PRIVACY BY DESIGN: AN ASSESSMENT OF LAW ENFORCEMENT DRONES

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Communication, Culture, and Technology

By

Sara Anderson, B.A.

Washington, DC
April 15, 2014
ABSTRACT

The manner in which values such as privacy are impacted by drones in the hands of law enforcement agencies is concerning. As the domestic use of drones for law enforcement activities is increasing, it is important to address the privacy concerns that will inevitably arise before drones penetrate the airspace. This thesis will take an analytical, retrospective approach to the application of Privacy by Design to drones used by law enforcement. I draw on prior research in the field of Values in Design in order to identify how biases and values may be embedded in design in order to make assertions regarding the values apparent in drones. My method consisted of a case study, technical investigation, and discussion applying PbD principles to each drone. The case studies discussed at least one instance of that drone model’s use and provided context for the technical investigations, which focused on four aspects of the technology: (1) size, (2) data collection sensors, (3) autonomous capabilities, and (4) altitudinal and geographic restrictions. In the technical investigations, my analyses showed that all three UAS designs do not currently meet the standards the Privacy by Design principles, drawing on the information from my technical analyses to make these conclusions. Based on my analysis in this thesis, I propose the idea of a warrant verification system integrated into drone design to better preserve privacy without dramatically inhibiting performance.
All my thanks for your encouragement and amazing feedback to Meg Ambrose

Many thanks,
Sara R. Anderson
# Table of Contents

Introduction ....................................................................................................................................... 1  

**CHAPTER I - REVIEW OF RELATED LITERATURE** ........................................................................ 4  
Privacy as a Value ................................................................................................................................. 4  
Protecting Privacy as a Value ............................................................................................................... 9  
Privacy by Design ................................................................................................................................. 16  
Protecting Privacy from Drones ......................................................................................................... 21  
How Technologies Embody Values ..................................................................................................... 26  

**CHAPTER II - METHODS** ............................................................................................................. 31  
Computer Ethics .................................................................................................................................... 31  
Reflective Design .................................................................................................................................... 32  
Participatory Design ............................................................................................................................ 33  
Value-Sensitive Design ........................................................................................................................ 34  
Social Informatics ................................................................................................................................... 35  
Values in Design Applications ............................................................................................................. 36  
Technical Investigations ...................................................................................................................... 39  

**CHAPTER III - CASE STUDIES AND TECHNICAL INVESTIGATIONS** ..................................... 42  
Predictor B ........................................................................................................................................... 42  
Falcon .................................................................................................................................................... 46  
Aeryon Scout ......................................................................................................................................... 49  

**CHAPTER IV - DISCUSSION** ....................................................................................................... 54  
1. Proactive not Reactive, Preventative not Remedial ......................................................................... 54  
2. Privacy as the Default Setting ......................................................................................................... 56  
3. Privacy Embedded into Design ....................................................................................................... 57  
4. Full functionality – Positive Sum, not Zero Sum ........................................................................... 59  
5. End-to-end security – Full Lifecycle Protection .............................................................................. 60  
6. Visibility and Transparency – Keep it Open ................................................................................... 60  
7. Respect for User Privacy – Keep it User-Centric .......................................................................... 61  
A 4th am and Government Drone Use Legislation Based Design Assessment .............................. 61  

**CHAPTER V - CONCLUSION** ...................................................................................................... 64  

**BIBLIOGRAPHY** ........................................................................................................................... 67
INTRODUCTION

Drones, also called Unmanned Aerial Vehicles (UAVs), are poised to enter domestic airspace in waves over the next decade (Cavoukian, 2012, p. 3). The use of the Falcon UAV in Colorado for relief after a flood, drones for promotional videos, drones for agriculture, drones for security, Amazon delivery drones, and the increasing use of drones by domestic government agencies ranging from the Department of Justice to local law enforcement and disaster response (e.g. the Yosemite wildfire fight), are just a few examples (Ackerman, 2013; Danigelis, 2013). Drones have captured the attention of the public and spurred hotly contested debates over regulation.

