Biomimetic spy drones

Let us now turn to the ethical issues that are inherent in the final category of drones, the biomimetic spy drones. In chapter 3, these drones were defined as very small systems that can hide in plain sight through mimicking the size and behavior of insects and birds, and as such have a great future potential for covert surveillance applications. In terms of their sensor capabilities, only visual-spectrum cameras are considered here. Three issues are found to be inherent in biomimetic spy drones, which are *concerns about privacy of the person*, *increased potential for privacy harms*, and *potential harm to (the experience of) wildlife*.

Concerns about privacy of the person

Like small general-purpose drones, biomimetic spy drones may infringe upon *privacy of the person* if they are fitted with sensors that allow various biometric properties of a surveillance subject to be recorded and analyzed. Since they are generally able to come closer to their targets due to their ability to hide in plain sight, biomimetic drones can use visual-spectrum cameras capture additional types of biometric data of their targets. Beyond plain imagery of people's faces, they might be able to obtain fingerprint data, and iris pattern data, all of which are very sensitive kinds of biometric data. Therefore, the use of these drones may constitute an even greater violation of privacy of the person.

Increased potential for privacy harms

Compared to large wide-area persistent surveillance drones and small general-purpose drones, biomimetic spy drones may have a somewhat stronger impact on privacy. Due to their ability to hide in plain sight, they can come closer to a person without being noticed than any other type of drone, which means that they can generally observe a given situation from better vantage points. Provided they are equipped with sensors of sufficient capability, they can covertly gather better data on people's behavior, their location, their property and their relations with other people. Therefore, their use may exacerbate some of the privacy issues listed for drone technology in section 5.1, such as behavioral privacy, privacy of location and space, privacy of property and privacy of association. The increased potential for privacy harms may in turn have other ethical impacts, such as an increased potential for unfair discrimination and various kinds of abuses. Since the development of biomimetic drones still has a long way to go, all of these issues are not near-term concerns, although they could become pertinent in 20 years time.

Potential harm to (the experience of) wildlife

Biomimetic drones could harm wildlife through their likeness to specific types of animals. Their existence may evoke aggression in people who dislike the possibility that they are being watched, which could result in physical harm to the animal species whose likeness is borne by these drones. When used in large numbers, they may also affect the normal behavior of insects and birds nearby and cause physical harm if for example an insect-like drone is consumed by a bird. Biomimetic drones might even adversely affect entire ecosystems. For instance, could the large-scale presence of insect-like drones have an impact on the pollinating behavior of local bee populations?

Furthermore, in areas where they are present, biomimetic drones may prevent people from experiencing wildlife in a pure, authentic form. Visitors of nature parks might not be able to reap the full psychological rewards of experiencing nature if in the back of their heads there is the ever-present possibility that they could be tricked by a drone pretending to be a butterfly.

5.2.4 Advanced additional features of drones

We have now discussed the ethical issues that are inherent in all three types of surveillance-capable drones. Since we only considered them in their most essential forms, we have left unanalyzed a range of potential additional features of drones. Therefore, I will now describe the ethical issues presented by the most important sensor systems and onboard data analysis systems that in fifteen years may "optionally" be present in (some of) the three types of drones. To be sure, an exhaustive analysis of all of these potential additional systems probably requires a chapter of its own. However, due to space constraints, I will stay

rather brief on this subject. Nonetheless, is highly advisable that the impacts of assorted sensor and data analysis systems are explored in further detail.

Additional sensor systems

Besides basic visible-spectrum cameras, drone-mounted sensor systems can include GPS systems, multispectral, thermal, and night vision imaging sensors, radar-based sensor systems, and so forth (see chapter 3). I will not discuss the impacts of these systems individually, as I do not have the space to do so here. Instead, I will briefly discuss them in general terms.

The additional sensor systems enable drone operators to gather more detailed information on people's behavior, their location, their property and their relations with other people. For example, multispectral, thermal, and night vision imaging sensors, as well as radar-based sensor systems, make it easier to discover individuals in foggy conditions, through tree foliage, and inside buildings (see chapter 3). Thus, their use may exacerbate all of the privacy issues mentioned so far, which include behavioral privacy, privacy of location and space, privacy of property, privacy of association, privacy of data and image, and privacy of the person. The increased potential for privacy harms may in turn have other ethical impacts, such as an increased potential for unfair discrimination and various kinds of abuses.

Advanced onboard analysis systems

Besides various types of sensors, drones may also be equipped with advanced onboard data analysis systems. Such systems include, for example, behavioral analysis systems, biometric analysis systems, and license plate recognition systems. When drones are equipped with automated behavioral analysis systems that can detect abnormal behavior in people (see chapter 3), the "chilling effect" of drones, as described in section 5.1.1, could become more pronounced. Surveillance would be felt more intensely as any form of deviant behavior at any time could have very real consequences.

Furthermore, when drones are equipped with facial recognition or license plate recognition systems, pedestrians and vehicles may be tracked for very long periods of time, which may cause increased harm to privacy of location and space. Moreover, facial recognition systems may expedite the process of identifying individual members of groups of people, thus posing a threat to privacy of association. Facial recognition systems and other biometric analysis systems may also cause further harm to privacy of the person by gathering data on the body functions and body characteristics of people.

Finally, to the extent that these systems are automated or autonomous, they could pose serious problems in terms of ascribing responsibility for the behavior of the drone—especially if the systems are self-learning. Andreas Matthias (2004) has argued that the use of so-called *machine learning technologies* will have serious ethical implications, for these technologies give rise to what he calls the "responsibility gap". Traditionally, the producer (designer or manufacturer) or the user (owner or operator) of a machine is held responsible for damages resulting from the machine's operation. The producer may be held responsible when the accident is a consequence of a (preventable) design or manufacturing error. The operator may be held responsible if the accident happened due to incorrect operation of the machine. Autonomous learning machines, such as facial or behavioral recognition systems based on *artificial neural networks*, create a new situation according to Matthias (2004). With neural networks in particular, producers and users are no longer in a position to predict exactly what the machine will do in normal operating environments, and to work out an appropriate response to their prediction. This is because

neural networks are black boxes: practically speaking, we cannot have a look at the information contained in a neural network. Thus, Matthias argues, neither producers nor users are able to exert full control on the future behavior of the machine. However, a person can be held responsible for something only if she has control over it. Therefore, producers and users cannot be ascribed responsibility for damages caused by learning machines (assuming the producer did not explicitly teach the machine to cause damage). Since no one else can be held responsible, we are facing "a responsibility gap, which cannot be bridged by traditional concepts of responsibility ascription" (Matthias, 2004, p. 175). Society, according to Matthias, must decide between not using learning machines and accepting this responsibility gap.

5.3 Conclusion

In this chapter, I have used Brey's (2012) anticipatory technology ethics approach to present ethical issues inherent in drone technology at large and issues inherent in each of the three types of drones as well as some optional features of drones. I have used Finn et al.'s (2013) "seven types of privacy" approach as a checklist to identify privacy issues, and I have used a bottom-up approach to identify other ethical issues, drawing from the drone literature and from my own moral intuitions.

At the technology level, ethical issues were considered that are inherent in drone technology at large, meaning that they are at least *likely* to occur with basic surveillance-capable drones of all types in many situations. First, I discussed a series of privacy issues. It was argued that widespread use of drone technology could induce a "chilling effect" on society—a decrease in the legitimate exercise of civil liberties, such as freedom of assembly and expression—because of citizens´ fear of being under surveillance. Furthermore, it was argued that drone technology is likely to infringe upon *privacy of location and space*, since drones almost unavoidably collect data that reveal the location of people and their presence in certain private spaces. It was also explained how drone technology poses a threat to *privacy of association* through its ability to capture images of congregated individuals, and how drone technology may violate *privacy of property* with its ability to shoot aerial footage, which is likely to include backyards and other private areas. Finally, it was argued that drone technology risks violating important data protection principles through its invisible and distanced collection of data, its indiscriminate and mass collection of data, and its wireless transmission of data.

Next, I discussed a series of non-privacy issues inherent in surveillance-capable drone technology. It was argued that, since drone technology has such a wide array of potential applications, there is a risk of "function creep", meaning that drones may be purchased for specific uses, but eventually used for additional, controversial purposes. Furthermore, it was argued that drone technology's negative effects may be unequally distributed among people, in that those who spend more time in outdoor public spaces are more likely to have their data captured by drones. Next, it was explained that drone technology may contribute to a wide variety of *discriminatory targeting* and *profiling* practices rooted in prejudice and bias, which would create further inequality and subsequent harms. It was also explained how drone technology has significant potential for abuse, error and accountability issues, which partly result from the covertness with which drones operate. Finally, it was argued that drone technology may shift certain societal norms such as privacy norms, which may be unethical if the new norms promote practices that violate fundamental civil and human rights.

We subsequently turned to the artifact level of analysis, where we looked at additional ethical issues specific to particular types of drone and various non-essential features of drones. First, I discussed two

issues with *large wide-area persistent surveillance* (WAPS) drones. It was argued that these drones may induce a "moral distance" effect in drone operators due to a less intimate presentation of surveillance subjects in drone imagery. In addition, it was pointed out that large WAPS drones are, at least in the near term, likely not going to be as safe as traditional manned aircraft. Subsequently, I discussed two issues with the *small general-purpose drones*. It was explained that these drones may infringe upon privacy of the person, since their relatively close-up use of high-resolution cameras enables them to capture biometric properties of a surveillance subject. It was further argued that mass deployment of such drones may also carry significant flight safety risks. Next, I discussed three issues with the *biomimetic spy drones*. It was explained that these drones, too, may infringe upon privacy of the person because they can capture close-up imagery of their targets. It was also argued that, compared to other drones, these drones may have a somewhat stronger impact on privacy in general, due to a close-up covert positioning advantage. Furthermore, various ways were described in which biomimetic drones could harm wildlife, and the experience of it, through their likeness to specific types of animals. Finally, I very briefly considered the issues presented by various advanced sensor systems and data analysis systems that may variously be present in drones. In general, these were found to exacerbate the privacy issues described in this chapter, and, to the extent that they are autonomous and self-learning, complicate the ascription of moral responsibility for drones' behavior.

Before we head to the next chapter, let me just emphasize that as I discussed the ethical issues in this chapter, I considered these issues mostly in terms of general *risks*. For the privacy issues in particular, it is worth stressing that whether these issues become a reality depends partly on the specific social contexts (and their informational norms) in which the drones are used (some contexts are more forgiving of "privacy-invading" technologies than others). However, I consider the likelihood of these issues becoming a reality for many or most potential contexts of use to be sufficiently high for these issues to be regarded "inherent" issues with either drone technology at large or particular types of drone.

6 Evaluating drone applications

In the previous chapter, we analyzed the ethical impacts of surveillance-capable civil drones at the technology and artifact levels of Brey's (2012) anticipatory technology ethics (ATE) approach. It is now time to aim our attention at the *application level*, where the objects of analysis are applications. An application, as Brey (2012) defines it, is "the concrete use of a technological artifact or procedure for a particular purpose or in a particular context, or a specific configuration of an artifact to enable it to be used in a certain way" (p. 8). The main goals in this chapter are to ethically evaluate a select number of interesting *drone applications with public surveillance aspects*, and to draw some insights as to the ethical admissibility of civil drone applications in general. The applications that I will evaluate are set in the future and vividly presented through scenarios. From a diverse collection of future drone application scenarios created for this study, I have carefully selected four scenarios for evaluation. To conduct the evaluations, I will use the adapted version of Nissenbaum's (2010) contextual integrity decision heuristic, which for reasons presented in chapter 4 is well suited for making analyses of an emerging technology at the application level. A secondary goal of this chapter is to demonstrate the usefulness of the decision heuristic for evaluating drone applications.

Since privacy is an important part of an ethical analysis of civil drone applications, it is only natural to rely heavily on an approach such as Nissenbaum's (2010). However, at this point it needs to be explained how Nissenbaum's approach, which is ostensibly focused on evaluating issues of *privacy*, can be used to make *general* ethical assessments in which a full range of potential ethical issues is considered. The explanation is as follows: while the *descriptive* part of the contextual integrity approach is focused on identifying violations of privacy norms resulting from a practice's disturbed flows of information, the *normative* part places the identified violations of privacy norms in the context of the practice's impacts on other values, thus leading to a comprehensive ethical assessment. The normative part is in fact excellently suited for making general ethical assessments because it uses *social context* not merely to analyze potential privacy issues, but all other ethical impacts as well. As I will argue in section 6.1, which focuses on balancing conflicting ethical values, social context is a very important factor in conducting a fair "balancing" of ethical impacts.

It must further be noted that, with respect to the application level of ethical analysis, I deviate from Brey's (2012) ATE approach in the sense that I use Nissenbaum's decision heuristic to both *identify* and *evaluate* ethical issues in one go, thus combining the ATE approach's *identification stage* and *evaluation stage* of ethical analysis. This is done because it is more convenient and more clarifying to apply the decision heuristic in whole each time we use it. Moreover, as I will explain in the next chapter, it is useful to evaluate first the drone *applications* since their evaluations inform the evaluations of drone technology and drone artifacts in terms of their ethical admissibility.

This chapter starts out with a section on how to balance competing ethical values in ethical evaluations. Since Nissenbaum's (2010) decision heuristic falls a bit short in this area, I supplement it with a description of some important balancing rules and pointers, which I use in my ethical evaluations here and in the next chapter. Then, in the second section, I use the decision heuristic to evaluate four future application scenarios. Finally, the chapter ends with a short concluding section that summarizes the

conclusions of the ethical evaluations and other findings of this chapter. In the next chapter, I use some of these conclusions in the final ethical evaluations at the technology and artifact levels.

6.1 Balancing conflicting values in ethical evaluations

Before we start applying the decision heuristic to the scenarios, a few things need to be said on how to resolve value conflicts in an ethical evaluation, which often pose a daunting problem for ethicists. For example, technologies that promote security and efficiency frequently have detrimental effects on privacy and associated values such as freedom, autonomy and democracy. When there are conflicting ethical values in an ethical evaluation, the notion of "balancing" or "trading off" often comes into play. Balancing is a metaphor, which assumes the shape of a scale: on one side are the goals to be achieved in terms of the promotion of particular values, and on the other side are the detrimental effects in terms of the limitation of other values, which often include human rights.

Not all may agree that balancing is a valid concept. An important objection raised against it refers to the *consequentialism*[24] that lies behind it; many ethical values are associated with rights, and rights discourse is often resolutely anti-consequentialist. To apply a cost-benefit analysis to a fundamental right is to succumb to the "tyranny of the majority" according to Ronald Dworkin (2006). Another objection is that the concept of balancing favors a *value monist* meta-ethical position and assumes that all fundamental values can be compared to one another (i.e., that they are *commensurable*).[25] This is not the place to delve into lengthy debates about these issues. It is my view that in "real-world" ethical cases it is often sensible to apply a balancing method whenever there are value conflicts, as this avoids situations where one is obligated to assume non-consensual, partisan ethical positions that can be considered "extreme"; balancing is thus a pragmatic solution to conflicts. However, it does essentially imply that one is taking the side of consequentialism and value monism. In what follows, I describe some important balancing rules and pointers that I use in my ethical evaluations here and in the next chapter.

First of all, if a technology, artifact or application is to be considered ethically justified, it has to represent a net gain when its benefits are weighed against its costs. (Thus, a gain in security should more than make up for a loss in privacy.) This requirement is called *proportionality stricto sensu*. Legal scholar Aharon Barak (2010) offers a fleshing-out of the concept that helps us to establish whether the benefits are proportional to the costs. In answering the question of how to determine the weight of each side of the scale, he contends that "the criterion is that of the relative *social importance* attached to each of the conflicting principles or interests at the point of conflict" (p. 7). Thus, we are to weigh the importance to society of the supposed benefits of a technology, artifact or application against the importance to society of preventing its costs. Of course, not all values are of equal social importance. What are primary values, Barak argues, depends on a society's own circumstances, reflecting its unique challenges, history, and self-perception. In addition to the social importance of the benefits and costs, we are to consider the urgency of achieving the benefits and probabilities that the benefits and costs will be realized. Furthermore, Barak argues that the comparison is actually between the *marginal* benefits to the realization of particular values

[24] Consequentialism is the class of normative ethical theories holding that the consequences of one's conduct are the ultimate basis for any judgment about the rightness or wrongness of that conduct.

[25] *Value pluralists* may disagree with the value monists and could argue that many fundamental values lack a common standard of comparison—an overarching goal, such as happiness. If values are incommensurable, balancing is not rationally possible.

and the *marginal* costs to the realization of other values, meaning that it is concerned with the marginal and the incremental with respect to the current situation. Finally, Barak also states that we must consider the existence of proportionate alternatives that perhaps have better benefits or are less costly. Barak's proportionality requirements culminate into a "basic balancing rule" that holds: "To the extent that greater importance is attached to preventing the marginal limit to a human right and to the extent that the probability of the right being limited is higher, the marginal benefit to the public interest brought about by the limitation must be of greater importance, of greater urgency, and possessing a greater probability of materializing" (p. 11).[26]

Besides these proportionality requirements, there are other things to consider for a proper balancing of values. Nissenbaum (2010) has some interesting things to say about the topic since balancing is an essential step in her decision heuristic. Indeed, the contextual integrity approach is not solely concerned with identifying and evaluating informational privacy violations. In the decision heuristic, privacy violations of a practice that is affecting information flows are eventually placed in the context of the practice's impacts on other values, thus leading to a comprehensive ethical assessment. The starting point of the approach is, however, always disturbed flows of information, which in our case is not a problem since with drones we are always dealing with many of such disturbed flows of information. Let us consider some of Nissenbaum's views on balancing.

Firstly, Nissenbaum (2010) warns us not to conflate *values* and *interests* in balancing. Value conflicts may be misconstrued is if interests are presented as values. For example, cases of nonconsensual collection, aggregation, and sale of personal information by businesses are often presented as a direct conflict of values—efficiency or liberty is pitted against privacy. In many instances, according to Nissenbaum, a closer look reveals that costs and benefits are unevenly distributed and that because benefits accruing directly to businesses come at a cost (or potential cost) to individuals, this conflict is more appropriately understood as a conflict of interests. Nissenbaum argues that for a resolution to be morally defensible "it should at least rise above brute competition among interest-based constituencies; it should also limit consideration only of demonstrably legitimate claims, and should be constrained by the requirement that the distribution of costs and benefits be a just one" (p. 111).

Secondly, Nissenbaum argues that contextual goals, values and ends are very important to consider in balancing. Whereas Barak (2010) believes that in the balancing process the weights given to the potential benefits and costs should be functions of the general social importance of these benefits and costs, Nissenbaum (2010) contends that the assigned weights should mainly depend on the specific context at hand. For full normative evaluations, she recommends comparing entrenched normative practices against novel alternatives or competing practices on the basis of how effective each is in supporting, achieving, or promoting relevant *contextual goals, values and ends*. For example, important values of an airport context will likely include safety, security, and efficiency of movement, so the benefits and costs associated with these particular values should be given the most weight in balancing when one is evaluating a new practice in an airport context.

[26] In his essay, Barak (2010) argues that this basic balancing rule can be translated into "principled balancing rules" that deal with the balancing of specific values, rights and interests. Although the use of such rules may be helpful, their creation requires a lot of work and falls outside the scope of this thesis.

Nissenbaum (2010) has stated that her balancing approach was influenced by the idea of *spheres of justice*, developed by political philosopher Michael Walzer (1984). A brief exposition of this idea may offer a better understanding Nissenbaum's balancing approach (and, I think, contextual integrity in general). In Walzer's pluralistic account of distributive justice as *complex equality*, a just society is one in which social life is made up of autonomous spheres defined by their ideologies and social goods. These social goods include such things as wealth, political office, honor, commodities, education, security and welfare, and employment. They are distributed not according to a single criterion, or principle, or a single set of criteria across all spheres, but according to different criteria within each of the distinctive spheres. Goods acquire their meaning from the spheres and ideologies of the spheres in which they operate, and the criteria, or principles of distribution according to which goods are distributed, are derived from this meaning of particular goods within respective spheres. For example, commodities in a marketplace are distributed according to preferences and ability to pay; and in the sphere of democratic politics, political office is (or should be) distributed on the basis of votes—not the ability to pay. Defined this way, justice allows for social goods to be distributed in unequal measure within particular spheres, as long as "no citizen's standing in one sphere or with regard to one social good can be undercut by his standing in some other sphere, with regard to some other good" (Walzer, 1984, p. 19). There are obvious parallels here with Nissenbaum's normative approach. Both Walzer and Nissenbaum contend that justice depends on context, and that contextual factors (Nissenbaum's contextual values or Walzer's principles of distribution of particular spheres) essentially determine what balance of benefits and harms, or advantages and disadvantages, is morally acceptable.

We now have two ways of weighing the importance of the potential benefits and harms of a technology, artifact or application in the balancing process—Barak's "societal importance" and Nissenbaum and Walzer's "contextual importance". I believe both are equally useful, but best suited for different kinds of analyses. Assigning weight to benefits and harms on the basis of their relative *social* importance is useful at the artifact and technology levels of Brey's (2012) anticipatory technology ethics approach since at these levels we are often considering ethical impacts at a society-wide scale. On the other hand, assigning weight to benefits and harms based on their effects on *contextual* goals and values is most useful at the application level since this is where the analysis focuses on specific social contexts. However, *to the extent that* a new application has ethical effects outside its context, on society at large, we may still want to allocate weight on the basis of social importance.

In my evaluations of the scenarios in this chapter, I make use of the above-mentioned balancing rules and recommendations by Barak and Nissenbaum. Since we are at the application level of ethical analysis, I mainly use Nissenbaum's method of weighing the importance of benefits and harms. However, I offer only a sparse account of the balancing process for the individual scenarios since the space I have here is limited.

To conclude this section, it should be noted that even if we adhere to all of the above rules and pointers, balancing—and, by extent, an entire ethical evaluation—remains a highly subjective endeavor. The interpretation of values, contexts, etc., is simply too dependent on one's personal system of values. Even though I strive to analyze the ethical issues and conduct the balancing in a conscientious way, others may hold different views and arrive at conclusions that are equally valid but different from mine.

6.2 Evaluating practices of application scenarios

It is now time for us to evaluate future drone applications. I present these future applications by means of *scenarios*. According to scenarios expert Peter Schwartz (1991), scenarios are "a tool for ordering one's perceptions about alternative future environments in which one's decisions might be played out […] Concretely, they resemble a set of stories" (p. 4). Scenarios, Swartz argues, "can help people make better decisions—usually difficult decisions—that they would otherwise miss or deny" (p. 4). For this study, a total of eleven future scenarios were created on the basis of the descriptions of future capabilities and applications of surveillance-capable drones in chapter 3. They are short narrative scenarios describing possible states-of-affairs in the year 2030, which reveal important ethical issues requiring careful ethical analysis. From this collection of eleven scenarios, four were selected for evaluation in this chapter; the remainder are presented in appendix C of this study. I have tried to select scenarios that are varied in terms of drone type, user type and application type, and pose a moral dilemma of sorts, so as to maximize the insights that can be drawn from the evaluations. The selected scenarios are: "Narcotics investigation" (subsection 6.2.1); "Terror at the Olympics" (6.2.2); "Google Maps in real-time" (6.2.3); and "Drone journalism" (6.2.4).

To make the evaluations, I use the augmented version of Nissenbaum's (2010) contextual integrity decision heuristic, which I described in chapter 4. This decision heuristic takes the form of guidelines that are articulated in a series of ten steps. The first six steps or components of the heuristic are descriptive; they help us to gain a clear understanding of the features in a new technology that may have implications for privacy. Here the main question is: *does the practice abide by privacy norms?* Steps seven through ten, on the contrary, are essentially normative in nature since they guide us in evaluating the features and practices associated with the new technology. Here the main question is: *is the practice ethically justifiable?* These last four steps are by far the most important in our case. The precise significance of each of the steps will become apparent as we apply the heuristic in the first scenario evaluation. Ample explanation is provided in this particular scenario evaluation. The three subsequent scenario evaluations, on the other hand, are much more concise in order to save space as the heuristic's steps will have become familiar.

As regards the identification of ethical issues concerning the practices described in the scenarios, I have used a list by Nissenbaum's (2004) of values that support or run counter to privacy, and a bottom-up approach that draws from the academic and non-academic literature on the societal impacts of civil drone applications as well as from generally accepted moral intuitions.

6.2.1 Scenario 1: Narcotics investigation

Let us start with the first drone application. This first scenario shows how a wide-area persistent surveillance (WAPS) drone might be used by the police to identify, track, and analyze the activities and network of, a suspected drug dealer. The scenario is based on an article by Gao, Ling, Blasch, et al. (2013) about the use of a WAPS drone with automated "context-aware" tracking and analysis software.

> *In 2030, the police have stumbled upon a location of interest: a suspected drug house, visited by some very shady characters. Since the police and the local prosecutor lack the evidence required to obtain a search warrant for the premises and to initiate a potentially high-profile case, they have to make do with temporary surveillance methods. They decide to use a wide-area persistent surveillance drone system to secretly monitor the house and track individuals who visit the house. Frequent visitors of the place are*

identified as persons of high interest, as they could be involved in drug dealing.[27] *The tracking data on suspect individuals is thoroughly analyzed, using context-aware clustering algorithms, to obtain data on their specific behaviors, or "pattern-of-life" data, which is later be used to set up a successful sting operation against them. In the process, however, data is also stored about many individuals who have at some point been in the vicinity of the supposed drug house and the suspects…*

Figure 14: Tracking a suspect in a criminal investigation.

Let us now apply Nissenbaum's decision heuristic to evaluate the practice described in this application scenario.

Step 1: Describe the new practice in terms of information flows

The first step of the decision heuristic is to describe the new practice in terms of information flows. The WAPS drone in the scenario captures top-down view motion imagery of large numbers of people for an extended period of time. It relays the imagery to detectives and other police personnel on the ground, who monitor and record the data. The police subsequently analyze the imagery using clustering algorithms in order to obtain information on the behaviors, or patterns-of-life, of specific persons whom they wish to focus their investigation on. The high-quality imagery makes many people, be they suspects or non-suspects, identifiable and has the potential to reveal sensitive information about them, such as familial, political, professional, religious and sexual details. For example, through the WAPS footage produced in this scenario one might be able to ascertain that an individual (who may be irrelevant to the investigation) is cheating on a romantic partner through regular visits to a brothel.

Step 2: Identify the prevailing context

The second step of the decision heuristic is to identify the prevailing social context. There are essentially three different social contexts in this scenario for two different groups: for the police investigators the context is *law enforcement*, or, more specifically, the *criminal investigation*; and for the people who are under observation the primary contexts are either *everyday life in outdoor public space* or *everyday life in outdoor private space* (since they are likely unaware of the criminal investigation).

[27] The police can infer that it is the same individual who is visiting the house multiple times over a couple of days on the basis of tracing data similarities and the visual appearance of an individual or a vehicle.

We can break down the contexts of everyday life in outdoor public and private space into further contexts. In outdoor public space, which includes streets, sidewalks, squares, parks, parking lots, etc., we find contexts such as transportation, public recreation, shopping, political activism, and informal exchange among strangers. In private outdoor space, which includes areas such as backyards, front yards, balconies, rooftops, etc., we find contexts such as private relaxation, private social gathering, gardening, and general housekeeping. For the sake of brevity, however, I only consider in this analysis the overarching contexts of everyday life in outdoor public space and outdoor private space, as well as the context of the criminal investigation.

Step 3: Identify information subjects, senders, and recipients

Let us now consider the actors in this scenario. The *information subjects* in this case are persons who are the target of the drug investigation, as well as many persons who are not of interest to the police. Both groups are not *senders of information* as they do not purposely engage in the sending of the information. The *recipients of information* are police personnel involved in the criminal investigation .

Step 4: Identify transmission principles

As a final step in laying the groundwork for an evaluation of the scenario, we need to identify the conditions, or "transmission principles", under which information is flowing. Using the WAPS drone and data analysis tools, the police covertly obtain motion imagery and pattern-of-life information of people across a wide area. There is little in the way of constraints on the flow of data from information subjects to police personnel. Importantly, there is no *reciprocity*, meaning that there is no flow of information going in the other direction, that is, from police personnel to information subjects. Moreover, there is no *consensuality* and *notice*, meaning that information subjects have neither consented to, nor know about, the transmission of their data.

Step 5: Locate applicable entrenched informational norms and identify significant points of departure

We may now try to answer the question of whether and how the practice of the scenario violates the entrenched informational norms of its contexts. These norms pertain to (1) the types of information that are flowing; (2) the types of actors involved (information subjects, senders, and recipients); and (3) the transmission principles governing the flow of information.

First, let us consider the entrenched surveillance practices that reflect the entrenched informational norms of the different contexts. Surveillance in the context of a criminal investigation is usually an affair with a clear focus and a limited scope. For example, police stakeouts focus on one or a few suspects at specific times and places. This limits the number of non-suspect persons caught up in the surveillance. Arguably, in the context of everyday life in outdoor public space, most of us seem to have accepted a moderate level of security surveillance (especially in crime-prone areas) through *conventional* (i.e., non-networked, non-"smart") CCTV cameras and patrolling police officers. This type of surveillance can involve large numbers of people not linked to any particular crime; crucially, however, this surveillance is not very *persistent*, meaning that it does not result in complete pictures of individuals' movements and behaviors. Moreover, people are usually aware of this kind of street surveillance, as security cameras, helicopters and patrolling officers are often easily spotted. Finally, in the context of everyday life in private outdoor space, it is accepted that there may be sporadic observation by helicopters and airplanes, which are sometimes used by police. Again, this kind of surveillance is arguably not very persistent and relatively easy to notice, as

conventional aircraft usually do not carry wide-area persistent surveillance equipment and often (especially in the case of helicopters) reveal their own presence through the noise they produce.

Comparing the practice described in the scenario with these entrenched practices, we may conclude that the new practice violates several *norms of appropriateness* (see chapter 4) in all three contexts. First, in the criminal investigation context, it does so by changing the set of actors "sending" information and the types of information that are transmitted; the new practice leads to an expansion in the number of non-suspect persons whose personal data are recorded by police investigators, and to an increase in the types and amounts of personal data and information collected of these persons—data that can make these non-suspect individuals identifiable and reveal all sorts of sensitive information about them, such as familial, political, professional, religious and sexual details. Second, in the context of everyday life in outdoor public space, the informational norms are violated through changes in the types of information transmitted, and changes in transmission principles; the practice again increases the types and amounts of personal data collected of people in public, and it also increases the covertness of observation, which constitutes a violation of the transmission principle of "notice". Finally, in the context of everyday life in outdoor private space, the violations are of the same kind as in public, but stronger—for private spaces are typically under less close and frequent observation than public spaces due to their often secluded nature.

Step 6: Prima facie assessment

It is now time to make a preliminary assessment. According to the contextual integrity framework, a breach of informational norms yields a *prima facie* judgment that contextual integrity has been violated because presumption favors the entrenched practice. I think the practice described in the scenario violates the informational norms to such an extent that we may indeed speak of a violation of contextual integrity. To be sure, this is not yet a normative assessment; further steps are necessary in order to arrive at a final verdict on the ethical admissibility of the practice.

Step 7: Evaluation I

The framework of contextual integrity is intended as a descriptive tool, systematically accounting for people's reactions to the myriad of technical systems that are radically affecting the flows of personal information (Nissenbaum, 2010). This is how we have used it up to this point. However, it is also intended as a framework for evaluating these systems from a moral and political point of view (Nissenbaum, 2010). The first of the additional steps to take for an ethical evaluation of the practice described in the scenario is to consider how the practice affects important moral and political factors. Thus, Nissenbaum has us asking: "What might be the harms, the threats to autonomy and freedom? What might be the effects on power structures, implications for justice, fairness, equality, social hierarchy, democracy, and so on?" In answering these questions, positive as well as negative impacts need to be considered, and the practice needs to be compared with alternative (entrenched) surveillance practices in a criminal investigation context.

Let us begin with the potential positive impacts of the practice. A common justification of novel technology-based monitoring and tracking systems is that they make surveillance more cost-efficient, as well as more efficacious in terms of promoting justice and security (Nissenbaum, 2010). In the case of WAPS drones, I believe this is a plausible argument. Monitoring and following potential suspects by regular means, such as stakeouts, CCTV cameras, undercover agents, etc., would likely require human, material, and financial resources that are greater than those needed when a future WAPS drone is used.

Greater efficacy in the solving and prosecuting of (drug) crimes can also be expected, provided the available wide-area aerial imagery is sufficiently useful, and effectively mined for evidence. As previously explained, such aerial imagery may contain a wealth of information on people's behaviors and movements, as well as on possible connections between individuals.

Now let us move to the new practice's potential negative aspects. To begin, the practice described in the scenario poses a threat to data subjects' freedom and autonomy due to a "chilling effect" (see chapter 5), where people adjust their behavior to the ever-present possibility that they are being watched. Typically associated with liberal political vision, autonomy is the mark of thoughtful citizens whose lives and choices are guided by principles they have adopted as a result of critical reflection (Dworkin, 1988). One needs freedom from scrutiny, as well as zones of relative solitude, in order to formulate goals, values, conceptions of self and principles of action, since freedom and solitude enable one to experiment, act, and decide without giving account to others or being fearful of retribution (Nissenbaum, 2004). Due to the great persistence and dragnet quality of WAPS drone surveillance, the potential harm to subjects' freedom and autonomy is much greater than is it with alternative surveillance methods.

The "chilling effect" may also have a detrimental effect on important human relationships and democracy. When outdoors, individuals may to some extent close themselves off socially in anticipation of the police surveillance, rather than fully engage in social interaction and risk a compromising disclosure to police personnel. According to Charles Fried (1968), controlling who has access to personal information about ourselves is a necessary condition for friendship, intimacy, and trust. In addition, the vitality of democracy may be reduced by the practice since a healthy democracy depends on an autonomous and thoughtful citizenry, and on protection against public scrutiny of certain spheres of decision-making—of which some are located in drone-observable places.

Finally, the practice has a significant potential for information-based harms as a result of the abuse, error and accountability issues inherent in drone technology. Since the police are dealing with a lot of personal data, this data is more likely to fall into the wrong hands. Furthermore, police drone operators can be tempted to engage in acts of voyeurism and stalking due to an increased "moral distance" (see section 5.2). Finally, there is a risk of institutional abuse, where the police at some time in the future use the drone's imagery for purposes other than the drug investigation, which may be more harmful. These issues are more pronounced than they are with existing surveillance practices.

Step 8: Evaluate whether the goals, values and ends of the context, as well as the balance between them, are fair, and amend them if they are not

In Nissenbaum's *original* decision heuristic, the next step would be to consider how the practice directly impinges on the goals, values and ends of the contexts, and to consider the meaning or significance of the previously described moral and political factors in light of these contextual goals, values and ends. In the revised version of the heuristic that I use here, this step remains, but we need to do something else first: we need to evaluate whether the goals, values and ends of the contexts in question, as well as the balance between them, are fair; and we need to amend them if they are not. This is a step that I have introduced into the original decision heuristic in chapter 4 to be able to deal with a potential situation where a context's underlying goals, values and ends can be considered unfair as a result of a social power imbalance in the context.

In a criminal investigation, the essential contextual goals are to identify, locate, and prove the guilt of, a criminal. More generally, in law enforcement the goals are to discover, deter, rehabilitate, or punish people who violate the rules and norms governing society. Jointly, these goals serve the values of justice and security in equal measure. I consider these to be fair goals and values for the context at hand.

Whereas the goals of a criminal investigation are pretty straightforward, the goals of everyday life in outdoor public space and outdoor private space require a little more elaboration. Let us first consider outdoor public space. This context provides a basis for informal social, civic, and public lives (Patton, 2000). It includes places such as streets, sidewalks, parks, and squares, which form a material basis for a wide range of activities or contexts, such as transportation, recreation, performance, shopping, political activism, opportunities for informal exchange, and chance meetings. These places are often collectively owned and, in principle, accessible to all members of the public.

The purposes of outdoor public space are varied and linked to the individual contexts that this overarching context is composed of. It can be argued that, in general, values such as autonomy, freedom, security, efficiency (of movement), equality, sociality and democracy are considered important in public space (at least in Western democratic societies). Now, if there is a kind of broadly accepted general *purpose* of outdoor public space, it could well be the *promotion of physical mobility*. Information and media studies scholar Michael Zimmer has proposed the concept of "spheres of mobility" (2007). Navigating public roadways for automobile drivers is one such sphere according to Zimmer. In spheres of mobility, individual autonomy and freedom are dominant; individuals in these spheres are generally permitted to act at their own discretion, to be answerable and accountable to no one. Without providing further argumentation, I contend that most outdoor public places can, at least in part, be considered "spheres of mobility" and that the values associated with such spheres (i.e., freedom and autonomy) are fair.

The promotion of physical mobility might not be the only purpose of outdoor public space. A second, perhaps equally important, general purpose may be the encouragement of informal everyday social life and community cohesiveness. It is worth emphasizing the social functions outdoor public places have besides their more basic material functions such as offering a means for transportation. By providing a place for diverse groups of people to mix, public places afford people with spontaneous face-to-face interaction and opportunities to participate in informal community life (Patton, 2000). They are sites for unplanned but common encounters with those who are not known. Through the day-to-day activities they allow people to engage in, public places help to affirm the social contract and the identities of communities (Patton, 2000). In my view, there is little arguing against the fairness of these social functions and values of outdoor public space.

Finally, let us turn to outdoor *private* space, which includes areas such as backyards, front yards, balconies, and rooftops. The first three of these can be considered an extension of the home. Here we find contexts such as private relaxation, private social gathering, gardening, and general housekeeping. There is no overarching purpose to these contexts, but inarguably all of them prominently involve the values of freedom and autonomy, which again seem like fair contextual values.

Step 9: Evaluation II

The next step is now to consider how the practice directly impinges on these justified contextual goals, values and ends, and to consider the meaning or significance of the previously described moral and political factors in light of these contextual goals, values and ends. This is where we assign weight to the

impacts on the basis of contextual importance, as prescribed in the previous section on balancing (section 6.1).

Compared to existing surveillance practices, which include stakeouts, CCTV cameras, and undercover police officers, the practice of using a WAPS drone may better fulfill the purposes of a criminal investigation context, which are to identify, locate and prove the guilt of a criminal. The practice may thus better serve the values of justice and security that are associated with the context.[28]

The practice of using a WAPS drone may perform far worse than existing practices in terms of fulfilling the general functions of outdoor public space, which are the promotion of physical mobility, and the encouragement of informal social life and community cohesiveness. The realization of values most prominently supported by these functions, which include autonomy, freedom, and sociality, is more negatively affected by drone use than by other surveillance practices. Finally, the underlying values of outdoor private space also prominently include autonomy and freedom, and their realization, too, is more negatively affected by drone use.

Step 10: Final verdict

A trade-off needs to be made between the *marginal* potential positive effects and the *marginal* potential negative effects of WAPS drone use with respect to existing surveillance practices. Such balancing is made difficult by the fact that there are different contexts in this case, which favor different outcomes. In the criminal investigation context, the use of a WAPS drone seems justified given the likelihood that the particular goals and values of the context (i.e., justice and security, in society at large) will be promoted. I believe that the extent of their promotion is only modest in this scenario, but can be much greater if other, more serious crimes are considered. In contrast, the use of the drone does not at all seem justified in the broad contexts of outdoor public space and outdoor private space. Although security is an important value in these contexts, many of the contexts' other values, such as freedom, autonomy, sociality, and democracy, are severely curtailed. Given the undisputable societal significance of the latter two contexts and their values, and the extent of the potential harms, I must assign more weight to the incremental harm that may be done to the fulfillment of the goals and values of these contexts than to the incremental benefit to (the efficacy and cost-efficiency of) justice and security in society at large. This leads me to decide that the practice of using the WAPS drone as described in this scenario cannot be ethically justified.

6.2.2 Scenario 2: Terror at the Olympics

The second scenario shows how a wide-area persistent surveillance (WAPS) drone might be used by law enforcement agencies to identify, track, and apprehend individuals suspected of committing an act of terror at the Olympic Games.

> *In 2030, law enforcement agencies use a large wide-area persistent surveillance drone to provide security against the threat of terrorism at the Olympic Games. It covertly flies over the Olympic village and sports venues, continuously recording detailed wide-area footage of these and surrounding areas and automatically tracking and analyzing the movement of the people within them. Inhabitants and visitors of the host city are informed that drones are being used for security purposes. At day 12 of the Olympics, a large bomb explodes just outside the Olympic Stadium, killing 15 people and wounding many more. Law*

[28] However, one could also argue that the practice does not do justice to the persons who are not suspects in the investigation but whose personal data is nonetheless recorded and analyzed through drone use.

enforcement agents use the drone footage to identify and locate the terrorists. Two suspects are seen placing the bomb and thanks to automated movement tracking they are apprehended within hours. The automated tracking software had tracked them to a house two kilometers from the Olympic Stadium. It later emerged the suspects had planned another attack for the very next day…

Figure 15: Providing security for an important public event.

Let us now apply Nissenbaum's decision heuristic to evaluate the practice described in this application scenario.