Of particular concern is how values such as privacy are impacted by drones in the hands of law enforcement agencies. As the domestic use of drones for law enforcement activities is increasing, it is important to address the privacy concerns that will inevitably arise before drones penetrate the airspace. One way to evaluate how well a technology protects privacy is to assess how well it adheres to Privacy by Design (PbD) principles. Ann Cavoukian, Canada’s Information & Privacy Commissioner, developed this framework, consisting of seven principles, in order to “anticipate poor privacy practices and outcomes” (Cavoukian, 2012, p. 17). Generally, these principles are an add-on to other sets of principles, like Fair Information Practice Principles (FIPPs), and are applied to the practices of non-government entities to influence the incorporation of specific safeguards. This thesis will take an analytical, retrospective approach to the application of PbD to drones used by law enforcement, taking into account some prior non-governmental applications of PbD.
The use of drones has been expanding into law enforcement and other areas from their original military implementation. Cavoukian attributes this increased market to “the decreasing cost of UAV technology, and to the fact that UAVs have distinct functional advantages over manned vehicles” (Cavoukian, 2012, p. 3). This adoption has been gradual, primarily due to the hurdles in obtaining FAA licensing. However, Cavoukian claims that “Domestic demand is expected to increase over the next decade, starting with government organizations requiring surveillance systems similar to military UAVs, such as coast guards, border patrol organizations, and similar national security agencies,” and the issue of how best to address the potential for privacy violations is becoming more pertinent, as the 130 state laws proposed in 2013 alone, federal bill in Congress, and six FAA test sites exemplify (Cavoukian, 2012, p. 4).

However, legislating privacy preserving standards for drone use poses some unique difficulties, due in part to the varying capabilities and potential uses of the technology. While much of my focus is on the aircraft itself, I will refer to unmanned aerial systems (UASs) as well. Law enforcement uses a wide range of drones for different scenarios, and I take an example of three types of drones for my analysis.

The basis for the methodology and analysis of my research is Values in Design. I draw on prior research in this field that identifies how biases and values may be embedded in design in order to make assertions regarding the values apparent in drones. Privacy by Design provides a metric against which to measure the privacy relevant capabilities of the drones.

With law enforcement drones, the values embodied in the technology potentially conflicts with privacy. There is also a lack of transparency in drone surveillance. This is certainly not to say there are no benefits to using drones in law enforcement, however. I will analyze three
particular drone designs in order to assess the political nature of the design, what biases are evident from the design, and how privacy values will be implicated by the design when used for law enforcement. My analysis shows that when PbD principles are applied to law enforcement drones, many legislative entanglements and privacy violations can be avoided. Based on my analysis in this thesis, I will suggest how drone design can better preserve privacy without dramatically inhibiting performance.

The first chapter will be a review of relevant literature and describes where my work is located in the field of Values in Design. I begin by addressing privacy as a value and briefly discuss the law’s role in protecting that value, including the incorporation of privacy by design in policy. It will then discuss privacy issues and laws relevant to drones. Finally, it will discuss the concept of values in design.

Following this, Chapter II is a detailed description of the methods used in my analysis and how it differs from other ways to approach the problem of privacy in law enforcement drones. I then provide case studies and perform a technical analysis of the MQ-9 Predator B, Falcon, and Aeryon Scout in Chapter III. Included in the case studies are the ways in which drones have been used, are planned to be used, and could be used by a number of different law enforcement agencies in a wide variety of circumstances, highlighting the privacy concerns that arise from such use. I will focus on these four features: (1) size, (2) data collection sensors, (3) autonomous capabilities, and (4) altitudinal and geographic restrictions. Then, Chapter IV is a discussion assessing the embodied values of the technology using PbD as a standard against which to assess the technical characteristics of the drones. Chapter V is my conclusion, reiterating the purpose of this research and synthesizing the findings from my analyses.
CHAPTER I

REVIEW OF RELATED LITERATURE

Before analyzing the embodiment of Privacy by Design principles in law enforcement drones, this thesis will address several prior works across fields that will frame my analysis. In this chapter, I will expand on our current social perspective on privacy, including a very short history of the development of privacy as a societal value. This includes addressing how privacy may conflict with benefits such as technological capability, with a pluralistic theory of value providing the best perspective. Second, I will discuss protecting privacy as a societal value in the light of technological change. The third section lays out the general legislative background for privacy and the legislation history of drones specifically, providing a basis for how our society has historically protected privacy from drones. The fourth point addressed in this chapter is an expansion on the PbD principles as a viable framework for a detailed technical investigation of how values can be embedded in the design of law enforcement drones. I conclude this chapter with a discussion of how technologies can embody values, setting embodied values up as a tool for assessing privacy threats.

Privacy as a Value

A Pluralist Theory of Value

The history and evolution of privacy informs how the public responds to privacy incidents and provides a basis for understanding the way privacy is embodied in technologies. Elizabeth Anderson discusses a pluralist theory of value from a philosophical perspective in her book Value in Ethics and Economics. Her theory builds on Franz Brentano’s claim that intrinsic value is objective, and the idea that whether it is correct or incorrect to love something determines its
value. Anderson expands on this, claiming that the “variety of ways of caring about things is the source of pluralism in my theory of value” (Anderson, 1993, p. 5). She discusses the limitations of Kantian ethics and the drawbacks of a monistic theory of value, primarily its reductive nature, in her argument as well. The values embodied in law enforcement drones must be looked at in a pluralistic manner, since the value of privacy may conflict with the capabilities of the technology.

**The Liberal Theory of Information Privacy**

This thesis discusses privacy as a value through the lens of the liberal theory of information privacy. In their book, *The Governance of Privacy*, Colin Bennett and Charles Raab list four assumptions that are foundational to this theory:

- that privacy is an individual right;
- that privacy is something that we once had and is now eroding;
- that the source of the privacy problem is structural – the set of impersonal and remote forces that together contribute to the declining ability of individual agents to control the circulation of information that relates to them; and
- that the organizations that are responsible for privacy invasion can be observed, resisted and regulated because they are subject to a set of obligations that stem from principles as embodied in the laws of discrete and bounded liberal democratic statutes. (Bennett & Raab, 2003, p. 26)

These assumptions are consistent in the privacy and surveillance literature the authors reviewed. The sources they reference are international and fairly interdisciplinary, and they share a focus
on the “idea that advanced industrial societies are creeping inexorably toward an unacceptable level of surveillance” (Bennett & Raab, 2003, p. 24).

Helen Nissenbaum’s *Privacy in Context* also approaches privacy as a value from the perspective of the liberal theory of information privacy. Central to her argument is the claim that “Privacy is important because it protects the diversity of personal choices and actions, not because it protects the freedom to harm others and commit crimes” and that “Pursuit of lifestyles and life choices that run afoul of particular community mores are not only tolerated in liberal societies but, according to classic traditions, are potential sources of advancement and development” (Nissenbaum, 2010, p. 59). This argument relies on Ruth Gavison’s characterization of privacy as “a condition that is measured in terms of the degree of access others have to you through information, attention, and proximity” (Nissenbaum, 2010, p. 53).

Nissenbaum brings in philosopher Jeroen van den Hoven’s work to offer “moral reasons for why privacy deserves protection” (Nissenbaum, 2010, p. 61). These moral reasons fall into the following categories; (1) information-based harm, (2) informational inequality, (3) informational injustice, and (4) encroachment on moral autonomy (Van den Hoven, 1997). She also addresses Julie Cohen’s related concern over “the move to frame privacy as a form of property, and, consequently, a marketable commodity,” and her insistence that “privacy deserves a place alongside values such as equality and freedom, because, she argues, privacy is crucial for the development of moral autonomy” (Nissenbaum, 2010, p. 59). Nissenbaum contextualizes privacy as a value, incorporating many foundational ideas that add to her argument, in order to provide a framework for addressing privacy harms appropriately.
Types of Privacy Harms

Daniel Solove’s “A Taonomy of Privacy” provides a basis for evaluating privacy as a value by comparing the similarities between privacy harms that fall into a broad range of categories. Solove’s intention is for the taxonomy to demonstrate “that privacy disruptions are different from one another and yet share important similarities,” and it is also discusses “privacy in a more multidimensional way” (Solove, 2006, p. 558). He shows that some privacy harms that may seem unrelated actually have features in common with yet another type of privacy harm, and can be linked in a tertiary manner. He claims that, “It is no accident that various problems are referred to as privacy violations; they bear substantial similarities to each other” (Solove, 2006, p. 486).