Steps 1–6: Prima facie evaluation of contextual integrity

This scenario has important similarities to the previous scenario. A WAPS drone is used in public airspace and captures top-down motion imagery of large numbers of people for an extended period of time. It relays the imagery to law enforcement personnel on the ground, who monitor and record the data, and analyze it using tracking algorithms. The imagery and tracking data make many people identifiable, regardless of whether they are potential suspects, and have the potential to reveal all sorts of sensitive information about them. There are essentially three different social contexts in this scenario: a *large-scale public event* context, which can further be specified as the *Olympic Games* context, and the by now familiar contexts of *everyday life in outdoor public space* and *everyday life in outdoor private space*. The transmission principles now include "notice" since the public is informed about the drone's presence.

The new practice is to be compared with the standard use of CCTV cameras and (undercover) patrolling law enforcement agents in large-scale public events. Comparing the practice with these entrenched practices, we can conclude that the new practice violates informational norms in all three contexts. In the context of the Olympic Games, and more so in the context of outdoor public space, the informational norms are violated through changes in the types of information transmitted, and changes in the transmission principles: the practice increases the amount of personal data collected of people in public, and it increases the covertness of observation—even if people are informed of the drone's presence. Finally, in the context of outdoor private space, the same violations are occurring at an even stronger level. All of this leads to a *prima facie* judgment that contextual integrity has been violated.

Steps 7–10: Final normative assessment

Let us now assess the ethical admissibility of the new practice. To begin, the potential positive and negative impacts on ethical values are similar to those listed in the previous scenario evaluation. Compared with surveillance using only CCTV cameras and patrolling police officers, surveillance that includes WAPS drones with automated tracking software is likely to be more cost-efficient, and more efficacious in terms of promoting security, public order and justice. As previously explained, the almost endless amounts of data the WAPS drone produces contain a wealth of information on people's behaviors, movements, and connections. When this data is effectively and efficiently analyzed it may prove quite helpful in reducing (but not eliminating) the probability and impact of terror attacks, including the time and effort needed to apprehend suspects. In terms of potential negative impacts, the new practice has a diminishing effect on data subjects' freedom, autonomy and social relationships, and on democracy, mainly due to the "chilling effect" it induces; and the practice enhances the risks of information-based harms, such as identity mistakes, voyeurism and stalking. These negative impacts are mitigated, however, by the fact that people are informed of the drone surveillance, and by the fact that this surveillance only lasts for the duration of the event.

Let us now consider the goals, values and ends of the contexts in question and evaluate whether these are fair. The essential purpose of the Olympic Games is to make the world come together in celebration of excellence in sport. In addition, the Olympics allow a host city (and host country) to showcase itself to the world, which may be the host city's prime motive for hosting the event. Given the high-profile nature of the event and a recent history of terror attacks (in Munich, 1972; and in Atlanta, 1996), public security and public order are considered to be of the utmost importance. The goals and values of everyday life in outdoor public space and outdoor private space have been described in the previous scenario; important in these two contexts, respectively, are the values of freedom, autonomy, security, efficiency, equality, sociality, and democracy, and the values of freedom and autonomy. In my view, the goals and values of all of these contexts are fair.

We may now consider the meaning or significance of the impacts in light of the contextual goals and values, and balance them so as to arrive at a verdict on the ethical admissibility of the practice. On the whole, I believe the goals and values of the Olympic Games context are better served by the new practice than the existing practices because of the new practice's strengthening effect on security and the relative lack of harm to this context's other goals and values. However, the new practice fares worse than the existing practices in terms of realizing the goals and values of everyday life in outdoor public space and outdoor private space. Again, balancing the impacts is complicated by the fact that there are different contexts that favor different outcomes. The context of the Olympic Games competes with the contexts of everyday life in outdoor public space and outdoor private space. In my view, the context of the Olympic Games is dominant while the event is taking place, and the incremental benefit to security and justice resulting from the new practice, in terms of the probability and impact of terror attacks, outweighs any temporary incremental harm to values such as autonomy, freedom, sociality, and democracy. This leads me to conclude that the practice of using a WAPS drone as described in this scenario is ethically justified.

6.2.3 Scenario 3: Google Maps in real-time

The third scenario shows how a wide-area persistent surveillance (WAPS) drone might be used by a commercial organization to provide the public with detailed *real-time* maps of whole urban areas. The

practice described in this scenario is not entirely about drone use; however, the use of drones is instrumental in the practice.

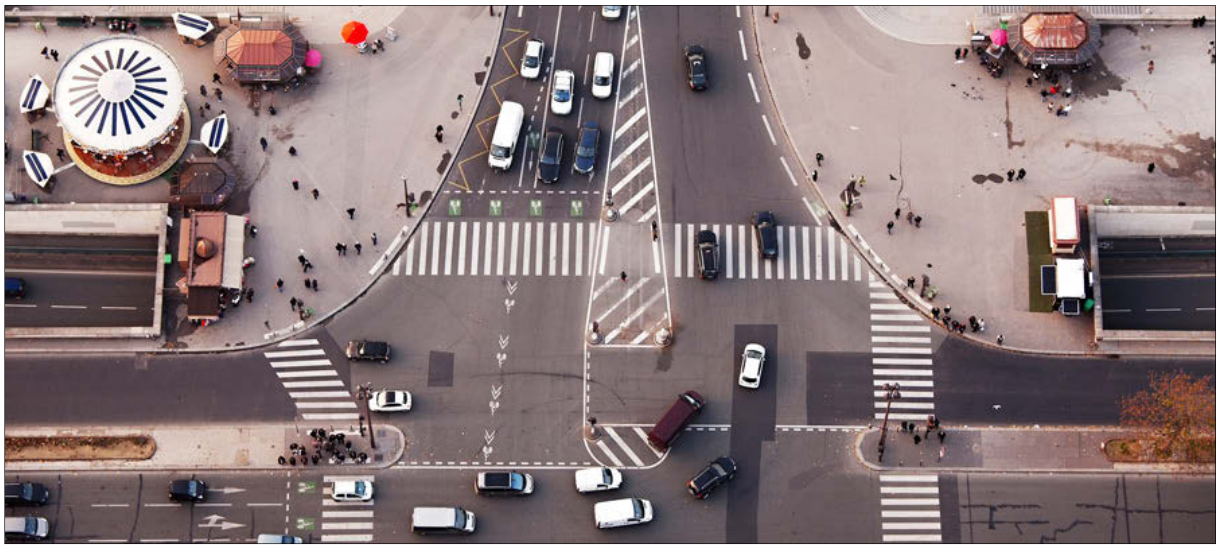

Figure 16: Providing a real-time bird's eye view of places.

> *In 2030, Google Inc. has launched a version of its popular web application Google Maps that provides top-down and angled aerial imagery of entire urban areas in near real-time, rather than dated still footage. The application is appropriately called Google Live Maps and everyone can use it for free. Google uses large WAPS drones circling above cities to capture and relay high-resolution (0,1 meter per pixel) images at a rate of one per second. The imagery is used by Google and the public for a multitude of purposes. Google uses it, for example, to analyze traffic movements, so that it can commercially offer up-to-date traffic information. The company is careful to point out that they do not analyze imagery data of private property and individual persons. However, they do provide these raw imagery data to the public at large. The public uses Google Live Maps for all kinds of mundane purposes such as checking live traffic conditions, looking for free spots in a parking lot, evading crowded areas at the beach, and checking up on one's home while on holiday. Only benefits one would think…*

Let us now apply Nissenbaum's decision heuristic to evaluate the practice described in this application scenario.

Steps 1–6: Prima facie evaluation of contextual integrity

Let us first analyze the new practice in terms of information flows, contexts, actors, and transmission principles. WAPS drones are used in public airspace and continuously capture top-down and angled aerial motion imagery of entire urban areas for an indefinite period of time. The drones relay the imagery to Google Inc., which uses a portion of the data to commercially provide real-time traffic information. The entire data stream is then made available to the public via the Google Live Maps application. Essentially, there are two different social contexts in this scenario, which again are the contexts of *everyday life in outdoor public space* or *everyday life in outdoor private space*. There are no noteworthy constraints on the flows of information in this scenario; *reciprocity*, *consensuality*, *notice*, *confidentiality*, etc., are all absent.

Comparing the new practice with the dated aerial stills of the old Google Maps,[29] we may conclude that the new practice violates norms of appropriateness and norms of distribution in both contexts. The violations are only in terms of the types of the information that is being recorded by Google and then made available to the public at large: through persistent drone observation, the new practice increases the types and amounts of personal data collected of people in public and distributed to the public. Previously, one was hard-pressed to identify someone from a single image in Google Maps. Even if users of the new application are still not able to do this (given the viewing angles and the image resolution of 0,1 meter per pixel), the persistence of the observation does allow users to track and analyze the movements of specific individuals and thus make inferences about their identities, behaviors, and connections, which can obviously constitute very sensitive personal information. Arguably, the violation is stronger in private space than it is in public space since people are a more used to surveillance in public space. All of this leads to a *prima facie* judgment that contextual integrity has been violated.

Steps 7–10: Final normative assessment

Let us now assess the ethical admissibility of the new practice. Starting with an assessment of the potential positive impacts, the new practice is likely to increase productivity and efficiency in various ways, for all kinds of users. For citizens the application may lead to greater convenience in such activities as checking traffic conditions, looking for free spots in a parking lot, evading crowded areas in outdoor recreational spaces, and checking up on one's home while on holiday. Google and other companies may benefit financially through a more productive and efficient use public and private infrastructure. Conceivably, one might even be able to use the drone data to estimate changes in a region's GDP on a daily basis (Oremus, 2014). Like the previous two scenarios, the new practice has an important negative effect on data subjects' freedom, autonomy, and social relationships, and on democracy due to the "chilling effect" it induces (as a result of violations of all the privacy types that were described in chapter 5). Furthermore, the practice enhances the risks of information-based harms such as voyeurism and stalking, even at the image resolution of 0,1 meter per pixel. Due to the distanced nature of such abuses, there is little chance of abusers being held accountable for their actions. Finally, public safety may be an issue if drones are used in many urban areas (due to hacking, improper maintenance, etc.).

Since the goals and values of everyday life in outdoor public space and outdoor private space have been adequately described and evaluated in the first scenario evaluation (section 6.2.1), we can now move directly to the balancing stage. The new practice performs worse than the existing practice in terms of realizing the goals and values of outdoor public space and outdoor private space. Even if we consider efficiency of movement an important factor in the context of outdoor public space (especially since it can be seen as having a positive impact on freedom and autonomy), there are pronounced incremental negative effects on other values in this context, which include autonomy, freedom, sociality, and democracy. Significantly, in the context of outdoor private space, there are no incremental positive effects at all in terms of the realization of contextual goals and values. Apart from the effects within the contexts,

[29] The difficulty with this scenario is comparing the new practice with the entrenched practice, which is actually not entirely entrenched. Google Maps is a relatively new application and there has been some controversy surrounding some of its functionality, especially its *Street View* function, which provides panoramic views from positions along many streets in the world. Its top-down ("satellite") view function, however, has generally had a much better reception and has started to become an indispensable aid to many. Since the new application is actually an extension of this particular function, this function's "practice" may serve, for our purposes, as the entrenched practice.

we also need to take into account the positive and negative effects *in general* (i.e., in society at large) and balance them in terms of their societal importance. This means including the expected incremental positive effects on the pursuit of wealth for companies and citizens, as well as the incremental negative effects in terms of information-based harms to citizens and accountability. Again, in my view, the balance tips comfortably in favor of rejecting the new practice. All of this leads me to decide that the practice of using a WAPS drone as described in this scenario is not ethically justified.

6.2.4 Scenario 4: Drone journalism

The fourth scenario illustrates how small general-purpose drones may be used by news organizations to improve news coverage of events that are socially significant.

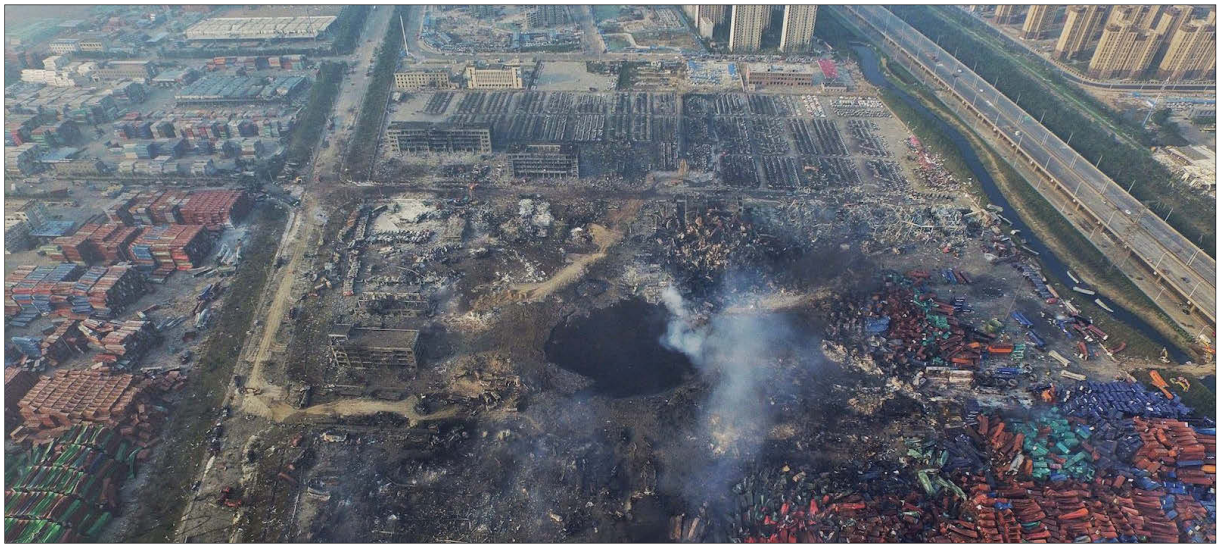

Figure 17: Observing the site of a disaster.

> *In 2030, a news organization has a fleet of small, but very capable, camera-equipped "general-purpose" drones. While it considers such drones to be great storytelling tools, the organization is well aware that use of the machines carries certain risks. For this reason, it has rules in place that only allow the drones to be used in cases where journalistic coverage is likely to be of high social importance and where such coverage is enhanced by the use of drones. When a potentially important story breaks, one of the drones is quickly sent out from the organization's headquarters and flown over the news scene where it shoots video so that workers in the news room can evaluate what to do next. Cases where the news organization uses the drones for extended observation are, in general, limited to coverage of public protests, coverage of high-magnitude accidents and natural disasters, and (covert) investigation of political corruption and corporate wrongdoing.*

Let us now apply Nissenbaum's decision heuristic to evaluate the practice described in this application scenario.

Steps 1–6: Prima facie evaluation of contextual integrity

Let us first analyze the new practice in terms of information flows, contexts, actors, and transmission principles. The drones are used in public airspace and capture aerial motion imagery and sound at specific locations of newsworthy events. The drones relay these data to the news organization, which uses it in their publicly broadcasted news bulletins. There are a lot of contexts in this case, which means that we are

approaching the limits of what can be effectively analyzed using the contextual integrity framework. Important contexts include *public protests*, *disasters*, and *high-profile crime cases*. The contexts of *everyday life in outdoor public* and *everyday life in outdoor private space* are present at the fringes of these contexts. Again, there are no noteworthy constraints on the flows of information in this scenario; *reciprocity*, *consensuality*, *notice*, *confidentiality*, etc., are all absent .

Comparing the new practice to the entrenched practices of video journalism, from land and, occasionally, manned aircraft, we may conclude that the new practice violates norms of appropriateness and norms of distribution in all contexts to varying degrees. The violations occur, firstly, due to changes in transmission principles. People in the areas that are observed will often not notice the news organization's drone, whereas normally they would notice camera crews and helicopters. In addition, (distanced) drone observation makes it harder to obtain consent for broadcasting up-close footage of individuals, which is often sought by journalists. Secondly, there are violations in terms of types of information. The drones increase the amount of personal information that is collected and distributed by allowing the news organization to shoot and broadcast more aerial footage. People at the scene of a newsworthy event have a higher chance to have their image captured and broadcast, and inaccessible private areas are now easily observed. All of this leads to a *prima facie* judgment that contextual integrity has been violated.

Steps 7–10: Final normative assessment

Let us now assess the ethical admissibility of the new practice, starting with the practice's potential positive and negative impacts. As regards the positive effects, the quality of the news reporting of important events is likely to go up: the use of the news organization's drones contributes to more accurate information and speedier coverage of events. For example, the drones can be used by investigative journalists as secret observation tools to uncover corruption scandals (by tracking individuals, peeking through high-level windows, etc.); they can be used to provide early estimations of the loss of life and property resulting from earthquakes; and they can be used to accurately gauge the size of public demonstrations. As for the negative effects, these very much depend on the context at hand. In the context of a disaster, the use of the drones can compromise the dignity of victims through indiscriminate observation. Furthermore, in the context of a public demonstration or public festivities, where there are large concentrated masses of people, safety is likely to be more of an issue. Also, there may be small incremental harms in terms of temporary loss of freedom and autonomy (due to the "chilling effect") for all people at and near the scenes where drone observation takes place. Finally, there are small increases in the risks of abuses such as stalking and voyeurism.

Let us now consider the goals, values and ends of the contexts in question and evaluate whether these are fair. Important contexts are *public protests*, *disasters*, and *high-profile crime cases*. What these contexts have in common is that they are newsworthy events where journalistic coverage is expected and socially desired. The goal of public protests is force action (through publicity) for a certain cause; the goal of disasters is to provide safety and security to those affected; the goal of high-profile crime cases is to have justice and truth. I see no issue with asserting that these goals are fair. The goals and values of everyday life in outdoor public space and outdoor private space have been adequately described and evaluated in the first scenario evaluation.

We may now consider the meaning or significance of the impacts in light of the contextual goals and values, and balance them so as to reach a verdict on the ethical admissibility of the practice. I believe the

goals and values of the contexts of *public protests*, *disasters*, and *high-profile crime cases* are better served by the new practice than the existing practices due to the new practice's strengthening effect on journalistic coverage and the relative lack of harm to the contexts' other goals and values. On the other hand, the new practice fares worse in terms of realizing the goals and values of outdoor public space and the values of outdoor private space. In my view, however, the incremental net benefit in the former three contexts outweighs the incremental net harm in the latter two contexts. Moreover, if I place the incremental positive effects of the new practice (i.e., better quality news reporting with resultant societal benefits) and the negative effects (i.e., a potential harm to the dignity of victims in some cases, a small harm to public safety, and temporary harms to freedom and autonomy) in the wider context of *society at large* and balance them in terms of their societal importance, I also find the balance tilting in favor of the new practice. This leads me to conclude that the practice of using general-purpose drones as described in this scenario is ethically justified.

To be sure, this scenario may warrant more detailed contextual evaluations that are focused on the individual sub-applications of drone journalism; however, the conclusion reached here would most likely stand.

6.3 Conclusion

In this chapter, I used the augmented version of Nissenbaum's (2010) contextual integrity decision heuristic to ethically evaluate future applications of surveillance-capable civil drones described by a select number of application scenarios created for this study. I showed that the heuristic can be used to make comprehensive ethical evaluations. The decision heuristic consists of guidelines that are articulated in a series of ten steps, of which the precise significance became clear as we evaluated the first application scenario. The first six steps in each scenario evaluation were descriptive and helped us to gain a clear understanding of the features of particular drone applications that may have implications for privacy. Here the main question was: *does the new practice abide by privacy norms?* Steps seven through ten, on the contrary, were normative and guided us in making general ethical evaluations of drone applications. Here the main question was: *is the new practice ethically justifiable?* A very importantly step in this normative part was making an assessment of a new practice's impacts as a function of their meaning or significance in relation to the aims, purposes, and values of the context at hand.

Before applying the Nissenbaum's (2010) decision heuristic, I discussed the topic of balancing competing ethical values in ethical evaluations, which required a little more discussion than Nissenbaum was able to offer. I presented important balancing rules and recommendations—some of which supplementing Nissenbaum's approach—and employed these in the ethical evaluations in this chapter. I argued that in the balancing process we need to consider such factors as: the *urgency*, *probability* and *marginal change* of the new practice's harms and benefits; the ethical performance of any *alternative practices*; the question of whether impacts affect *interests* or *values*; and the question of whether impacts are to be weighed in terms of *contextual importance* or *societal importance*. With regard this last issue, I argued that assigning weight to benefits and harms on the basis of their relative societal importance is most useful at the artifact and technology levels of Brey's (2012) anticipatory technology ethics approach since at these levels we are often considering ethical impacts at a society-wide scale; and I argued that assigning weight to benefits and harms based on their effects on contextual goals and values is most useful at the application level since this is where the analysis often focuses on specific social contexts.