Warren and Brandeis linked privacy as an incorporeal injury to intellectual property rights in their article, “The Right to Privacy,” stating that “From corporeal property arose the incorporeal rights issuing out of it; and then there opened the wide realm of intangible property” (Warren & Brandeis, 1890, p. 194). The authors focused primary on legal recourse to do with defamation, and put forward an argument that the law should apply to a broader category of injuries. Solove summarizes and builds on this argument, stating that, “There are other kinds of dignitary harm beyond reputational injury. These are the harms of incivility, lack of respect, or causing emotional angst” (Solove, 2006, p. 486).

Solove’s taxonomy transitions from Warren and Brandeis into his concept of “‘architectural problems’” (Solove, 2006, p. 387). He describes two primary issues that emerge through his analysis, the first being, “the enhancement of the risk that a harm will occur,” and the second is that “a particular activity can upset the balance of social or institutional power in
undesirable ways” (Solove, 2006, p. 487). The example Solove provides for the first issue is that “Activities involving a person’s information … might create a greater risk of that person being victimized by identity theft or fraud” (Solove, 2006, p. 487). For the second, he states that “a particular activity can upset the balance of social or institutional power in undesirable ways,” as in the case of “law enforcement officials having too much power, which can alter the way people engage in their activities” (Solove, 2006, p. 487). He ties these ideas into the theory of constitutive privacy, which he notes “has been further developed by Julie Cohen and Paul Schwartz, who both argue that privacy is a constitutive element of a civil society” (Solove, 2006, p. 488).

Within this framework, Solove identifies four groups of harmful activities from the most control the individual has to the least. They are, “(1) information collection, (2) information processing, (3) information dissemination, and (4) invasion” (Solove, 2006, p. 488). The privacy discussions surrounding law enforcement drones primarily fall into the information collection and invasion groups. The two types of information collection discussed in the taxonomy are surveillance and interrogation. Of the two, surveillance is more directly relevant to the capabilities of drones, but Solove makes interesting connections between the two types of collection. I will further discuss the policy implications of information collection harms in the Protecting Privacy as a Value section of this chapter.

Invasion harms, on the other hand, “differ from the harms of information collection, networking, and dissemination because they do not always involve information” (Solove, 2006, p. 549). The two types of invasion he discusses are intrusion and decisional interference (Solove, 2006, p. 549). This draws on the idea that “Protection against intrusion involves protecting the
individual from unwanted social invasions, affording people what Warren and Brandeis called ‘the right to be let alone’” (Solove, 2006, p. 550).

While aggregated data collected by drones may be a concern, it is not entirely dissimilar to examples of privacy harms due to information processing from internet tracking data or footage collected from a CCTV system. The general concern about these technologies is that, “When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected” (Solove, 2006, p. 507).

**Protecting Privacy as a Value**

Protecting privacy has its limitations in the legal system of the United States, due in part to the rapid development of technologies that can create privacy incidents. In my analysis, I will be focusing on privacy as a value from the perspective of the United States legal system. Solove’s “A Brief History of Information Privacy Law” details the development of international privacy legislation from colonial America to consumer privacy legislation in the mid 2000’s. Among other things, the chapter addresses early information privacy laws concerning things like census data confidentiality, opening of mail, telegraph security, and telephone wiretapping. While Solove’s overview transitions through the progress of financial privacy legislation and the development of federal privacy statutes over the course of the rise of the internet, my focus is less centered on broader legislative trends and more on specific legislation surrounding electronic surveillance and intelligence.
Fair Information Practice Principles

Most modern information laws and policies around the world draw on the Fair Information Practice Principles (FIPPs), which are also referred to as Fair Information Principles or Fair Information Practices (FIPs). “A Brief History of Information Privacy Law” discusses the development of these principles. Solove identifies the “increasing computerization of information and the burgeoning repositories of personal data in federal agencies” as part of the initiating issue for the development of these principles (Solove, 2006a, p. 25). He notes that, “In 1973, the United States Department of Health Education and Welfare (HEW) issued a report, ‘Records, Computers, and the Rights of Citizens,’ which analyzed these problems in depth” (Solove, 2006a, p. 25). The following are the Fair Information Practices recommended by the report:

• There must be no personal data record-keeping systems whose very existence is secret.

• There must be a way for an individual to find out what information about him is in a record and how it is used.

• There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

• There must be a way for an individual to correct or amend a record of identifiable information about him.

• Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data. (Solove, 2006a, pp. 25-6)
The Federal Trade Commission (FTC) also has a very similar set of FIPPS, and Solove notes that they have “been bringing actions against companies that violate their own privacy policies” since 1998 (Solove, 2006a, p. 39).

While this thesis focuses on US practices and policies, international principles reveal similarities between most FIPPs. Solove discusses some of these, mentioning the international forum provided by the Organization of Economic Cooperation and Development (OECD) and its contribution to a “substantial growth in information privacy law” through the creation of information privacy protection guidelines in 1980. He notes that, “The OECD Privacy Guidelines built upon the Fair Information Practices articulated by HEW in 1973” (Solove, 2006a, p. 35). The OECD Guidelines are comprised of the following eight principles:

(1) collection limitation—data should be collected lawfully with the individual’s consent;
(2) data quality—data should be relevant to a particular purpose and be accurate;
(3) purpose specification—the purpose for data collection should be stated at the time of the data collection and the use of the data should be limited to this purpose;
(4) use limitation—data should not be disclosed for different purposes without the consent of the individual;
(5) security safeguards—data should be protected by reasonable safeguards;
(6) openness principle—individuals should be informed about the practices and polices of those handling their personal information;
(7) individual participation—people should be able to learn about the data that an entity possesses about them and to rectify errors or problems in that data;
(8) accountability—the entities that control personal information should be held accountable for carrying out these principles. (Solove, 2006a, p. 35)

Much of the legislation I will discuss in this section of the literature review is based on principles like these that share many goals and properties. While FIPPs offers general principles to be followed by those that collect, manage, and process data, government access to and use of data is hindered by additional safeguards, including the Fourth Amendment and specific laws.

**Fourth Amendment and Surveillance Legislation**

Many of the laws regulating government access to and use of data fall into the category of surveillance legislation. Legislation in this category may apply to aural, visual, and electronic communications. Solove examines the progression of these laws in “A Brief History of Information Privacy.” One example is Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Solove, 2006a, p. 23). While Title III “extended the reach of wiretap regulations to state officials as well as to private parties,” it also had its limitations (Solove, 2006a, p. 23). It was limited in that it only “applied to the interception of ‘aural’ communications; it did not apply to visual surveillance or other forms of electronic communication” (Solove, 2006a, p. 23). Then, in 1986 Congress “expanded Title III to new forms of communications, with a particular focus on computers” with the Electronic Communications Privacy Act (ECPA), which “restricts the interception of transmitted communications” (Solove, 2006a, p. 34).

Some of the most important legislation discussed by Solove in the Proskauer on Privacy includes the 1966 Freedom of Information Act (FOIA), the Privacy Act of 1974, and the 2002 Homeland Security Act. He summarizes them as follows: “Under FOIA, ‘any person’ may request ‘records’ maintained by an executive agency;” the Privacy Act “requires agencies to
inform people of ‘the principal purpose or purposes for which the information is intended to be used’ when their information is collected;” and the Homeland Security Act “created the Department of Homeland Security (DHS), consisting of twenty-two federal agencies,” in addition to creating “a Privacy Office for ensuring compliance with privacy laws” (Solove, 2006a, p. 24, 519, 42).

One of the shortcomings of the Privacy Act is that it only applies to federal agencies, and does not regulate the private sector or local and state agencies (Solove, 2006a, p. 27). Its implementation under the 2002 E-Government Act is flexible as well, and it is under the authority Office of Management and Budget to give agencies guidance on said implementation (“Existing Federal Privacy Laws,” n.d.-a). The E-Government Act requires federal agencies to conduct privacy impact assessments (PIAs) as well, which, according to Warren et al.’s (2008) article should ideally:

(i) Conduct a prospective identification of privacy issues or risks before systems and programmes are put in place, or modified;

(ii) Assess the impacts in terms broader than those of legal compliance;

(iii) Be process rather than output oriented;

(iv) Be systematic. (“Existing Federal Privacy Laws,” n.d.-a; A. P. Warren et al., 2008)

Additionally, it “expands e-government initiatives in the executive branch,” and provides “privacy protections, such as prohibitions on the secondary disclosure of information obtained for statistical purposes” (“Existing Federal Privacy Laws,” n.d.-a).