We ethically evaluated the practices of four scenarios—"Narcotics investigation", "Terror at the Olympics", "Google Maps in real-time", and "Drone journalism"—and came to the following final conclusions. First, the practice of using a WAPS drone during a drugs investigation, as described in the first scenario, was found *not ethically justified*, since the practice's potential marginal harms to freedom, autonomy, sociality and democracy outweigh the potential marginal benefits to justice and security, considering the contextual values and comparative societal importance of a drugs investigation and everyday life in outdoor public space and outdoor private space. Secondly, the practice of using WAPS drones to prevent terrorism during the Olympic Games was found *ethically justified* since here the potential marginal benefits to justice and security outweigh the potential *temporary* marginal harms to freedom, autonomy, sociality and democracy, given the preeminence of the context of the Olympic Games. Thirdly, the practice of using WAPS drones to provide a real-time public mapping service was considered *not ethically justified*, since the potential marginal harms to freedom, autonomy, sociality, democracy, accountability, and safety from informational harms outweigh the potential marginal benefits to efficiency of movement, convenience and the pursuit of wealth, given the contexts of everyday life outdoor public space and outdoor private space. Finally, the practice of using drones to report on news of socially important events was deemed *ethically justified* since the potential marginal benefits to the quality of news reporting and associated societal effects outweigh the potential marginal harms to human dignity, safety, freedom and autonomy, in light of important news reporting contexts.

It is important to note that in all four scenario evaluations I did not list all of the issues that are inherent in drone technology and the respective types of drone (all of these issues were described in the chapter 5). Even though almost all of the inherent issues, by necessity, did have an impact (as they are *inherent* issues), many of them were of decidedly minor import in the evaluations here. Thus, for the sake of brevity and clarity, I decided not to mention some of these issues.

Needless to say, these scenario evaluations are only the beginning of a comprehensive evaluative analysis of surveillance-capable civil drone applications in public space; many more evaluations are necessary to obtain a comprehensive and fine-grained picture of the ethical admissibility of drone applications. This holds true especially if we consider that ethical justifiability is highly dependent on the specific parameters of the application scenarios. Nevertheless, by using the decision heuristic to conduct detailed evaluations of a limited number of drone applications, I have made it easier to make more of such evaluations. What is more, the evaluations made thus far already allow us to draw a few general insights. Firstly, we may conclude that even if there are great concerns about civil drone use, as we have seen in the previous chapter, by far not all drone applications are morally unacceptable; given the right circumstances and parameters, even persistent surveillance applications for law enforcement purposes can be ethically justified. Secondly, we may conclude that the justifiability of drone applications is in general highly dependent on whether the goals and values of the general contexts of everyday life in outdoor public space and outdoor private space are served, as these contexts have an overwhelming presence in drone applications. Thus, any impacts of drone use on outdoor physical mobility, informal social life and community cohesiveness, and the associated values of freedom, autonomy and sociality, can be expected to be of high ethical importance.

Finally, at a methodological level, we have observed that we are often dealing with multiple social contexts at once when evaluating drone applications. This is mainly because outdoor public space is host to a great number of social contexts, some of which can occur simultaneously, at the same place and the same time,

for different individuals. In balancing the impacts of drone applications in cases where different contexts favor different outcomes, I have found it apt to determine the relative societal importance of these contexts themselves and include this as a factor in the balancing process. Naturally, identifying and determining the relative importance of contexts is somewhat of a subjective process.

7 Final evaluations

In chapter 6, we used Nissenbaum's (2010) contextual integrity approach to make comprehensive ethical evaluations at the application level of ethical analysis. At the technology and artifact levels, however, we have thus far only *identified* ethical issues. It is now time to make ethical evaluations at these levels, too. In this chapter, we will therefore carry out the *evaluation stage* of ethical analysis of the Brey's (2012) anticipatory technology ethics (ATE) approach. At this evaluation stage, according to Brey, "the potential importance of ethical issues is assessed, the likelihood that they will become a significant issue in society, as well as their relation to each other, including potential value conflicts" (p. 12). In this chapter, we will use this stage to provide the remaining answers to the two main research questions of this thesis, which hold: *To what extent is the civil use of unmanned aerial systems (UASs) that are capable of public surveillance ethically justified in light of its potential effects on privacy and other ethical values?* And: *What ethical issues need to be considered in efforts to improve the ethical justifiability of the civil use of unmanned aerial systems (UASs) that are capable of public surveillance?* Of course, with regard to the application level of analysis, we already dealt with these questions in the previous chapter.

In order to be able to answer these questions with respect to drone technology and drone artifacts, I will use the first two sections of this chapter to present methods to, respectively, (1) evaluate the importance of ethical issues at the technology and artifact levels of the ATE approach, and (2) evaluate the ethical admissibility of a particular technology or artifact. The first section adds some detail to my account of Barak's (2010) concept of *societal importance* (which I only briefly touched upon in the previous chapter), which I will use to establish what ethical values are to be considered important in our evaluations. The second section explains the general conditions that, in my view, need to be satisfied if a technology or artifact is to be prohibited on ethical grounds.

I will use the third and fourth sections to conduct the actual ethical evaluations for drone technology and drone artifacts, and to provide the outstanding answers to the two main research questions of this thesis. The third section evaluates, respectively, the importance of the ethical issues concerning surveillance-capable drone technology at large and the technology's ethical admissibility in civil contexts. The fourth section does the same, but for the three main types of drone artifact we distinguished in chapter 3. This chapter ends with a short concluding section that summarizes the conclusions of the ethical evaluations and other findings of this chapter.

7.1 Determining the relative importance of ethical values

To determine the importance of the ethical impacts that are evaluated in this chapter, I will use Barak's (2010) proportional balancing approach, which I outlined in the previous chapter. In this section, I would like to add a little more detail to my account of this approach, and I would like to use the approach to establish what ethical values are to be considered important in our evaluations.

As we have seen in the previous chapter, a central feature of Barak's balancing approach is to determine the importance of benefits and harms on the basis of their relative *societal importance*. I have argued that this method of weighing benefits and harms is useful at the artifact and technology levels of ethical analysis

since at these levels we are generally considering ethical impacts on a society-wide scale. The societal importance of benefits and harms is of course partly[30] derived from the societal importance the basic values that are affected, not all of which are of equal societal importance. The question now arises: how do we know the relative importance of these values?

What are the primary values, according to Barak (2010), depends on a society's own circumstances, reflecting its unique challenges, history, and self-perception. Often, these are enshrined in a country's constitution. For example, South Africa's new constitution, influenced as it was by the country's recent history of apartheid, specifically and explicitly considers the rights to dignity, equality, and freedom, and the derivative rights of these three, to be of central importance to South African society. Furthermore, according to Barak, a value of which the realization constitutes a condition for the realization of another value should be regarded as being the more important of the two. From this we can infer the relative importance of privacy, as it is often seen as a condition for the realization of many other values. Finally, Barak argues, the distinction with respect to the importance of a value is not limited to the context of comparison between different values and is likewise applicable *within the context of* any given value. Accordingly, within the scope of the right of freedom of expression, we can distinguish between freedom of political expression and freedom of commercial expression, with greater importance assigned to the former type.

Let us now try to establish what ethical values are to be considered as socially most important for our analysis. To keep things relatively simple, I take "socially important" to mean "important in a liberal democratic (Western) society", and I take what is socially important in the European Union (EU) to be a reasonably good proxy for what is socially important in liberal democratic societies at large. Thus, we are to determine the values that are of high social importance in the EU. According to the *Treaty on European Union* (as amended by the Treaty of Lisbon), "[t]he European Union is founded on the values of respect for *human dignity*, *liberty*, *democracy*, *equality*, *the rule of law* and respect for *human rights*, including the rights of persons belonging to minorities," and these values are common to the EU member states whose societies are characterized by "pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men." These values are echoed by the *Charter of Fundamental Rights of the European Union*, which describes the substantive rights of each EU citizen under the headings of dignity, freedoms, equality, solidarity, citizens' rights and justice. (Much of this charter is based on the Council of Europe's *European Social Charter* and *European Convention on Human Rights*.) We will later use these values to gauge the importance of the ethical issues that are evaluated in this chapter.

Instrumental in realizing some of the above-mentioned values is of course *privacy*, which makes this a value that is of high social importance as well—and perhaps, if we follow Barak (2010), it is of *higher* importance than many of the values it supports. The importance of privacy in terms of its support of other values is, however, somewhat dependent on which of its varied aspects, or types, we are considering. This is why I will offer an expanded discussion of the importance of privacy in relation to drone technology and drone artifacts in sections 7.3 and 7.4.

[30] Other factors include of course the extent of the harm and benefit to the values, and the probabilities that they will materialize.

7.2 Determining the ethical admissibility of technologies and artifacts

There is one more topic that needs to be discussed before we can begin our evaluations of drone technology and artifacts. In order to determine the *ethical permissibility* of drone technology and artifacts, we must first know what general conditions need to be satisfied for a technology or artifact to be banned. As regards the *technology level*, I contend that, from an ethical standpoint, a technology should be prohibited outright only if

1) all imaginable uses of the technology can, with a reasonable amount of certainty, be considered ethically unjustified,

or, in case ethically justified uses *are* imaginable, if

2) the *marginal net harm* presented by the *risk(s) inherent in the technology that ethically unjustified uses will occur* outweighs the *marginal net benefit* presented by the aggregate of ethically justified uses of the technology.

Now, for the *artifact level*, the set of conditions is very similar. From an ethical standpoint, I argue that an artifact should be disallowed only if

a) all imaginable uses of the artifact can, with a reasonable amount of certainty, be considered ethically unjustified,

or, in case ethically justified uses *are* imaginable, if

b) the *marginal net harm* presented by the *risk(s) inherent in the artifact that ethically unjustified uses will occur* outweighs the *marginal net benefit* presented by the aggregate of ethically justified uses of the artifact.

Some explanatory remarks are in order here. Firstly, in the set of conditions for the technology level the word "uses" is meant to indicate applications as well as artifacts, so these conditions mean that we should have a look at the artifacts and applications of a technology before we decide on its ethical admissibility. In the set of conditions for the artifact level, "uses" only refers to applications.

Secondly, the phrases "*marginal* net harm" and "*marginal* net benefit" refer to, respectively, the net harm presented by the inherent risk(s) of unethical uses and the net benefit of ethical uses, both of them *compared to existing and alternative practices*. Furthermore, *to the extent that* the expected ethically unjustified and justified uses of the new technology or artifact likely cannot be effectively prevented through a prohibition of this technology or artifact (as, perhaps, the "technological genie" is already out of the bottle), these unjustified and justified uses should, too, form part of the basis of comparison in determining the marginal net harm and marginal net benefit.

Thirdly, by "*inherent* risk(s) of ethically unjustified uses" I mean risks of unethical uses that are very hard to prevent as they mostly result from the technology or artifact itself—not from individual applications. Unethical uses that occur in the context of particular applications (such as harassment by journalists in the gathering of news using drones) should be factored in into the evaluations of these applications; however, some unethical uses constitute applications themselves (such as terrorists using drones to scope out government buildings) and, as such, their occurrence should be seen as inherent risks of either the technology at large or the artifact category.

Fourthly, care must be taken to properly account for issues that are hard to pick up on when considering *individual* uses of a technology or artifact, but which can clearly be seen when the *sum totals* of risks and ethically justified uses are considered. For example, when a single application of drones is evaluated, it is easy to overlook its relatively insignificant contribution to a societal "chilling effect"; however, when considering all drone applications at once, this "chilling effect" becomes much more apparent.

Fifthly, to *prohibit* a technology or an artifact can mean one of several things: prohibition of the development and use of the technology or artifact, prohibition only of its use, or prohibition only of its use in one or more particular contexts (such as a civil, military, or scientific context). The precise definition of the term can have a significant influence on whether or not the conditions for prohibition are met. When evaluating the prohibition of a technology or artifact in terms of its *development and use*, we must, when considering the second condition, account for any inherent risks that the *mere existence* of a technology or artifact will eventually lead to it being appropriated in ethically unjustified ways;[31] when evaluating whether only its *use* should be prohibited, we focus only on those risks inherent in the technology or artifact that are the result of any of its potential applications being allowed.[32]

Sixthly and finally, for all the uses that are considered in the evaluation of a technology or artifact, the marginal harms and benefits should be given weight on the basis of their *societal importance*. As I have argued in the previous chapter (and reiterated in section 7.2), assigning weight to benefits and harms on the basis of their relative societal importance is most useful at the artifact and technology levels since at these levels we are often dealing with ethical impacts at a society-wide scale. However, if the focus is clearly on whether to prohibit of the use of a technology or an artifact *within a particular context* (of society), then we should switch back to assigning weight on the basis of *contextual* importance. Nevertheless, the *civil context*—which will be the context of our evaluations in this chapter—can roughly be equated to society at large, allowing us to still use the concept of societal importance. Finally, to determine the final balance at the second condition, it is most convenient to aggregate separately all weighted marginal harms and all weighted marginal benefits, over all ethical and unethical uses under consideration, and then compare the two totals.

Considering all of the above, it is harder for a technology or artifact to be deemed ethically impermissible on the basis of the first condition than it is on the basis of the second condition. For example, whereas human cloning technology may not be disallowed on the basis of the first condition, given the sole fact that ethically justified *therapeutic* applications of cloning are imaginable, many would argue that it should be disallowed based on the second condition, considering that permitting such therapeutic applications creates an unacceptable risk of *reproductive* applications of cloning eventually being realized as well. In most cases, however, it is a tall order to ban a technology or artifact on the basis of these conditions. Nevertheless, even if a technology or artifact has previously been considered admissible, the evaluation should regularly be performed again to factor in new facts and insights.

Unfortunately, the method argued for here of evaluating the admissibility of a technology or artifact is not entirely free of issues. First of all, for many emerging technologies, establishing the risks and determining their importance is a highly speculative endeavor. If the risks are *potentially* very high, it might be better to

[31] An example of such a risk is criminals or rogue government agencies trying to get their hands on a technology or artifact that exists on paper or in prototypes, but has never seen practical applications due to ethical considerations.
[32] For example, in the general use of a particular technology or artifact, there might be an inherent risk of *function creep* or abuse (as we have seen in the case of drones).

apply the *precautionary principle*[33] than the method described here. Secondly, in most cases, the importance of the inherent risks of ethically unjustified uses is at least somewhat dependent on the ethically justified uses: the occurrence of certain *unjustified uses* may be less likely if certain other *justified uses* do not occur. Properly accounting for this effect would make the evaluation significantly more complicated. Thirdly and finally, this method does not distinguish between present uses and effects of a technology or artifact and likely future uses and effects; a technology could be admissible now given the state of the technology and society, while in 20 years its development may have reached a point where the importance of the inherent risks renders it inadmissible. Clearly, these issues deserve much more attention than I am able to give them here; however, I still consider our method sufficiently useful for evaluating the admissibility of drone technology and artifacts.

Thus, I will use the above-described conditions for ethical prohibition of a technology or artifact to determine the ethical admissibility of surveillance-capable drone technology and all three types of surveillance-capable drone artifact in the next two sections of this chapter.

7.3 Evaluating drone technology

Let us now evaluate surveillance-capable drone technology at large. As stated in chapter 5, "drone technology capable of public surveillance" refers to a collection of the most elemental features of surveillance-capable drones. In the introduction, I have defined surveillance-capable drones as unmanned, non-tethered aircraft, including supporting systems on the ground, that can fly using an onboard means of propulsion; are remotely controlled by human pilots or self-controlled by onboard computers; and contain onboard sensor systems consisting of at least a visual-spectrum camera. In addition, the quintessential drone would have a relatively low visual and audial profile and would send sensor data to the ground via wireless communication.

This section has two parts, serving two main purposes. In the first part, we will evaluate the importance of the ethical issues inherent in drone technology at large, which were identified level in chapter 5. With respect to the technology level of ethical analysis, we thus intend to answer the second main research question of this thesis, which holds: *What ethical issues need to be considered in efforts to improve the ethical justifiability of the civil use of unmanned aerial systems (UASs) that are capable of public surveillance?* We start off with the second research question because the answer to this question informs the answer to the first research question.

In the second part, we will evaluate whether, from an ethical standpoint, we ought to allow drone technology to be used *in a civil context*. With respect to the technology level, we thus intend to answer the second main research question of this thesis, which holds: *To what extent is the civil use of unmanned aerial systems (UASs) that are capable of public surveillance ethically justified in light of its potential effects on privacy and other ethical values?* The final verdict on the ethical admissibility of drone technology at large is made on the basis of the present and predicted future state of the technology (in about the year 2030); potential future policy measures taken on the basis of an analysis of the ethical issues concerning this technology and their societal importance could render the technology more ethically justified than argued for here.

[33] The precautionary principle states that any action or policy that could carry a risk of causing (major) harm to the public or to the environment should not be carried out in the absence of scientific consensus that the action or policy does not present any (major) risk, with the burden of proving the action is not harmful falling on those intending to take the action.

Figure 18: Assembling a drone.

Importance of the identified ethical issues

We are now to determine the importance of the inherent ethical issues identified at the technology level in chapter 5. To some extent, this importance could already be inferred from the descriptions of the issues in that chapter. However, this section offers some clear arguments and statements concerning the matter on the basis of Barak's (2010) concept of societal importance. It is worth noting that the levels of importance we will arrive at are *averages* because the significance of ethical issues that are inherent a technology is always somewhat variable in the context of particular applications.

Let us start with the issues of privacy, which we have already termed as some of the most important issues inherent in drone technology. First, we need to consider why we view privacy—in particular, the kinds of privacy that are under threat by drone technology—as being important. In chapter 4, we learned from Finn et al. (2013) that the five types of privacy that drone technology at large is expected to have a negative impact on are instrumentally valued for their collective support to the values of autonomy; freedom of thought, action, assembly, speech, worship and expression; and democracy. Moreover, we found that any of the five individual types of privacy supports at least some form of freedom or autonomy.

With regard to the importance of privacy *in general*, Helen Nissenbaum (2010) references the work of Jeroen van den Hoven (2001), who, she argues, "offers one of the clearest accounts of the value of privacy for individuals" (p. 78). Van den Hoven identifies four types of moral reasons for why privacy deserves protection. Firstly, he argues, privacy offers protection against *informational harm*, as it protects against identity theft and undesirable access to personal information. Secondly, privacy reduces *informational inequality*, as it restricts the ability of governments and corporations to collect information about individuals in a one-way, opaque fashion. Individuals engaging with providers of goods and services may be unaware that information is being systematically collected, have no idea what happens to it beyond the point of the initial transaction, and not realize that information they share freely has a value in the information marketplace. Thirdly, privacy protects against *informational injustice*, as it ensures that information is only used in the appropriate context. Building on Michael Walzer's (1984) concept of "spheres of justice" (which we discussed in the previous chapter), Van den Hoven argues that information

belonging in one sphere should not be allowed to migrate into another or others, because if it does, informational injustice will have been perpetrated.[34] Finally, privacy guards against *encroachment on moral autonomy*, as it constitutes one of the conditions for developing critical faculties and moral independence among individuals.[35] In my view, the first and fourth of these reasons—protection against informational harm and encroachment of moral autonomy—are the most important justifications for privacy at the technology level of our analysis since the issues of informational inequality and informational injustice are very much dependent on the specific applications of drones.[36]

We can now determine the importance of the privacy issues inherent in surveillance-capable drone technology. It appears from the analyses of Finn et al. (2013) and Van den Hoven (2001) that the basic values affected by privacy issues at the technology level include various kinds of freedom, safety from informational harm, moral autonomy, and democracy.[37] Now, what would be the societal importance of these values? Naturally, in a liberal democratic society, all of these values are considered very important, if not fundamental. Thus, considering the potential extent of the *marginal* privacy violations (i.e., with respect to existing practices) as described in chapter 5, and the societal significance of the underlying values that are affected, I must conclude that these harms are of very high importance. Of particular importance, perhaps, is the impact on *behavioral privacy*, as it contributes very strongly to a "chilling effect" (see section 5.1.1) in outdoor space—one involving serious harms to freedom, autonomy and democracy. It is through this "chilling effect" that large-scale civil drone use may evoke images of a dystopian societal *panopticon*.[38]

We now need to evaluate the importance of the other potential ethical issues inherent in drone technology that were identified in chapter 5. To begin, the issue of *function creep* can have an impact on various types of privacy and on values such as equality and safety. Given the fact that these values are important socially, the fact that surveillance-capable drone technology has a very wide range of potential applications that includes many controversial uses, and the fact that drone use tends to entail diminished transparency and accountability, I conclude that this ethical issue, too, is very important—though not quite as important as the privacy issues.

As regards the issues of *unequal burden of surveillance*, *discriminatory targeting* and *profiling*, these all have an impact on equality, which is of fundamental value to liberal democratic societies in the EU. Discriminatory targeting in drone surveillance practices can significantly increase social alienation and distrust among affected individuals and groups, and undermine social cohesion (Finn et al., 2013). In

[34] Note the similarity to contextual integrity. An example of such injustice would be if a job candidate's medical history or religious affiliation found its way into the files of a company considering him for employment.

[35] Moral autonomy, according to van den Hoven, is "the capacity to shape our own moral biographies, to reflect on our moral careers, to evaluate and identify with our own moral choices, without the critical gaze and interference of others and pressure to conform to the 'normal' or socially desired identities" (2001, p. 439).

[36] Van den Hoven (2001) presents informational inequality as an issue involving government and corporate actors, and in the previous chapter we have learned that flows of personal information between contexts can be justified in certain drone applications.

[37] There is some interrelatedness among these values; for example, informational safety benefits freedom, and autonomy is necessary for a healthy democracy.

[38] The panopticon is a type of prison building designed by the English philosopher and social theorist Jeremy Bentham in the late 18th century. The concept of its design is to allow all inmates to be observed by a single watchman without them being able to tell whether or not they are being watched. Although it is physically impossible for the single watchman to observe all cells at once, the fact that the inmates cannot know when they are being watched means that all inmates must act as though they are watched at all times, effectively controlling their own behavior constantly.

addition, profiling practices aided by drones can generate unparalleled levels of social sorting and segmentation which could have consequences that are profoundly unfair. Therefore, I consider these two ethical issues to be very important. In my view, the unequal burden of surveillance that may be experienced by waste collectors, gardeners, couriers, and police patrolmen and other groups that spend a lot of time outdoors is of somewhat lesser importance since the members of these groups are usually not specifically targeted by the surveillance for the sole reason of being outside.

The issues of *abuse, error and accountability* inherent drone technology can have an impact on values such as privacy (and its underlying values), equality, safety from informational harm, and accountability. In light of the fact that drones have a natural tendency to operate covertly, and thus without transparency, the incidence of these issues and extent of the harm they present to the affected values is likely to be great. Considering this and the societal significance of the values at stake, I conclude that the abuse, error and accountability issues are generally also of high importance.

Finally, let us evaluate the importance of the issue of the *shifting of ethical norms* resulting from the use of drone technology. As argued in chapter 5, any shift in ethical norms as a result of drone use may be unethical if the new norms are conducive of practices that violate fundamental civil and human rights such as those outlined in the United Nation's Universal Declaration of Human Rights and the Council of Europe's European Convention on Human Rights. Various values could be affected, such as privacy, equality, and freedom. While the effects of a shift in ethical norms could be very serious, it is not certain that drone technology can bring it about. Roger Clarke (2014) argues that even as technological development continually expands the capacity of other parties to invade private space, the underlying human need for (and the reasonableness of the expectation of) privacy does not change. Considering this uncertainty, I deem the issue to be of moderate importance.

Ethical admissibility of surveillance-capable drone technology

We have just evaluated the importance of all the ethical issues of drones at the technology level. Given the seriousness of many of these issues, I believe it is fair to ask whether, from an ethical standpoint, we ought to allow the surveillance-capable drone technology to be used in civil contexts. After all, there have been many voices in recent years calling for a total ban on all drone activity in most or all civil contexts (for example: Zorn, 2015; DiMascio, 2015; Schaper, 2015).[39] Let us therefore try to answer this question by applying our method of evaluating a technology's ethical permissibility to our case.

In section 7.2, I argued that a technology should be prohibited outright only if

1) all imaginable uses of the technology can, with a reasonable amount of certainty, be considered ethically unjustified,

or, in case ethically justified uses *are* imaginable, if

2) the *marginal net harm* presented by the *risk(s) inherent in the technology that ethically unjustified uses will occur* outweighs the *marginal net benefit* presented by the aggregate of ethically justified uses of the technology.

[39] To be fair, the arguments provided for banning drone use in civil contexts generally do not exclusively relate to the surveillance capabilities of drones. Often, their potential weapons capabilities and their potential use by terrorists receive more prominent attention.

To begin, it is quite obvious that drone technology does not meet the first condition, since, as we have seen in the previous chapter, ethically justified civil applications of surveillance-capable drones do exist. We even argued that, given the right circumstances and parameters, persistent surveillance applications of drones for law enforcement purposes can be ethically justified.

Evaluating whether the second condition is met takes a bit more effort, as this depends on determining the inherent risks of the occurrence of unethical uses of drone technology, and on identifying the ethically justified uses of drone technology. While we have learned about the risks inherent in drone technology in chapter 5, we do not have at our disposal a complete contextual analysis of all possible drone applications. Therefore, as to the marginal net benefit offered by the collection of ethically justified drone applications, we must make do with some educated guessing. There are a number of applications of which I expect that they will offer significant marginal benefits and relatively small marginal harms. These applications are in contexts where there are fewer people, meaning that the ethical issues identified in chapter 5 are generally of lesser importance here. One prominent example is drone-aided agriculture, where drones fly above farm fields to inspect crops, providing about five Euros in cost savings per hectare (Levin, 2015) (thus potentially providing billions of Euros in cost savings to the entire agriculture sector), while only few people end up involuntarily having their personal data captured. Another example is search and rescue missions, where drones may be of great help in locating missing persons in mountainous areas that are sparsely visited, meaning that surveillance harms are minimal (though not non-existent). Wildlife monitoring, climate research, mining, and disaster response are other prime examples where one would expect the benefits to clearly outweigh the costs. To be sure, there may still be other beneficial uses of drones, which is something we should take into account in this evaluation.

The net benefit of all of these applications needs to be weighed against the net harm presented by the inherent risks of unethical applications of drone technology. Some of these risks of unethical applications result from *function creep* (see section 5.1.2). One example of a function creep risk is a situation where the police purchases drones to help with road accident investigations, but ends up using them primarily to patrol crime-ridden neighborhoods—which, from an ethical viewpoint, may be questionable. Other risks can be grouped as purposely illegal usage by government agencies, companies and private users (see section 5.1.2). As previously argued, government agencies may be eager to take the use of developed drone technology to the limits of its capabilities for the sake of national security, even if there is no democratic mandate and no widely accepted moral justification for doing so. Drone technology may thus become a tool for institutional abuse. Furthermore, in the commercial sector, a corporate spy could use a drone to spy on a competitor company to learn about this company's trade secrets. Finally, it is not hard to image advanced drone technology falling into the hands of criminals who could use drones to secretly transport illicit substances or scope out places in the context of crimes they plan to commit. If drone technology is available, such questionable, or simply unethical, uses of drones would be hard to prevent.

It is now time to weigh the marginal net harms and marginal net benefits on the basis of their societal importance. This is a difficult task to perform since we have analyzed neither the ethically positive nor (the risks of) the ethically negative applications in a comprehensive way. Our evaluation therefore will have a significant subjective component, as gaps in our knowledge will need to be filled in with assumptions. That said, we can conclude the following. In abbreviated terms, the ethically most justified applications of drone technology are likely to offer great marginal benefits in terms of the pursuit of wealth, efficiency, safety, security, and environmental protection, while presenting comparatively small marginal harms to

values such as privacy, autonomy, and freedom. On the other hand, through function creep, overzealous government organizations, and criminally-minded companies and citizens, there is a moderately high risk of drone applications emerging that may in some cases provide significant marginal benefits to society in terms of justice and security, but at an often underappreciated high marginal cost to privacy, freedom, autonomy, democracy and other values. Nevertheless, with proper policy measures, I think the incidence of such ethically unjustified uses and the extent of their harms are manageable. So, even though many of society's most important values (which, according to section 7.2, include *human dignity*, *liberty*, *democracy*, *equality*, *the rule of law*, respect for *human rights*, and *privacy*) are negatively impacted, the severity of the impacts on these values is rather small; and although the positive impacts mostly concern interests and values that are of somewhat lesser importance socially, the severity of the impacts on these interests and values are significant. Thus, in my view, the sum of expected marginal benefits comfortably outweighs the sum of expected marginal harms. From this brief and necessarily incomplete analysis, it must therefore be concluded, at least for now, that civil surveillance-capable drone technology at large should not be banned from civil contexts.

What we have not considered thus far is the practicality of prohibiting drone technology from civil contexts. Civil drone technology has been around for some time now. Its use is widely distributed across the globe and its development is dispersed among many professional engineers and hobbyists. Furthermore, drone technology is, in part, an assemblage of various different technologies, such as electric and combustion motors, propellers, gyroscopes, batteries, and video cameras, all of which have many other practical purposes and therefore cannot be disallowed. Moreover, there exists military drone technology which is not likely to disappear and can easily be adapted for civil use. All of this would severely complicate any effort to enforce a hypothetical ban on drone technology, and affects the balancing of marginal benefits and harms in a way that renders banning drone technology an even less favorable option.

7.4 Evaluating drone artifacts

Now that we have evaluated civil surveillance-capable drones at the technology level of ethical analysis, it is time for us to conduct the same ethical evaluations at the artifact level for each of the three main types of drone artifact we distinguished in chapter 3. This section has three subsections, which respectively focus on evaluations of *large wide-area persistent surveillance drones* (section 7.4.1), *small general-purpose drones* (section 7.4.2), and *biomimetic spy drones* (section 7.4.3). Each subsection has two parts that jointly answer the two research questions for the respective type of drone. In a similar fashion to the previous section, we will evaluate first the importance of the ethical issues inherent in the drone category, and second whether, from an ethical standpoint, we ought to allow the type of drone to be used in a civil context. With regard to the latter evaluation, we will not focus solely on the ethical issues presented by the three main types drone in their basic, quintessential form, but also consider ethical issues presented by various additional advanced sensor systems and onboard data analysis systems that the drones may come equipped with.

Before we begin, let me reiterate that the final verdict on the ethical admissibility of each drone artifact is made on the basis of present and predicted future capabilities and applications (in about the year 2030). Future policy measures based on an analysis of an artifact's ethical issues may still improve the artifact's ethical justifiability. Let me also repeat that all of the ethical issues at the technology level apply to each of the three types of surveillance-capable drones. So, the issues that are now evaluated can be considered an extension to the evaluations of section 7.3 for each of the three types of drone.

7.4.1 Large wide-area persistent surveillance drones

Let us first evaluate the inherent ethical issues and ethical admissibility of large wide-area persistent surveillance (WAPS) drones. In chapter 3, these drones were defined as large, technologically advanced systems that have great endurance and offer so-called *persistent surveillance* capabilities over an extensive ground area. Automated person tracking systems are considered an essential future feature of these drones. In chapter 5, we identified two issues that are inherent in large WAPS drones, which are *increased moral distance to surveillance subjects* and *safety of flight*.

Figure 19: Wide-area persistent surveillance control room.

Importance of the identified ethical issues

The first inherent ethical issue of large WAPS drones raised in section 5.2.1 was the *increased moral distance to surveillance subjects*. The remoteness of WAPS drone pilots from their targets might cause in these pilots a detachment from the physical reality of the individuals who are in their sights, which may weaken the pilots' constraints of conscience and increase the risk of their committing abuse. This detachment is made substantially worse by the fact the images captured by WAPS drones are less clear and vivid representations of a particular situation, with the effect that the drone operators experience less intimacy with their targets. The increased moral distance to surveillance subjects has an impact on the various types of privacy and on values such as equality and safety. Given that these values are very important socially, combined with the fact that drone use tends to entail diminished transparency and accountability (which makes it harder for individuals to guard themselves against the harms resulting from this ethical issue), I conclude that this ethical issue is very important.

The second ethical issue concerning large WAPS drones raised in section 5.2.1 was *safety of flight*. For the near future, it can be expected that large wide-area persistent surveillance drones are not going to be as safe as traditional manned aircraft. Specific issues include a limited ability to detect and avoid trouble; pilot error; persistent mechanical defects; and unreliable communications links (Whitlock, 2014). Only one of these—the unreliability of communications links—may be a permanent issue with large wide-area persistent surveillance drones due to the fact that wireless communication makes drones inherently vulnerable to hacking, and by extent vulnerable to be used as a weapon in a terrorist attack. Considering

the relatively low numbers of WAPS drones that are likely to fly above population centers, I expect all of these problems to moderately increase the safety risks for other (passenger) aircraft and people on the ground. Thus, given that safety from physical harm is of fundamental importance to any society, I consider the issue of flight safety to be of moderate to high importance.

Ethical admissibility of large wide-area persistent surveillance drones

Given the seriousness of both these issues, it is fair to ask whether we ought to allow WAPS drones to be used at all. Let us therefore apply our method of evaluating an artifact's ethical permissibility. In section 7.2, I argued that an *artifact* should be prohibited outright if

a) all imaginable uses of the artifact can, with a reasonable amount of certainty, be considered ethically unjustified,

or, in case ethically justified uses *are* imaginable, if

b) the *marginal net harm* presented by the *risk(s) inherent in the artifact that ethically unjustified uses will occur* outweighs the *marginal net benefit* presented by the aggregate of ethically justified uses of the artifact.

The first condition is clearly not satisfied, since ethically justified civil applications of WAPS drones do exist. In the previous chapter, we saw that law enforcement applications of WAPS drones can be ethically justified in special circumstances, such as the Olympic Games. Now, to evaluate whether the second condition is met, we first need to estimate the inherent risks of unethical applications of WAPS drones, and we must identify, in broad stokes, the ethically justified uses of these drones. Then, we need to estimate, respectively, their collective marginal net harm and collective marginal net benefit.

There are a number of ethically justified potential applications of WAPS drones in a civil context. Applications in search and rescue missions, wildlife monitoring, disaster response, and *some* law enforcement contexts are likely to prove beneficial. However, the *marginal* net benefits they provide—with respect to *small general-purpose drones*—are probably not very great. In fact, in many of these applications, the use of these small general-purpose drones may prove equally or more beneficial. This is because much the surveillance capacity of WAPS drones is likely to be redundant in many of these applications, and because the use of small general-purpose drones is probably significantly more cost-efficient. Only in some critical law enforcement applications do WAPS drones really come into their own.

Now, any collection of permitted of WAPS drone applications brings with it risks of function creep and intentional misappropriation. A situation could emerge where a WAPS drone is acquired by law enforcement to help protect an important public event, such as the Olympic Games, but ends up being used for generalized round-the-clock public surveillance. Furthermore, intelligence services could intentionally misappropriate a WAPS drone to spy on large numbers of individuals who fit a certain profile. Even though such unethical potential applications can have very significant impacts, I believe the risks of these becoming a reality are only moderate. In my view, it is probable that systematic departures from the accepted use pattern of WAPS drones are discovered rather quickly, as these systems are quite large and cannot be operated in a fashion that is completely covert; and such transgressions are likely to be promptly denounced by the public at large.

We may now weigh the marginal net benefits against marginal net harms on the basis of their societal importance, and decide on the ethical admissibility of WAPS drones in a civil context. Many of society's

most important values, such as privacy, autonomy and democracy, are negatively impacted in a situation where ethical justified civil uses of WAPS drones are allowed (the impacts are caused by both the justified uses and the accompanied risks of unjustified uses); however, I deem the general severity of the impacts on these values to be rather small. On the other hand, the socially important values of justice and security are positively impacted, and although these values are fewer in number, the intensity of the impacts on them is moderate. In my view, the sum of all expected marginal benefits just about balances out the sum of all expected marginal harms, meaning that the second condition for prohibition, too, is not satisfied. Therefore, I must conclude from this brief and necessarily incomplete analysis that large WAPS drones should not be banned in advance from civil contexts.

7.4.2 Small general-purpose drones

Let us now evaluate the inherent ethical issues and ethical admissibility of small general-purpose drones. In chapter 3, these drones were defined as systems that lack the range, the speed, the wide-area perspective, and the sophisticated sensor payload of WAPS drones, but are much cheaper and easier to procure, operate, and maintain, and can observe and record scenes in high detail from up close and from many different angles, thus making them highly versatile. Two ethical issues were found to be inherent in small general-purpose drones, which are *concerns about privacy of the person* and *safety of flight*.

Figure 20: Various small general-purpose drones.

Importance of the identified ethical issues

As we saw in subsection 5.2.2, there is a set of privacy concerns specific to small general-purpose drones that relates to *privacy of the person*, which refers to the right to keep one's body functions and body characteristics private. Small general-purpose drones may substantially infringe upon privacy of the person due to their powerful camera systems, which allow various biometric properties of a surveillance subject, such as facial characteristics, to be recorded and analyzed. Bodily privacy is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society (Finn et al., 2013). Given the high societal importance of this type of privacy, and the extent of the harm to it, I consider this set of privacy concerns to be of high importance.

A second issue relating to small general-purpose drones that was explained in subsection 5.2.2 was that their large-scale deployment is likely to carry significant flight safety risks. Drones of this type are likely to be less well built, less well maintained, and less well piloted than manned aircraft. Moreover, massive numbers of them could be zipping through the skies in the future. Also, like large wide-area persistent surveillance drones, they are inherently vulnerable to cyber-attacks. Even with proper standards and regulations in place, the risks to other (passenger) aircraft and people on the ground could be significant. Considering all of this and the societal importance of safety from physical harm, I consider safety risks to be of high importance.

Ethical admissibility of small general-purpose drones

Given the importance of these issues, it is fair to ask whether we should disallow the use of small general-purpose drones. Once again, let us apply our method of evaluating an artifact's ethical permissibility—which holds that an artifact should be prohibited outright if (a) all imaginable uses of the artifact can, with a reasonable amount of certainty, be considered ethically unjustified, or, in case ethically justified uses are imaginable, if (b) the marginal net harm presented by the risk(s) inherent in the artifact that ethically unjustified uses will occur outweighs the marginal net benefit presented by the aggregate of ethically justified uses of the artifact.

The first condition is obviously not met, since we saw in the previous chapter that at least certain applications of small general-purpose drones in journalism can be ethically justified. Now, to evaluate whether the second condition is met, we first need to estimate the inherent risks of unethical applications of small general-purpose drones, and we must identify, in broad stokes, the ethically justified applications of these drones. We then need to estimate, respectively, their collective marginal net harm and collective marginal net benefit.

Owing to the high versatility of small general-purpose drones, the number of ethically justified potential applications in a civil context is large. These ethically justified applications are virtually the same as those listed for drone technology at large in section 7.3. What is crucial about them is that they are often set in contexts where there are generally fewer people, meaning that the inherent ethical issues identified in chapter 5 are generally of somewhat lesser importance. Thus, there are likely to be many net beneficial applications in areas such as agriculture, journalism, transportation, infrastructure inspection, search and rescue, wildlife monitoring, mining, climate research, health emergency response, and disaster response. It is almost certain that a few further fields exist in which small general-purpose drones can be used in ethically justified ways, which is something that needs to be taken into account here. Since we can expect very significant cost savings in agriculture, transportation, mining, etc., and much increased effectiveness in search and rescue, disaster response, etc., the marginal net benefit offered by the aggregate of the ethically justified applications of small general-purpose drones is likely going to be very high.

As for the inherent risks of unethical applications of small general-purpose drones, these result from function creep and malicious intent by various parties. Given the great versatility of these drones, these risks are significant. The police may acquire drones to help with the search for missing persons, but ends up using them to check for parking violations; companies may use them illegally to spy on competitors to learn about their trade secrets; and private citizens may use them to harass other persons, engage in voyeurism, and other more serious criminal behavior. These are just a handful of the unethical applications of small general-purpose drones that are likely to emerge (a few more have been mentioned

before in previous chapters). In 2030, when drone use could be a fully established part of society, the marginal net harm presented by the aggregate of such applications of is likely going to be high.

Let us now weigh the marginal net benefit against marginal net harm on the basis of their societal importance, and decide on the ethical admissibility of small general-purpose drones in civil contexts. Many of society's most important values, such as privacy, freedom, autonomy, dignity, equality and democracy, are negatively impacted in a situation where ethically justified civil uses of small general-purpose drones are allowed (the impacts being caused by both the justified uses and the accompanied risks of unjustified uses); and I consider the general intensity of the impacts on these values to be moderate to high. On the other hand, other values and interests, such as the pursuit of wealth (with trickle down benefits to society at large), public health, justice, security, various kinds of efficiency, convenience, and entertainment, are positively impacted. Some of these are perhaps of somewhat lesser social importance; however, the intensity of some of the positive impacts (such as on wealth, efficiency, security and public health) is likely to be very high. In my view, the sum of all expected marginal benefits outweighs the sum of all expected marginal harms by a considerable margin, meaning that the second condition for prohibition, too, is not satisfied. Thus, I must conclude from this brief and necessarily incomplete analysis that small general-purpose drones should not be banned in advance from civil contexts.