Other legislation focuses on how data is stored and shared. The Intelligence Reform and Terrorism Prevention Act, passed by Congress in 2004, was intended to “facilitate greater
information sharing between federal agencies” by requiring “intelligence be ‘provided in its most shareable form’” (Solove, 2006a, p. 42). Solove addresses information storage and sharing in the Taxonomy as well. While government agencies have an investment in information sharing between them, Solove claims that they “might want to keep certain record systems pertaining to law enforcement or intelligence confidential so as not to tip off those who are being investigated” (Solove, 2006, p. 521). However, he also states that this “creates an architectural problem,” and that this type of “Exclusion reduces accountability on the part of government agencies and businesses that maintain records about individuals” (Solove, 2006, p. 521).

Congressman Ed Markey’s 2013 Drone Aircraft Privacy and Transparency Act encourages broad oversight for the use of commercial and law enforcement drones and the data they collect (Hans, 2013). The Act requires a “data collection statement” to be submitted to the FAA in order to be issued a drone operating license (Hans, 2013). This statement is to include “the name of the operator of the drone; where it will be operated; what data will be collected and how the data will be used and retained; and whether data will be sold to third parties” (Hans, 2013). It also regulates surveillance by requiring data minimization statements (Hans, 2013).

The fourth amendment can address privacy concerns relating to surveillance as well, providing limitations on the use of these technologies. However, the protections of the Fourth Amendment only go so far. Two examples of the significant alteration of existing statues include the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act’ (USA PATRIOT Act) of 2001 and the authorization of “warrantless electronic surveillance of American citizens” by the National Security Administration (NSA) that was authorized by Bush (Solove, 2006a, p. 43). The NSA’s efforts also weakened the
Computer Security Act of 1987, which gave the responsibility of keeping non-military government computer systems secure to the National Institute for Standards and Technology (NIST) for the protection of unclassified information military intelligence agencies would seek out ("Existing Federal Privacy Laws," n.d.-b).

The following examples of surveillance jurisprudence also cover what technological developments may be employed in data collection, e.g. Dow Chemical Co. v. United States, in which it was decided “that the government could not only fly over the petitioner’s property and observe it with the naked eye, but could also use a powerful aerial mapping camera that enabled the identification of objects as small as one-half inch in diameter” (Solove, 2006, p. 496). The case of Kyllo v. United States provides an example, in that “the Court concluded that the Fourth Amendment required a warrant in order to use a thermal-imaging device to detect heat patterns emanating from a person’s home” because, “though conducted outside the petitioner’s home, the surveillance was capturing information about activities within it: ‘We have said that the Fourth Amendment draws a firm line at the entrance of the house’” (Solove, 2006, p. 496). It additionally applied in U.S. v. Jones, in which the Court held that it was necessary to obtain a warrant before tracking Jones with a GPS planted on his car (Smith, 2012). This case set boundaries to protect privacy through the way the Court handled issues of privacy in public as well as what constitutes a search (Smith, 2012).

While there are many theories on the best way to update or otherwise alter legislation, Technological developments in surveillance, data collection, and data retention have largely informed opinions on privacy and its regulation, which have evolved significantly over time.
Privacy by Design

One of the foundational resources in PbD research is “Privacy and Drones: Unmanned Aerial Vehicles.” Ann Cavoukian, who conceived of PbD and advises on how the principles can be met, focuses on a general application of the principles to drones based on their current use and the privacy implications. She discusses the challenges to privacy protection presented by UAVs, “due to their ability to use a variety of sensors to gather information from unique vantage points – often for long periods and on a continuous basis” (Cavoukian, 2012, p. 2). The following are the seven principles of the Privacy by Design approach:

1. Proactive not Reactive, Preventative not Remedial;
2. Privacy as the Default Setting;
3. Privacy Embedded into Design;
4. Full functionality – Positive Sum, not Zero Sum;
5. End-to-end security – Full Lifecycle Protection;
6. Visibility and Transparency – Keep it Open; and

She recommends privacy impact assessments and other measures in addition to these principles. PbD principles line up rather nicely in most situations with the Federal Trade Commission’s (FTC) FIPPs. Aneta Podsiadla, a researcher who examines standards of privacy and security by design in robotics, compares US and EU laws and considers the Federal Trade Commission’s relation to PbD. Her claim is founded on being all inclusive of PbD principles and FIPPs. She states that, “In addition to these principles, in order to ensure Privacy by Design, companies are advised to implement Fair Information Practices… at every stage of data
processing from collection to deletion” (Podsiadla, 2013, p. 7). In general, PbD principles are meant to be integrated into the design process. They are employed iteratively with the intention of creating a product that preserves privacy in a wide variety of contexts. My analysis, on the other hand will be a technical investigation of deployed technologies, but still incorporates the principles of Privacy by Design. As such, I will describe how these principles have been applied by other researchers.

**Implementation**

Most authors discussing Privacy by Design describe what it means to apply the principles in a specific context. However, some concepts surrounding the implementation of the principles are fairly consistent across the board. Podsiadla identifies one of PbD’s goals, stating that, “In practice it means translating the legal obligations into programming language” (Podsiadla, 2013, p. 7). Lessig’s claim in “Code is Law” also goes to the point. Podsiadla quotes him as saying, “‘code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed’” (Podsiadla, 2013, p. 7).

In their article, Rubinstein and Good (2012) discuss the application of design principles based on Fair Information Practices. Google and Facebook are case studies, and the authors apply their ideas by making recommendations on how Google and Facebook could have applied PbD principles in specific instances to avoid certain privacy incidents. They describe the intent of their article as translating “privacy into design practices” (Rubinstein & Good, 2012, p. 16).

The principles have seen their intended use as a guideline for designing privacy preserving systems, however, and have not simply stayed a thought experiment. According to
Rubinstein and Good, “a few private sector firms have developed more detailed privacy guidelines, explaining how to integrate privacy into the several stages of the software development process (requirements, design, implementation, verification, and release)” (2012, p. 8). Their example is Microsoft’s 2006 publication of guidelines that “explores nine specific development scenarios and identifies over 120 required and recommend practices for creating notice and consent experiences, providing sufficient data security, maintaining data integrity, offering customers access to their data, and supplying other privacy controls (Rubinstein & Good, 2012, p. 8).

**Limitations**

Rubinstein and Good assert that “while FIPs underlie privacy by design, they are not self-executing. Rather, privacy by design requires the translation of FIPs into engineering and design principles and practices” (2012, p. 9). The authors identify some of the limitations of PbD as it is applied to the design process. They claim that, “As several European computer scientists recently concluded, the principles as written do not make it clear “what ‘privacy by design’ actually is and how it should be translated into engineering practices” (Rubinstein & Good, 2012, p. 7). They also suggest that “business concerns often compete with and overshadow privacy concerns” (Rubinstein & Good, 2012, p. 2).

Langheinrich describes another limitation in his paper, which is that, “In many cases, privacy is a latent concern, and hard to recognize without additional training or awareness” (Langheinrich, 2001, p. 33). I will be referencing Cavoukian’s principles in my analysis to describe the measure of privacy embodied in the drone designs, and the limitations of applying them may imply other values embodied in the technology that conflict with privacy.
Recommendations

Podsiadla specifically addresses the second, third, and fifth Privacy by Design principles in her paper, expanding on what focus should be taken when using them as a framework in the design process. Her recommended perspective for the second principle is that “privacy as the default setting means that privacy is built into a product in such a way that does not require any further action from the consumer” (Podsiadla, 2013, pp. 6-7). Additionally, she recommends that companies should focus on “data minimization related to narrowing purpose specification (collection, retention and use of data only for a specific purpose); mechanisms for data deidentification, and control mechanisms of data access, alteration, copying, and sharing” (Podsiadla, 2013, pp. 6-7).