7.4.3 Biomimetic spy drones

Finally, let us evaluate the inherent ethical issues and ethical admissibility of the last category of drones: the biomimetic spy drones. In chapter 3, these drones were defined as very small systems that can hide in plain sight through mimicking the size, appearance and behavior of insects and birds, and as such have a great future potential for covert surveillance applications. Three issues were found to be inherent in biomimetic spy drones, which are *concerns about privacy of the person*, *increased potential for privacy harms*, and *potential harm to (the experience of) wildlife*.

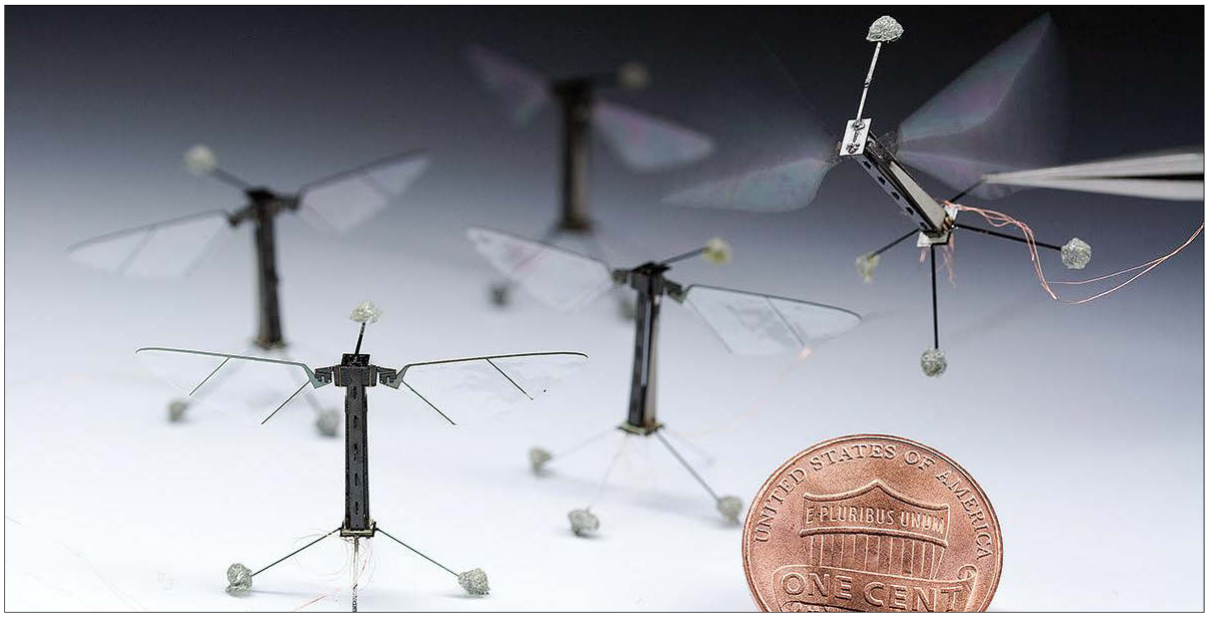

Figure 21: Very small insect-like drone prototypes.

Importance of the identified ethical issues

In section 5.2.3 it was argued that, like small general-purpose drones, biomimetic spy drones may infringe upon *privacy of the person* since they can get very close to people without being noticed and use their cameras to capture various types of biometric data of their targets. Beyond plain imagery of people's faces, they might be able to obtain fingerprint data, and iris pattern data, all of which are very sensitive kinds of biometric data. Given the high societal importance of this type of privacy, and the extent of the harm to it, I consider this set of privacy concerns to be of high importance.

Another issue was that, compared to drones of other types, biomimetic spy drones have an exacerbated impact on other types of privacy, including behavioral privacy, privacy of location and space, privacy of property and privacy of association. Due to their ability to hide in plain sight, they can come closer to a person without being noticed than any other type of drone, which means that they can generally observe a given situation from better vantage points. It is thus likely that they can covertly gather better data on people's behavior, their location, their property and their relations with other people. The values affected by the exacerbated privacy issues include various kinds of freedom, safety from informational harm, moral autonomy, and democracy. As mentioned earlier, these are socially very important values. Considering all of this, I must conclude that these exacerbated privacy issues are of very high importance.

Finally, in section 5.2.3 it was argued that biomimetic drones could harm wildlife through their likeness to specific types of animals. Their existence may evoke aggression towards animals whose likeness is borne by these drones. When used in large numbers, they may also affect the normal behavior of insects and birds nearby and cause physical harm to animals that see these drones as prey. Ultimately, biomimetic drones might even adversely affect entire ecosystems. Furthermore, in areas where they are present, they may prevent people from experiencing wildlife in a pure, authentic form. Thus, the values that are potentially harmed include animal wellbeing, the natural order of things, and general human wellbeing. Although these values are not mentioned in the *Treaty on European Union*, animal rights and the protection of ecosystems have become increasingly important in liberal democratic Western societies. I therefore consider the issues of harm to wildlife and harm to the experience of wildlife to be very important.

Ethical admissibility of biomimetic spy drones

Considering the importance of these issues, it is fair to ask whether we should disallow the use of biomimetic spy drones. One last time, we are going to apply our method of evaluating an artifact's ethical permissibility—which holds that an artifact should be prohibited outright if (a) all imaginable uses of the artifact can, with a reasonable amount of certainty, be considered ethically unjustified, or, in case ethically justified uses are imaginable, if (b) the marginal net harm presented by the risk(s) inherent in the artifact that ethically unjustified uses will occur outweighs the marginal net benefit presented by the aggregate of ethically justified uses of the artifact.

Let us consider the first condition. As explained in chapter 3, biomimetic drones will add an important dimension to the repertoire of drone capabilities, in that they will be able to come very close to their targets while going largely unnoticed—or, at least, unnoticed *as being drones*. This capability will make them very formidable spying tools. For some high-stakes covert surveillance applications—for example, in the field of counter-terrorism—their use will undoubtedly be ethically justified, meaning that the first condition for prohibition of these drones is not satisfied.

Let us now evaluate whether the second condition is satisfied. As stated in chapter 3, civil applications of biomimetic drones will include security surveillance, search and rescue, traffic monitoring, environmental monitoring, include workplace security, private investigations, inner-city courier services, outdoor event documenting, and athlete tracking at sports events, home security, amateur photography and filmmaking, citizen journalism, advanced gaming, snooping on other people and transporting illicit substances. In the majority of the applications, the use of these bird-like or insect-like aircraft presents very serious risks of various kinds of privacy infringement and resultant informational harm, loss of freedom and loss of autonomy, as well as other risks, such as potential harm to animal wellbeing, ecosystems and the enjoyment of nature. Furthermore, in many applications, the *marginal* net benefit of the use of biomimetic drones is going to be small or nonexistent when compared to the use of *small general-purpose drones*. Therefore, in my view, many civil applications of biomimetic drones are not ethically justifiable. The only applications I would consider ethical are for critically important law enforcement missions, mainly in the area of counter-terrorism. Thus, the marginal net benefit offered by the aggregate of the ethically justified applications of biomimetic spy drones is likely going to be fairly small.

Inherent risks of unethical applications of biomimetic spy drones may result from function creep within law enforcement. Considering the insidiousness of the function creep effect and the high versatility of these drones, the risks are quite significant. In 2030, biomimetic drones may well be capable of swarming through alleys, crawling across windowsills, and perching on power lines, all the while capturing decent quality audio and video while their targets would be none the wiser. For law enforcement and intelligence organizations, the temptation to use these drones for other, more mundane purposes than counter-terrorism missions may be too great to resist. A large swarm of biomimetic drones could, for example, be used to create a surveillance dragnet for an entire neighborhood, which could save costs on regular police patrols and increase suspect apprehension rates. There is also a small chance that through law enforcement use these drones could eventually come to be used by commercial security providers and other companies, or fall into the hands of ordinary citizens or criminals, which may lead to further unethical uses. Such spreading of the use of biomimetic drones beyond law enforcement applications may have a profound social effect in that it might make the public wary of everything that looks like an insect or a bird—for anyone from a law enforcement agent to the next-door neighbor could secretly be watching. In light of all this, I judge the marginal net harm presented by the risks of unethical applications (in case usage of these drones is restricted to critical law enforcement applications) to be moderate.

Let us now weigh the marginal net benefit against marginal net harm on the basis of their societal importance, and decide on the ethical admissibility of biomimetic spy drones in civil contexts. Many of society's most important values, such as privacy, freedom, autonomy, dignity, equality and democracy, are negatively impacted in a situation where ethical justified law enforcement uses of biomimetic drones are permitted; and I consider the general intensity of the impacts on these values to be moderate to small. On the other hand, the socially important values of justice and security (and their cost-efficiency) may be positively impacted, and the intensity of these impacts is likely to be moderate. In my view, the sum of all expected marginal benefits is slightly outweighed by the sum of all expected marginal harms. Thus, I conclude from this brief analysis that biomimetic spy drones should be banned from all civil contexts, including law enforcement, ahead of the realization of their use potential in real-world applications.

It must be emphasized that, in this case, the balance is not overwhelmingly in favor of a ban. If it is convincingly shown that there can be adequate safeguards to counter the threat of function creep, one

might still be able to justify a decision to allow the usage of biomimetic drones for specific law enforcement applications. However, these drones should, in my view, certainly be banned in all other civil contexts—at least to the extent that they are highly imperceptible and easily mistaken for insects, birds or other animals.

7.5 Conclusion

In this chapter, I carried out the *evaluation stage* of ethical analysis at the technology and artifact levels of Brey's (2012) anticipatory technology ethics (ATE) approach. I used this stage to provide the remaining answers to the two main research questions of this thesis. The first research question was: *To what extent is the civil use of unmanned aerial systems (UASs) that are capable of public surveillance ethically justified in light of its potential effects on privacy and other ethical values?* The second was: *What ethical issues need to be considered in efforts to improve the ethical justifiability of the civil use of unmanned aerial systems (UASs) that are capable of public surveillance?* Thus, I evaluated the ethical admissibility and the importance of inherent ethical issues of drone technology at large and all three main categories of drones. To do so, I used the concept of *societal importance* from Barak's (2010) proportional balancing approach to establish what ethical values are to be considered important in our evaluations, and I devised a set of general conditions that, in my view, need to be satisfied if a technology or artifact is to be prohibited from an ethical perspective.

I first showed how the relative importance of ethical values can be determined for evaluations of the importance of ethical issues inherent in drone technology at large and drone artifacts. Following Barak (2010), I explained that what are primary values at the technology and artifact levels depends on a *society's* own circumstances and constitution, reflecting its unique challenges, history, and self-perception; and it depends on whether a value's realization constitutes a condition for the realization one of more other values. Then, I established what ethical values are socially most important for our analysis. Drawing inspiration from the Treaty on European Union, I listed dignity, freedoms, equality, solidarity, democracy, citizens' rights and justice as fundamental values. Privacy, I argued, is perhaps even more important since it provides crucial support to the realization of many of these values.

I subsequently presented a method to determine the *ethical permissibility* of drone technology and artifacts. I contended that, from an ethical perspective, a technology or artifact should be prohibited outright only if (1) all imaginable uses of the technology or artifact can, with a reasonable amount of certainty, be considered ethically unjustified, or, in case ethically justified uses *are* imaginable, if (2) the *marginal net harm* presented by the *risk(s) inherent in the technology or artifact that ethically unjustified uses will occur* outweighs the *marginal net benefit* presented by the aggregate of ethically justified uses of the technology or artifact.

Finally, I made evaluations of the ethical admissibility and the importance of inherent ethical issues of drone technology at large and all three main categories of drones. At the technology level, it was found that the previously identified privacy concerns, especially those pertaining *behavioral privacy* (mainly, the "chilling effect" on society), are of a very high importance. As for the other ethical issues at this level, the issues of *function creep*, *discriminatory targeting and profiling*, and *abuse, error and accountability* were considered to be very important; the issues of *unequal burden of surveillance* and *shifting of ethical norms* were deemed to be of only moderate importance. As regards the ethical admissibility of drone technology

at large, I concluded that there should not be a categorical ban on the use of drone technology in civil contexts, since the marginal benefits provided by such use comfortably outweigh the marginal harms.

At the artifact level, it was found that, for large wide-area persistent surveillance drones, the issues of *increased moral distance to surveillance subjects* and *safety of flight* are respectively of high importance and moderate importance; for small general-purpose drones, the issues of *concerns about privacy of the person* and *safety of flight* were both judged to be of high importance; and for biomimetic spy drones, the issue of *increased potential for privacy harms* was judged of very high importance, and the issues of *concerns about privacy of the person* and *potential harm to (the experience of) wildlife* were considered to be of high importance. As regards the ethical admissibility of the three main types of drones, we concluded that there should not be a categorical bans on the use of large WAPS drones and small general-purpose drones in civil contexts; however, I concluded that a ban ought to be placed on biomimetic spy drones in civil contexts, unless there can be adequate safeguards against the threat of function creep, and at least to the extent that these drones are highly imperceptible and easily mistaken for the animals they are intended to mimic.

To conclude this chapter, I would like to make few final remarks. First of all, it should be noted that these evaluations, by necessity, had a rather large speculative and subjective component. Although I judged the importance of values and estimated the intensity of risks in a conscientious manner, others may hold somewhat different views and may arrive at conclusions that are different from mine but deserve equal merit. It is the methods that I devised, amended and used in this chapter—and indeed in this entire thesis—rather than the ethical conclusions reached here, that are the easiest to endorse. Secondly, there are no neat distinctions between the three types of drone; rather, there exists a continuum between them. How to deal with drones that are hybrids of, for example, small general-purpose drones (judged ethically admissible in civil contexts) and biomimetic spy drones (deemed ethically inadmissible in civil contexts) is an issue deserving of further analysis. Thirdly, the ethical conclusions reached here are not set in stone; it is important for the evaluations to be performed again at regular intervals in the future to account for potential new facts and insights—especially if the balance tilted only slightly in favor of one side. Fourthly and finally, the occurrence of some of the issues evaluated in this chapter is typically hard to prevent, but might be mitigated if appropriate policy measures are taken. Such policy measures may also improve the ethical justifiability of drone technology and artifacts. I will offer some recommendations as to such policy measures in the conclusion of this thesis.

8 Conclusion

This study has made a contribution to the ethical understanding of surveillance-capable drones in a civil context. I have set out to analyze the present and potential future capabilities of drones, the ethical issues they bring up, and their ethical admissibility. In all these areas, there has been little in the way of systematic and comprehensive research. Since the use of drones with aerial observation and surveillance capabilities is variously argued to present great benefits but also significant ethical concerns, such research was deemed in order. Specifically, I have tried to answer the following questions:

1. To what extent is the civil use of drones that are capable of public surveillance ethically justified in light of its potential effects on privacy and other ethical values?
2. What ethical issues need to be considered in efforts to improve the ethical justifiability of the civil use of drones that are capable of public surveillance?

In answering these questions, I focused separately on surveillance-capable drone technology at large, three types of surveillance-capable drones, and a small number of applications of such drones. Regarding *surveillance-capable drone technology*, I concluded that its use in civil contexts is ethically justified in principle since the marginal benefits offered by its present and future use in such contexts comfortably outweigh the marginal harms. Nevertheless, I found that many of the ethical issues inherent in the technology are very significant and deserving of careful consideration in any efforts to further improve its ethical acceptability. Firstly, it was argued that the privacy concerns relating to *behavioral privacy*, *privacy of location and* space, *privacy of association*, *privacy of property*, and *privacy of data and image* are of a very high societal importance. Of particular importance, perhaps, is the impact on *behavioral privacy*, as it contributes very significantly to a "chilling effect" on society in outdoor space—one that involves serious harms to freedom, autonomy and democracy. As for the other ethical issues at this level of analysis, the issues of *function creep*, *discriminatory targeting and profiling*, and *abuse, error and accountability* were judged to be very important; and the issues of *unequal burden of surveillance* and *shifting of ethical norms* were deemed to be of moderate importance.

In the analysis of *drone artifacts*, I distinguished three broad categories of surveillance-capable drones: *large wide-area persistent surveillance* (WAPS) *drones*, *small general-purpose drones*, and the anticipated *biomimetic spy drones*. As regards the ethical justifiability of these three types, I concluded that there should not be categorical bans on the civil use of large WAPS drones and small general-purpose drones; on the other hand, I argued that, unless there can be adequate safeguards against the threat of *function creep*, a ban ought to be placed on the civil use of biomimetic spy drones—a ban that should at least cover those biomimetic drones that are highly imperceptible and easily mistaken for the animals they are intended to mimic. All three types of drone were found to bring about important ethical issues that should be considered in efforts to mitigate their ethical consequences. For large wide-area persistent surveillance drones, the issues of *increased moral distance to surveillance subjects* and *safety of flight* are respectively of high importance and of moderate importance; for small general-purpose drones, the issues of *concerns about privacy of the person* and *safety of flight* were both judged to be of high importance; and for biomimetic spy drones, the issue of *increased potential for privacy harms* (due to their capability for stealthful, up-close observation) was judged to be of critical importance, and the issues of *concerns about*

privacy of the person and *potential harm to (the experience of) wildlife* were considered to be of high importance.

Finally, with regard to *applications of surveillance-capable drones* in civil contexts, I concluded that, while there are great concerns about such applications in general, by far not all of them are morally unacceptable; given the right circumstances and parameters, even persistent surveillance applications for law enforcement purposes can be ethically justified. In particular, under the conditions set by four specific but realistic application scenarios, I judged as *ethically justified* the use of small drones for journalistic coverage of socially important news events, and the use of WAPS drones to prevent terrorism during a very high-profile public event; and I judged as *not ethically justified* the use of a WAPS drone during a drugs investigation of moderate significance, and the use of WAPS drones to offer a real-time public mapping service. I further concluded that the justifiability of drone applications is generally highly dependent on whether the goals and values of the general contexts of everyday life in *outdoor public space* and *outdoor private space* are served, since these contexts have an overwhelming presence in drone applications. Hence, any impacts of drone use on outdoor physical mobility, informal social life and community cohesiveness, and the associated values of freedom, autonomy and sociality, can be expected to be of high ethical importance and need to be considered in efforts to improve the overall ethical acceptability of civil drone use.

From these findings, it appears that the civil use of surveillance-capable drones is, *in principle*, largely justified. Only the civil use of biomimetic drones is judged to be categorically unethical. In terms of applications, the justification of drones seems to be something of a mixed bag. This, however, is not to understate the severity of the ethical issues, which is very considerable at all levels of ethical analysis.

This study has had a number of limitations, some of which providing avenues for further research. Firstly, due to resource limitations, the futures research that has been conducted for this study is limited in its reliance on *interaction* and *creativity* as sources of knowledge. Additional futures methods that are focused on interaction and creativity could be employed to improve the accuracy and range of the predictions. Secondly, the categorization of surveillance-capable drones that is used in this study may be a little crude. In future analyses, it may be helpful to distinguish between more than three classes of surveillance-capable drones. Also, how to deal with drones that straddle two or more categories is an issue deserving further analysis. Thirdly, with respect to the ethical evaluation of civil drone *applications*, only a few scenario evaluations have been performed. Needless to say, these scenario evaluations are only the beginning of a comprehensive evaluative analysis of surveillance-capable civil drone applications in civil contexts. New applications should be evaluated in various different scenarios as soon as they start to emerge. Fourthly, the ethical conclusions that were reached in this analysis are not set in stone; it is important for the evaluations to be performed again at regular intervals (and perhaps with a little more detail in places where I took shortcuts) to account for new facts and insights. Such new facts could potentially be significant developments in terms of effective and efficient technical countermeasures against civil drones (i.e., methods for tracking and intercepting drones), which could ease some of the ethical concerns. Currently, the efforts in this area are very much in their infancy. Fifthly and finally, let me emphasize that since this study has concerned itself with ethical evaluations of an *emerging* technology, it has had, by necessity, a rather large speculative and subjective component. Nevertheless, even as others might see things differently, I believe my ethical evaluations contain some very important insights and could prove persuasive to a wide audience.

In the context of future work, let me also briefly draw attention to the significance of one particular topic that has been outside the scope of this study, namely, the potential weapons capabilities of civil drones. Such capabilities may have very serious ethical implications. Even the most basic of small surveillance-capable drones may prove a deadly force if they are fitted with explosives. (For other examples of the potential weapons capabilities of civil drones, see footnote no. 5 in the introduction chapter.) There is no doubt that a proper ethical analysis of potential weapons capabilities and applications would require an extensive study of its own.

Furthermore, let me emphasize that as civil drones will gradually become more autonomous, they will increasingly become subjects of study in the nascent field of *robot ethics*, where fundamental issues are studied relating to the ascription of moral responsibility in socio-technical contexts involving robots, and relating to the regulation of behavior of people and robots in these contexts. For example, weaponized police surveillance drones that autonomously decide on which individuals to target during a riot can be seen as taking decisions with very significant consequences—decisions which humans would consider value-based, ethical or moral in nature. If these drones have built-in self-learning systems to resolve moral dilemma-choices, then who would be morally responsible for the actions of these systems? What level of responsibility would be carried by the designers, the users (the police in this case), and perhaps even the drones themselves? In future analyses, issues like these should receive significantly more attention than I have given them in this study.

In addition to the ethical conclusions about the civil use of surveillance-capable drones, there are a few conclusions to be drawn about the methodology that was used in this analysis. Firstly, Philip Brey's (2012) anticipatory technology ethics (ATE) approach, with its three levels of ethical analysis, has proven very useful as an overarching methodology for this study, as it allowed for a very comprehensive ethical analysis of civil drone technology. I expanded the ATE approach by offering an extensive account of how to resolve value conflicts during an ethical evaluation, which has been lacking in the ATE approach. Importantly, I argued that, in a "balancing" process, assigning weight to benefits and harms on the basis of their relative *societal* importance is most useful at the artifact and technology levels of the ATE approach since at these levels we are often considering ethical impacts at a society-wide scale; and I argued that assigning weight to benefits and harms based on their effects on *contextual* goals and values is most useful at the application level since this is where the analysis often focuses on specific social contexts. I further expanded the ATE approach by presenting a method to determine the ethical permissibility of a technology or artifact. An interesting implication of this method is that the ATE approach's three levels of analysis cannot be kept completely separate when evaluating the ethical admissibility of a technology or artifact, for such an evaluation requires at least some knowledge of specific applications and the benefits and harms they present. All told, I believe both of these evaluative methods constitute useful conceptual additions to the ATE approach's evaluation stage of ethical analysis.

Let me also say a few things about the operational approaches to privacy that I have used in this analysis. First, I have found the *contextual integrity* approach by Helen Nissenbaum (2010) to be very helpful in conducting "micro-level" evaluations at the application level of the ethical analysis of drones. As I have argued repeatedly throughout this study, contextual factors (i.e., norms, goals, values and ends) are of instrumental importance at the application level. On the basis of my analysis, I would suggest that the decision heuristic of Nissenbaum's approach can be used successfully in comprehensive contextual ethical evaluations (*comprehensive* in the sense that the focus is not solely on evaluating privacy issues) of many

other emerging technologies that impact flows of personal information. Secondly, the pragmatic "seven types of privacy" approach by Finn, Wright & Friedewald (2013) has proven to be a very convenient checklist for quick and accurate identification of more general privacy issues. In my view, the types of privacy outlined in this approach should feature in any ethical checklist used to evaluate emerging technologies at the technology and artifact levels of ethical analysis. Finally, to both of these privacy approaches some minor improvements were made in the course of this analysis, the adoption of which I would like to encourage.

On the basis of all of the findings presented in this study, let me now conclude by offering a few brief governance recommendations, which I intend as a way to jumpstart a more comprehensive future discussion about the policy implications of surveillance-capable drone use in civil contexts.

- *Usage restrictions.* This study clearly implies that drones should be subject to strict regulations to ensure their ethical use. For example, the use of biomimetic spy drones should not be allowed in civil contexts, unless it is proven that there can be adequate safeguards against the threat of function creep. In addition, the use of WAPS drones for mass surveillance or observation purposes should be restricted to very special circumstances where the projected marginal benefits outweigh the significant marginal harms that are typically associated with WAPS drone use. It is necessary to conduct further assessments at the application level to determine the full range of permissible and impermissible civil uses of drones, or the *conditions* for civil drone use. Importantly, such conditions should not only pertain to drone use in the strictest sense, but also to the retention, sharing and use of personal data that have been acquired via drones—which in most cases should be severely restricted.
- *Ongoing ethical assessments.* As we have seen, drones are an emerging technology with a potential to raise serious ethical issues. We should therefore continuously keep track of important developments and their ethical implications. Investments in novel applications of surveillance-capable drones should not be made without clear, systematic (contextual) ethical evaluations, in which the impacts on outdoor physical mobility, informal social life and community cohesiveness are to receive special attention.
- *Democratic decision-making.* Moreover, since civil drone use is likely to affect a large percentage of the population, deployment and policy decisions surrounding (surveillance-capable) civil drones use should be decided democratically based on open information.
- *Oversight.* Independent audits should be put in place to track the use of surveillance-capable drones by public and private sector organizations, so that citizens and watchdog organizations can tell whether the rules are being followed.
- *Awareness.* Policy makers, developers, users, and citizens at large should be made aware of all the inherent issues with regard to drone technology and drone artifacts. This might help to mitigate the impact of these issues, as policy makers adapt their policies, as developers make adjustments to the technology, as users change the way they use their drones, and as the citizens are more mindful of how drone use can potentially affect them.
- *Transparency.* We have seen that many of the ethical issues of civil drone use result from a lack of transparency; the use of drone technology has an inherent tendency to be not very transparent. However, there may be ways to increase transparency. The policies and procedures for the use of drones by public and private sector organizations should be made public. And, ideally, citizens

should be provided with real-time information, perhaps though a web-based information system, on all drone activity that is currently being undertaken by organizations in their area—the owners of these drones, their capabilities, their purposes, et cetera. This requires that organizations make such data available. Of course, for some organizations, such as the law enforcement, it would legitimate to keep certain details of their drone operations confidential. Such measures to increase transparency could help to substantially reduce the impact of ethical issues such as the "chilling effect" and "function creep".

In my view, these recommendations represent but the beginning of a robust system of protections for all citizens. Even as much work remains to be done, I am confident that it is ultimately possible to integrate drones into society in responsible ways that allow us to truly benefit from all the good that drone technology has to offer.

References

ABC (2012). Drone films Polish police riots. *ABC*, February 21, 2012. http://www.abc.net.au/news/2012-02-21/drone-films-polish-riots/3840652

AFP (2014). Post startet Drohnen-Verbindung zur Nordsee-Insel Juist. *AFP*, September 24, 2014. https://de.nachrichten.yahoo.com/post-startet-drohnen-verbindung-nordsee-insel-juist-134738436.html

Airforce-technology.com (no date). Zephyr Solar-Powered HALE UAV, United Kingdom. http://www.airforce-technology.com/projects/zephyr

Anderson, C. (2014). Agricultural Drones: Relatively cheap drones with advanced sensors and imaging capabilities are giving farmers new ways to increase yields and reduce crop damage. *MIT Technology Review*. www.technologyreview.com/featuredstory/526491/agricultural-drones

Aquilina, K. (2010). Public security versus privacy in technology law: A balancing act? *Computer Law & Security Review*, Vol. 26, No. 2, pp. 130–143.

Barak, A. (2010). Proportionality and Principled Balancing. Law & Ethics of Human Rights, Vol. 4, No. 1, pp. 1–18.

BBC (2014). Flying drone inspired by swimming jellyfish. *BBC*, January 15, 2014. http://www.bbc.com/news/science-environment-25732293

Bennett, C.J., & Raab, C.D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge, MA: MIT Press.

Bentham, J. (1843). *The Works of Jeremy Bentham, vol. 4 (Panopticon, Constitution, Colonies, Codification)*, Liberty Fund, Inc. http://oll.libertyfund.org/titles/1925

Birnhack, M.D. (2011). A Quest for a Theory of Privacy: Context and Control. *Jurimetrics: The Journal of Law, Science, and Technology*, Vol. 51, No. 4.

Bishop, P., Hines, A., & Collins, T. (2007). The current state of scenario development: an overview of techniques. *Foresight*, No. 1, pp. 5–25.

Boenink, M., Swierstra, T., & Stemerding, D. (2010). Anticipating the Interaction between Technology and Morality: A Scenario Study of Experimenting with Humans in Bionanotechnology. *Studies in Ethics, Law, and Technology*, Vol. 4, No. 2.

Booth, W. (2011). More Predator drones fly U.S.-Mexico border. The Washington Post, December 21, 2011. http://www.washingtonpost.com/world/more-predator-drones-fly-us-mexico-border/2011/12/01/gIQANSZz8O_story.html

Bowcott, O., & Lewis, P. (2011). Attack of the drones. *The Guardian*, 16 January 2011. Retrieved on 22 May 2014, from http://www.guardian.co.uk/uk/2011/jan/16/dronesunmannedaircraft

Boyle, D. (2015). Strangeways prison smugglers crash drone delivering drugs and mobile phones. The Telegraph, November 9, 2015. http://www.telegraph.co.uk/news/uknews/law-and-order/11983257/Strangeways-prison-smugglers-crash-drone-at-HMP-Manchester.html

Brey, P.A.E. (2012). Anticipatory Ethics for Emerging Technologies. *Nanoethics*, Vol. 6, pp. 1–13.

Brown, M. (2012). Lockheed uses ground-based laser to recharge drone mid-flight. *Wired*, July 12, 2012. http://www.wired.co.uk/news/archive/2012-07/12/lockheed-lasers

Clarke, R. (1997). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. http://www.rogerclarke.com/DV/Intro.htm

Clarke, R. (2014). The Regulation of Civilian Drones' Applications to the Surveillance of People. http://www.rogerclarke.com/SOS/Drones-BP-140109.html

Corcoran, M. (2012). Drone journalism takes off. *ABC*, February 21, 2012. http://www.abc.net.au/news/2012-02-21/drone-journalism-takes-off/3840616

Cossairt, O.S., Miau, D., & Nayar, S.K. (2011). Gigapixel Computational Imaging. http://www1.cs.columbia.edu/CAVE/publications/pdfs/Cossairt_ICCP11.pdf

Cummings, R. (2015). Hillview man arrested for shooting down drone; cites right to privacy. WDRB.com, July 28, 2015. http://www.wdrb.com/story/29650818/hillview-man-arrested-for-shooting-down-drone-cites-right-to-privacy

Dictionary of Military and Associated Terms (no date). S.v. "persistent surveillance." http://www.thefreedictionary.com/persistent+surveillance

DiMascio, S. (2015). Drone legislation could ban all unmanned, RC aircrafts in Albany County. *News10.com*, December 8, 2015. http://news10.com/2015/12/08/drone-legislation-could-ban-all-unmanned-rc-aircrafts-in-albany-county

Dunlap, T. (2009). Comment: we've got our eyes on you: when surveillance by unmanned aircraft systems constitutes a Fourth amendment search. *South Texas Law Review*, Vol. 51, No. 1, pp. 173–204.

Durand, F., & Freeman, W.T. (2012). Video Magnification. http://people.csail.mit.edu/mrub/vidmag

Dworkin, G. (1988). *The Theory and Practice of Autonomy*. Cambridge, MA: Belknap Press of Harvard University Press.

Dworkin, R. (2006). It is absurd to calculate human rights according to a cost-benefit analysis. *The Guardian*, 24 May 2006. Retrieved on 5 July 2015, from http://www.guardian.co.uk/commentisfree/2006/may/24/comment.politics

Economist, The (2007). Unmanned aircraft: the fly's a spy. The Economist, 1 November 2007. Retrieved on 24 May 2014, from http://www.economist.com/node/10059596

European RPAS Steering Group (2013). Roadmap for safe RPAS integration into European Air System, Annex 3: A study on the societal impact of the integration of civil RPAS into the European Aviation System. http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap-annex-3_en.pdf

European Union (2000). Charter of Fundamental Rights of the European Union. *Official Journal of the European Communities.* Retrieved on 18 May 2014, from http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Evans, C. (2014). Paparazzi now using drones to hunt down and photograph stars. *CBS News*, August 23, 2014. http://www.cbsnews.com/news/paparazzi-take-to-the-skies-to-pursue-stars-with-drones

Farivar, C. (2014). The airborne panopticon: How plane-mounted cameras watch entire cities. *Ars Technica*, July 10, 2014. http://arstechnica.com/tech-policy/2014/07/a-tivo-for-crime-how-always-recording-airborne-cameras-watch-entire-cities/2

Federal Aviation Administration (2014). Fact Sheet – Unmanned Aircraft Systems (UAS). *Federal Aviation Administration*, January 6, 2014. http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153

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

Finn, R.L., Wright, D., & Friedewald, M. (2013). Seven Types of Privacy. In: S. Gutwirth et al. (Eds.), *European Data Protection: Coming of Age*, Dordrecht: Springer Science+Business Media.

Flock, E. (2012). Drone journalism, businesses and policing — the pilotless aircraft could soon fill U.S. skies. *Washington Post*, February 21, 2012. http://www.washingtonpost.com/blogs/blogpost/post/drone-journalism-businesses-and-policing--the-pilotless-aircraft-could-soon-fill-us-skies/2012/02/21/gIQAxB2gRR_blog.html?tid=sm_twitter_washingtonpost

Foucault, M. (1979). *Discipline and Punish: The Birth of the Prison*, New York: Vintage.

Fox, S. (2009). Hydrogen-Powered Navy UAV Shatters Flight Endurance Record. *Popular Science*, October 14, 2009. http://www.popsci.com/technology/article/2009-10/hydrogen-powered-navy-uav-shatters-flight-endurance-record

Fried, C. (1968). Privacy. *Yale Law Journal*, Vol. 77, No. 475.

Friedewald, S., Gutwirth, M., Wright, D., Mordini, E., et al. (2011). Legal, social, economic and ethical conceptualisations of privacy and data protection. PRESCIENT Deliverable 1. Karlsruhe: Fraunhofer Institute for Systems and Innovation Research.

Gao, J., Ling, H., Blasch, E., Pham, K., Wang, Z., & Chen, G. (2013). Pattern of life from WAMI objects tracking based on visual context-aware tracking and infusion network models. *Proceedings SPIE 8745*, *Signal Processing, Sensor Fusion, and Target Recognition XXII*, 87451K.

Geffray, E. (2013). Drones, innovations, vie privée et libertés individuelles. *La lettre innovation et prospective de la CNIL*, No. 6, p. 4.

Geradts, Z., & Sommer, P. (2006). D6.1: Forensic Implications of Identity Management Systems. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf

Goertzel, T. (no date). Methods and Approaches of Futures Studies. http://crab.rutgers.edu/~goertzel/futuristmethods.htm

Greenwood, F. (2014). Drones, The Civil Surveillance Equalizer? *sUAS News*, July 24, 2014. http://www.suasnews.com/2014/07/30184/drones-the-civic-surveillance-equalizer

Groff, L., & Smoker, P. (no date). Introduction to Futures Studies. http://www.csudh.edu/global_options/IntroFS.HTML#FSMethodols

Grossman, D. (1996). *On Killing: The Psychological Cost of Learning to Kill in War and Society*, London: Back Bay Books.

Heller, A. (2011). From Video to Knowledge. *Science & Technology Review*, April/May 2011. https://str.llnl.gov/AprMay11/vaidya.html

Hennigan, W.J. (2011). It's a bird! It's a spy! It's both. *Los Angeles Times*, February 17, 2011. http://articles.latimes.com/2011/feb/17/business/la-fi-hummingbird-drone-20110217

Hildebrandt, M., & Gutwirth, S. (2008). *Profiling the European Citizen: Cross Disciplinary Perspectives*. Dordrecht: Springer.

Horgan, J. (2013). The Drones Come Home. *National Geographic*, March 2013. http://ngm.nationalgeographic.com/2013/03/unmanned-flight/horgan-text

Hruska, J. (2013). Intel's former chief architect: Moore's law will be dead within a decade. *ExtremeTech*, August 30, 2013. http://www.extremetech.com/computing/165331-intels-former-chief-architect-moores-law-will-be-dead-within-a-decade

Hughes, B.M. (2015). FAA Aims to 'Seamlessly Integrate' Drones Into National Airspace; Industry Report: $82.1B Economic Benefit to U.S. *CNS News*, August 19, 2015. http://cnsnews.com/news/article/brittany-m-hughes/faa-aims-seamlessly-integrate-drones-national-airspace-industry

Iannotta, B. (2013). After Boston, new motivation for surveillance techies. *Deep Dive Intelligence*, April 22, 2013. http://www.deepdiveintel.com/2013/04/22/after-boston-new-motivation-for-surveillance-techies

Insinna, V. (2014). Start-Up Debuts Sense-and-Avoid System for Quadcopters. *National Defense*, July, 2014. http://www.nationaldefensemagazine.org/archive/2014/July/Pages/Start-UpDebutsSense-and-AvoidSystemForQuadcopters.aspx

Jay, S., & Crump, C. (2011). Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft. ACLU, December 2011. https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

Jenkins, D., & Vasigh, B. (2013). The Economic Impact of Unmanned Aircraft Systems Integration in the United States. https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf

Johnson, D. (2014). The Future of Drones in the Insurance Industry. *Insurance Journal*, March 7, 2014. http://www.insurancejournal.com/news/national/2014/03/07/322658.htm

Kanha Sar, R., & Al-Saggaf, Y. (2014). Contextual Integrity's Decision Heuristic and the Tracking by Social Network Sites. *Ethics and Information Technology*, Vol. 16, No. 1, pp. 15–26.

Kaspar, D.V.S. (2005). The Evolution (or Devolution) of Privacy. *Sociological Forum*, Vol. 20, No. 72.

Kelley, M.B. (2013). 'Bug-Sized' Drones Are The Most Frightening Type Of Killer Robot Yet. *Business Insider*, February 20, 2013. http://www.businessinsider.com/air-force-bug-sized-drones-are-scary-2013-2#ixzz3IY0nw9Ax

King, D.W., Bertapelle, A., & Moses, C. (2005). UAV failure rate criteria for equivalent level of safety. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.467.517&rep=rep1&type=pdf

Kopp, C. (2011). Impact or exponential growth laws in military systems. *Defence Today*, June 2011. http://www.ausairpower.net/PDF-A/DT-Moores-Law-Jun-2011.pdf

Lai, R. (2011). Festo's SmartBird robot takes off with elegance, doesn't poop on you. *Engadget*, March 25, 2011. http://www.engadget.com/2011/03/25/festos-smartbird-robot-takes-off-with-elegance-doesnt-fight-s

Lee, K. (2014). NYU Researchers Create a Super Light, Flying Jellyfish Drone that Flaps into the Air. *Inhabitat*, Januari 16, 2014. http://inhabitat.com/nyu-researchers-create-a-superlight-flying-jellyfish-drone-that-flaps-into-the-air

Levin, A. (2015). FAA: Small Drones Will Provide Significant Benefits. http://www.bloomberg.com/news/articles/2015-02-14/small-drones-to-provide-significant-benefits-faa-says

Lewis, P. (2010). CCTV in the sky: police plan to use military-style spy drones. *The Guardian*, 23 Jan 2010. Retrieved on 22 May 2014, from http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones.-

Lucivero, F., Swierstra, T., & Boenink, M. (2011). Assessing Expectations: Towards a Toolbox for an Ethics of Emerging Technologies. *Nanoethics*, Vol. 5, pp. 129–141.

Lyon, D. (2003). *Surveillance after September 11*, Cambridge: Polity Press.

Marx, G.T. (2002). What's new about the new surveillance?: classifying for change and continuity. *Surveillance & Society*, Vol. 1, No. 1, pp. 9–29.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, Vol. 6, No. 3, pp. 175–183.

McBride, P. (2009). Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations. *Journal of Air Law and Commerce*, Vol. 74, 2009.

McNeal, G.S. (2012). A Primer on Domestic Drones: Legal, Policy, and Privacy Implications. *Forbes*, April 10, 2012. http://www.forbes.com/sites/gregorymcneal/2012/04/10/a-primer-on-domestic-drones-and-privacy-implications

Merrill, J., & Troen, O. (2014). Drones are filling Britain's skies: Look up now to see what is looking back down at you. *Independent*, September 23, 2014. http://www.independent.co.uk/news/uk/home-news/drones-are-filling-the-skies-look-up-now-to-see-what-is-looking-back-down-at-you-9746459.html

Moskvitch, K. (2014). Are drones the next target for hackers? *BBC*, February 6, 2014. http://www.bbc.com/future/story/20140206-can-drones-be-hacked

Myers Morrison, C. (2013). Dr. Panopticon, or, How I Learned to Stop Worrying and Love the Drone. *Journal of Civil Rights and Economic Development*, forthcoming, 2014. Retrieved on 15 May 2014, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2319215

Nevins, J. (2011). Robocop: Drones at Home. *Boston Review*, January/February 2011, pp. 32-37.

Newell, P.B. (1995). Perspectives on Privacy. *Journal of Environmental Psychology*, Vol. 15, No. 2, pp. 87–104.

Nissenbaum, H. (1997). Toward an Approach to Privacy in Public: The Challenges of Information Technology. *Ethics and Behavior*, Vol. 7, No. 3, pp. 207–219.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, Vol. 17, pp. 559–596.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, Vol. 79, No. 1, pp. 119–158.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press.

Oremus, W. (2014). Google's Eyes in the Sky. Slate.com, 13 June 2014. Retrieved on 6 October 2015, from http://www.slate.com/articles/technology/technology/2014/06/google_skybox_titan_aerospace_acquisitions_why_it_needs_satellites_and_drones.html

Organisation for Economic Co-operation and Development (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://oecdprivacy.org

Palm, E., & Hansson, S.O. (2006). The case for ethical technology assessment (eTA). *Technological Forecasting and Social Change*, No. 73, pp. 543–558.

Patton, J.W. (2000). Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics and Information Technology*, Vol. 2 pp. 181–187.

Piore, A. (2014). Rise Of The Insect Drones. *Popular Science*, January 29, 2014. http://www.popsci.com/article/technology/rise-insect-drones

Popper, R. (2008). Foresight Methodology. In: Georghiou, L., Cassingena, J., Keenan, M., Miles, I. and Popper, R. (eds.), *The Handbook of Technology Foresight*, Cheltenham: Edward Elgar Publishing, pp. 44–88.

Qu, Y., Wang, T., & Zhu, Z. (2009). Remote audio/video acquisition for human signature detection. *Computer Vision and Pattern Recognition Workshops, 2009. CVPR Workshops 2009. IEEE Computer Society Conference on*, pp.66–71.

Reid, B. (2009). Coarse Gaze Estimation in Visual Surveillance. http://www.robots.ox.ac.uk/~lav/Research/Projects/2009bbenfold_headpose/project.html

Research Group of the Office of the Privacy Commissioner of Canada (2013). Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy? https://www.priv.gc.ca/information/research-recherche/2013/drones_201303_e.asp

Reuters (2013). AIRSHOW-Sky's the limit for civil drones. Reuters, 19 June 2013. Retrieved on 24 May 2014, from http://www.reuters.com/article/2013/06/19/air-show-drones-civilian-idUSL5N0EM1NJ20130619

Rosen, J. (2004). The Naked Crowd: Balancing Privacy and Security in an Age of Terror. *Arizona Law Review*, Vol. 46, No. 4, pp. 607–619.

Sánchez-Oro, J., Fernández-López, D., Cabido, R., Montemayor, A.S., & Pantrigo, J.J. (2013). Urban Traffic Surveillance in Smart Cities Using Radar Images. *Lecture Notes in Computer Science*, Vol. 7931, Chapter: Natural and Artificial Computation in Engineering and Medical Applications, pp. 296–305.

Schaper, D. (2015). Chicago City Council Approves Ban On Drones. *NPR*, November 19, 2015. http://www.npr.org/2015/11/19/456600405/chicago-city-council-approves-ban-on-drones

Schechter, E. (2013). Solar-Powered Drones' Bright Future. *Popular Mechanics*, August 13, 2013. http://www.popularmechanics.com/technology/aviation/solar-powered-drones-bright-future-15803525

Schwartz, P. (1991). *The Art of the Long View*, Chichester: John Wiley & Sons.

Science Learning (2014). Hi-tech drones copy nature's design. *Science Learning*, September 17, 2014. http://www.sciencelearn.org.nz/News-Events/Latest-News/Hi-tech-drones-copy-nature-s-design

Sengupta, S. (2013). U.S. Border Agency Allows Others to Use Its Drones. *The New York Times*, July 3, 2013. http://www.nytimes.com/2013/07/04/business/us-border-agency-is-a-frequent-lender-of-its-drones.html?pagewanted=all&_r=0

Shachtman, (2011). Army tracking plan: Drones that never forget a face. *Wired*, September 28, 2011. http://www.wired.com/2011/09/drones-never-forget-a-face

Singer, P.W. (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. Penguin Books.

Solove, D. (2008). *Understanding Privacy*, Cambridge: Harvard University Press.

Stahl, B., Heersmink, R., Goujon, P., Flick, C., Van den Hoven, J., & Wakunuma, K. (2010). Identifying the ethics of emerging information and communication technologies: an essay on issues, concepts and method. *International Journal of Technoethics*, Vol. 1, No. 4, pp. 20–38.

sUAS News (2013). UAV: fixed wing or rotary? sUAS News, September 24, 2013. http://www.suasnews.com/2013/09/25214/uav-fixed-wing-or-rotary

Surveillance Specialist Group (no date). Private Investigators Are Using Drones After Legal Ruling. https://ssgllc.org/private-investigators-using-drones-legal-ruling

Tavani, H.T. (2012). Defending a Context-Based Framework of Privacy [Book Review]. *IEEE Technology and Society Magazine*, Vol. 31, No. 4, pp. 7–11.

Thalen, M. (2013). Drones With Face Detection Cameras Obey Visual and Vocal Commands. *Infowars*, November 26, 2013. http://www.infowars.com/drones-with-face-detection-cameras-obey-visual-and-vocal-commands

The Quad Cops (2014). Quadcopter longest flight time. http://the-quad-cops.co.uk/quadcopter-longest-flight-time

Thomasnet.com (2013). Milipol 2013: Camero Launches Xaver(TM) AID - Airborne Imaging Drone - The First Unmanned VTOL Structure-Penetrating Life Detection System. http://news.thomasnet.com/companystory/milipol-2013-camero-launches-xaver-tm-aid-airborne-imaging-drone-the-first-unmanned-vtol-structure-penetrating-life-detection-system-20018062

Van den Hoven, J. (2001). Privacy and the Varieties of Informational Wrongdoing. In: R. A. Spinello & H. T. Tavani (Eds.), *Readings in CyberEthics*, Sudbury, MA: Jones and Bartlett Publishers, pp. 488–500.

Vásárhelyi, G., Virágh, C., Somorjai, G., et al. (2014). Outdoor flocking and formation flight with autonomous aerial robots. https://hal.elte.hu/flocking/export/6043/project/trunk/public/references/vasarhelyi/Vasarhelyi2014outdoor.pdf

Venier, S., Mordini, E., et al. (2010). *Deliverable 4: Final Report — A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies*. Karlsruhe: Fraunhofer Institute for Systems and Innovation Research.

Waldron, J. (2003). Security and Liberty: The Image of Balance. *The Journal of Political Philosophy*, Vol. 11, No. 2, pp. 191–210.

Walzer, M. (1984). *Spheres of Justice: A Defense of Pluralism and Equality*. New York: Basic Books.

Weiss, R. (2014). DHL Beats Amazon, Google to First Planned Drone Delivery. *Bloomberg*, September 25, 2014. http://www.bloomberg.com/news/2014-09-25/dhl-beats-amazon-google-to-first-scheduled-drone-delivery.html

Whitehead, J. W. (2010). Drones over America: tyranny at home. *The Rutherford Institute*, 28 June 2010. Retrieved on 10 May 2014, from http://www.rutherford.org/articles_db/commentary.asp?record_id¼661

Whitlock, C. (2014). When Drones Fall from the Sky. *Washington Post*, June 20, 2014. http://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky

Whitlock, C. (2015). FAA records detail hundreds of close calls between airplanes and drones. The Washington Post, August 20, 2015. https://www.washingtonpost.com/world/national-security/faa-records-detail-hundreds-of-close-calls-between-airplanes-and-drones/2015/08/20/5ef812ae-4737-11e5-846d-02792f854297_story.html

Williams, V. (2009). Memorandum by Dr Victoria Williams. *Surveillance: Citizens and the State - Constitution Committee.* Retrieved on 18 May 2014, from http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/8051402.htm

Wingfield, N., & Sengupta, S. (2012). Drones Set Sights on US Skies. *The New York Times*, February 18, 2012. http://www.cnbc.com/id/46439061

Woollacott, E. (2012). Gigapixel camera could revolutionize photography. *TG Daily*, June 21, 2012. http://www.tgdaily.com/hardware-features/64190-gigapixel-camera-could-revolutionize-photography

Zimmer, M. (2007). *The Quest for the Perfect Search Engine: Values, Technical Design, and the Flow of Personal Information in Spheres of Mobility*. Unpublished PhD diss., New York University.

Zorn, E. (2015). We must ban drones before it's too late. *Chicago Tribune*, February 27, 2015. http://www.chicagotribune.com/news/opinion/zorn/ct-drones-ban-chuy-garcia-rahm-emanuel-perspec-0302-jm-20150227-column.html

Appendix A – Questions for expert interview

At the end of 2014, I conducted an open-ended interview with a drone researcher at Netherlands Organization for Applied Scientific Research (TNO). The areas of expertise of this researcher were stated to include "unmanned systems, integration and C^{4}ISR" (Elands, 2014). The following questions were posed:

Interview on the potential future public surveillance and control capabilities and applications of drones

Name interviewee:

Areas of expertise of the interviewee:

Question 1:

What technical capabilities relevant to applications of domestic public surveillance and control do you think unmanned aerial systems will *potentially* have 20 years from now? Please explain in general terms for each of the following categories (a-f) what you think will be in the realm of the possible by the year 2035. Also, please try to distinguish in your answers, as you see fit, between *large drones* (weight > 50 kg), *medium-sized drones*, and *insect-sized drones*.

a. **Potential future sensor capabilities:** (Types of sensors, sensor resolution, through-wall imaging, etc)

   Response:

b. **Potential future audiovisual analysis capabilities:** (Moving-object detection and tracking over wide area ("persistics" data processing), facial and behavioral recognition, downlink data transfer rate, etc)

   Response:

c. **Potential future actuator capabilities:** (Crowd control, non-lethal incapacitation of targets, etc)

   Response:

d. **Potential future flight and stealth capabilities:** (Level of miniaturization, flight endurance, audibility (engine noise), visibility, etc)

   Response:

e. **Potential future autonomous decision-making capabilities:** (Autonomous flight navigation (including "sense and avoid" ability), coordination with other aircraft (swarm behavior), etc)

   Response:

f. **Other potential future capabilities worth mentioning:** (If any)

Response:

Question 2:

What applications of domestic public surveillance and/or control do you think unmanned aerial systems will *potentially* have 20 years from now? Please, explain for each of the following categories (a-c) what you think will be in the realm of the technically possible by the year 2035. Provide a brief description for each application that you mention.

a. **Potential future applications by governmental parties:** (Applications by, for example, police departments, national security agencies, taxation offices, and waste management offices)

Response:

b. **Potential future applications by commercial parties:** (Applications by, for example, advertising and marketing agencies, security companies, outdoor event organizers, private detectives, and insurance agencies)

Response:

c. **Potential future applications by private individuals:** (Applications by, for example, stalkers, hackers, and terrorists)

Response:

Appendix B – Drone capabilities and applications overview

The following table (Table 1) offers an overview of the capabilities and applications of the three categories surveillance-capable drones described in chapter 3.

	Large persistent surveillance drones	Small general-purpose drones	Biomimetic spy drones
Size of vehicle	- Medium to very large; weight more than 20 kg and often in excess of 1000 kg	- Small; weight usually between 2 and 20 kg	- Small to very small; weight in the order of kilograms for bird-like systems and grams for insect-like systems
Costs per system	- High to very high costs per system	- Very low to high costs per system, depending on capabilities	- Very low to high costs per system, depending on capabilities
Sensor capabilities	- Often extremely large coverage area, the size of an entire city - Mostly low level of detail (in terms of area per pixel) - Video sensors; audio, thermal, night vision, radar, and multi-/hyperspectral sensors may also be present	- Medium-sized coverage area, the size of a few city blocks - Often high level of detail (in terms of area per pixel) - Audio and video sensors; for high-end systems also thermal, night vision, and radar sensors	- Small coverage area - High level of detail (in terms of area per pixel), especially when close to target - Audio and video sensors
Analysis capabilities (including integration with other systems)	- Possibly onboard data analysis systems - Possibly automated tracking of large numbers of people - Possibly advanced behavioral recognition - Possibly pattern-of-life analysis	- Possibly automated facial recognition of everyone through links with biometric and social network databases - Possibly advanced behavioral recognition - Possibly Eulerian video magnification - Possibly Gaze direction identification	-
Flight capabilities	- Medium to very high altitude - Flight duration in the order of days - Large to very large range; tens or hundreds	- Low to medium altitude - Flight duration in the order of hours - Small to medium range; multiple kilometers	- Very low altitude - Flight duration less than an hour - Very small range; less than a kilometer

	of kilometers		
Stealth capabilities	- Sometimes noticeable; can be almost unnoticeable from the ground when at high altitude	- Can be almost unnoticeable when at large distance and hidden behind tree foliage or on rooftop	- Almost unnoticeable, even from up-close, due to being camouflaged as bird or insect
Autonomy	- Potentially a high degree of autonomy - Automatic take-off and landing - Automatic collision avoidance	- Potentially a high degree of autonomy - Automatic take-off and landing - Automatic collision avoidance	- Potentially a high degree of autonomy
Numbers in the skies	- Very low numbers flying in the skies	- Potentially large numbers in the skies	- Potentially large numbers in the skies
Public sector applications	- Border surveillance - Crime surveillance over urban areas - Criminal investigation in urban areas - Security monitoring of large crowds - Search and rescue - Emergency and disaster response	- Border surveillance - Traffic accident investigations - Criminal investigation in urban areas - Search and rescue - Tactical operations - Tax investigation - Environmental protection monitoring	- Criminal investigation in urban areas - Search and rescue - Tactical operations - Tax investigation - Environmental protection monitoring - Traffic monitoring
Private sector applications	- Security monitoring of large crowds - Photography and filmmaking - Industrial espionage	- Security monitoring - Infrastructure monitoring - Investigation by private investigators - Parcel and grocery delivery - Property damage evaluation by insurers - Photography and filmmaking - Industrial espionage - (Paparazzi) Journalism - Real estate advertising	- Workplace security monitoring - Private investigation - Inner-city courier services - Outdoor event documenting - Athlete tracking at sports events
Recreational and hobbyist applications	-	- Snooping on others - Amateur filmmaking - Amateur journalistic reporting - Drone usage through hacking	- Home security monitoring - Amateur photography and filmmaking - Citizen journalism - Advanced gaming

Table 1: Future capabilities and applications of the three drone categories

Appendix C – Drone application scenarios

For this study, I have created a set of eleven drone application scenarios revealing some of the important ethical issues of future drone applications. In chapter 6, I presented and evaluated four of these scenarios. In this appendix, the remaining seven scenarios are presented. Without a doubt, the scenarios presented here and in chapter 6 describe but a few of the many significant applications of surveillance-capable drones. However, I think that together they offer a decent impression of the wide range of ethically laden applications of surveillance-capable drones in civil contexts.

Scenario 1: "Smart" and pervasive public surveillance in urban centers

The first scenario demonstrates one possible future use of semi-autonomous swarms of small drones for the purpose of public surveillance by law enforcement agencies. It was built on the premise that national law enforcement agencies in many countries will continue the post-9/11 trend of building increasingly pervasive public surveillance systems. Small drones here are part of a large interconnected web of surveillance systems containing an array of different technologies.

> *In 2030, small police surveillance drones patrol the down-town areas of a big city in swarms. Linked to government databases containing photos and personal details, they sweep through the streets and identify many people instantly by their faces. At some point, an individual is spotted whose nervous loitering at a particular location combined with information on her criminal history triggers a red flag by the predictive behavioral analysis system. Alerted security analysts must now decide on appropriate action with regard to the individual. Since there are no grounds for an immediate arrest, a single drone is dispatched to preemptively follow and observe the individual. The individual is completely unaware of the fact that she is getting extra attention, since there are many drones in the sky and since the drone's powerful sensors allow it to keep a large distance. Her moves are recorded in great detail and automatically analyzed as she goes about her way in the city. After about an hour of uneventful observation, the targeted surveillance is stopped.*

Scenario 2: Targeted advertising by a mail order company

The second scenario explains how a small general-purpose drone might be used by a mail order company to make targeted offers to potential customers.

> *In 2030, a mail order company is using small drones equipped with cameras and GPS systems to film houses and gardens in several residential areas. The company assigns a profile to each home that includes information on whether there are likely to be children and pets in the household, whether the residents own a car (and what type), whether there is a swimming pool in the backyard, et cetera. This information is all gleaned from the drone footage, some of it automatically. The company uses the GPS data to match the footage with the addresses of the homes. This information is then used to send out discount offers on specific products the mail order company has in its inventory, such as children's playhouses, pet food, gardening equipment, et cetera.*

Scenario 3: A realtor's advertisement revealing neighborhood private property

The third scenario shows how a small general-purpose drone might be used by real estate agencies to make videos advertisements of client's houses, which also reveal the immediate surrounding neighborhood.

> *In 2030, a large real estate agency owns a fleet of camera-equipped drones which it uses to make appealing video advertisements of the houses it has for sale. An operator flies one of the drones above a house the company has for sale, filming the building, the land included with the sale and the surrounding neighborhood. In the footage, the right-side neighbors' playing children, their car, and their patio furniture are clearly visible, as is the left-side neighbor, who is bringing out the trash. A video containing the footage is featured on the realtor's popular website.*

Scenario 4: An architecture enthusiast peeping through high-level apartment windows

The fourth scenario illustrates how a small general-purpose drone might be used by an architecture enthusiast to film high-rise residential buildings, inadvertently (or not) capturing footage of peoples' private dwellings.

> *In 2030, an architecture enthusiast has purchased a camera-equipped drone to shoot footage of interesting architectural structures, including some famous high-rise residential buildings. The residents living at the highest floors of these buildings are used to having a high level of privacy in their homes, even if no curtains are covering their large panoramic windows. This is, of course, because it is normally quite difficult to peer through their windows from the ground below. Equipped with a drone, the architecture enthusiast does not experience this problem, however. She flies the drone close to residents' windows, ostensibly to capture footage of the building's marvelous architectural elements. What also ends up being recorded, however, is the interior spaces of unsuspecting people's residences. Unbeknownst to the residents, the architecture enthusiast places some of the drone footage with visible private interior spaces on her publicly accessible personal website.*

Scenario 5: Insect-like biomimetic drones at a political demonstration

The fifth scenario demonstrates the possible future use of biomimetic spy drones by the police for the purpose of monitoring and identifying political protesters. This scenario represents just one of the multiple highly significant surveillance-type applications of biomimetic drones.

> *In 2030, a number of insect-like spy drones have been dispatched to covertly monitor a deeply controversial political demonstration in the streets of a large city. The police's antiterrorism unit is looking to identify individuals who may be harboring ill intent. As some of these individuals are masked, they cannot be identified by facial recognition systems. The insect-like drones are therefore instructed to stealthily land on their targets and stay on them. The targeted individuals take no notice of the silent robotic creatures that are sitting on them. As these drones are equipped with GPS modules, the police are now able to track their targets as they are heading home after the demonstration has ended. The drones are sending back GPS coordinates in real-time. Upon arrival at what are presumed to be the residences of the persons of interest, the drones are instructed to leave their hosts and return to base.*

Scenario 6: Identifying neighborhood troublemakers

The sixth scenario shows how a bird-like biomimetic drone may be used neighborhood watch team to covertly investigate a group of teenage troublemakers.

> *In 2030, a local neighborhood watch team is seeking to identify and gather evidence against a group of teenagers who have been committing anti-social activities. It is using the services of a drone operator who specializes in covert surveillance. A bird-like biomimetic drone fitted with audio and video sensors and a GPS system is placed on a tree branch, from which a neighborhood playground frequented by the troublemakers can be overlooked. The drone records audio and video data of everyone in the vicinity of the playground. At some point, the troublemakers are sighted and the operator uses the drone to follow them around. Eventually, he is led to the home of one of them.*

Scenario 7: Criminals spying on the police

The seventh and final scenario shows how biomimetic drones (like small general-purpose drones) can democratize surveillance. Citizens may, for example, use them to spy on police forces. A negative consequence of this counter-surveillance, as put forth by Venier et al. (2010), is that it severely hinders the police's ability to catch criminals in the act.

> *In 2030, affordable insect-like biomimetic drones are available to anyone. Relaxation of aviation authority's rules regarding the private use of drones has resulted in an explosion in the numbers of these small aircraft flying in the skies. Ordinary citizens are primarily using the drones harmlessly to monitor and record their lives and activities. Other citizens, however, are using them for more sinister purposes. Some criminals have begun using insect-like drones to monitor police locations and activities. A notorious local crime syndicate, for example, uses them to monitor police activities, procedures and habits. One day, the police are about to execute a raid of the syndicate's headquarters. A SWAT team is assembling a few blocks away and preparing to move in. Unfortunately, however, they have been spotted by the syndicate's insect-like drones that are secretly patrolling the neighborhood. Alerted to the fact that the SWAT team is approaching, the syndicate's members remove important evidence of their crimes from the premises and subsequently flee the scene. Thus, the SWAT team's raid failed to yield any arrests or evidence against the syndicate.*