In making recommendations for the third principle, Podsiadla asserts that “privacy embedded into design does not focus only on IT system architecture but also on the business operation that will implement privacy requirements” (Podsiadla, 2013, p. 7). Her practical recommendation for accomplishing that is, “the process of product development should integrate Privacy Impact Assessment, convert legal rules into technical solutions, and focus on education of staff and promotion of responsible engineering” (Podsiadla, 2013, p. 7). Similarly, Rubinstein and Good identify a potential response to the issue of needing better oversight and guidance for balancing privacy and the goals of business as “providing firms with much clearer guidance about applicable design principles and how best to incorporate them into their software development processes” (Rubinstein & Good, 2012, p. 2).

Discussing the fifth PbD principle, Podsiadla states that the “end-to-end security principle focuses on building in security in the whole lifecycle management of information” (Podsiadla,
She argues that “The measures to be adopted are: encryption by default, secure destruction and disposal of information, physical and digital security” (Podsiadla, 2013, p. 7).

Langheinrich’s ideas about security are that, first, “The important aspect to realize is that security might not be the panacea it appears to be, and it might not need to be that panacea either” (Langheinrich, 2001, p. 15). He suggests that, “If we consequently apply principles like proximity, locality, and proportionality, much of our basic infrastructure could indeed function without any explicit security model at all, while still adequately respecting the privacy needs of its users” (Langheinrich, 2001, p. 15).

Langheinrich presents a set of assessment criteria frequently raised in privacy discussions. They complement the Privacy by Design principles by providing specific issues to focus on when implementing them:

– **Feasibility**: what can technology achieve (or better: prevent)? All laws and legislation require enforceability. If privacy violations are not traceable, the much stressed point of accountability (as developed in the fair information practices) becomes moot.

– **Convenience**: the advantages of free flow of information outweighs the personal risks in most cases. Only highly sensitive information, like sexual orientation, religion, etc might be worth protecting. Semi-public information like shopping habits, preferences, contact information, even health information, might better be publicly known so that I can enjoy the best service and protection possible.

– **Communitarian**: personal privacy needs to be curbed for the greater good of society (trusting the government). Democratic societies may choose to appoint trusted entities to oversee certain private matters in order to improve life for the majority.
– **Egalitarian**: if everybody has access to the same information, it ceases to be a weapon in the hands of a few well-informed. Only when the watchers are being watched, all information they hold about me is equally worth the information I hold about them. Eventually, new forms of social interaction will evolve that are built upon these symmetrical information assets. (Langheinrich, 2001, pp. 5-6)

These points are primarily for the purposes of making recommendations about how to embody values in technology, but most can be adapted for the purpose of assessing embodied values. My technical investigation will essentially reverse engineer the implementation process to discover the embodied values in law enforcement drones based on the available system information and how the use of technologies with these attributes reflects privacy as a value. The PbD principles provide a solid basis for defining privacy as a value and protecting privacy as a value, and serve as a large part of the framework for my analysis.

**Protecting Privacy from Drones**

In the January 2013 Congressional Research Service Report, Legislative Attorneys Alissa Dolan and Richard Thompson offer information and advice to members and committees of Congress regarding legal issues implicated by drones. The Federal Aviation Administration (FAA) receives its timelines and priorities from Congress, but resolutions have not been established as of yet for some persistently unanswered legal concerns surrounding drone policy. Two overarching areas of concern are airspace ownership and invasion of privacy. As a potential baseline for drone legislation, current regulations on fixed wing aircraft and helicopters are discussed along with cases showing the trends in Court decisions. The potential benefits of drones are discussed as well, along with their capabilities and their potential for abuse.
Current regulation for drone operation states that the agency operating the drone “must obtain a certificate of authorization or waiver (COA) from the FAA” (Dolan & Thompson II, 2013, p. 3). Once this has been submitted, the FAA places limits on its operation based on an operational and technical review of the drone. This procedure may be eroding, however, as there has been pressure from Congress on the FAA to lighten restrictions of drone use and integrate the use of civilian unmanned aerial vehicles into national airspace. One way the FAA may be carrying out Congress’s instruction in this area is that there are no minimum altitude regulations for drones like there are for other types of aircraft. If regulation were to develop, the authors suggest basing the safe operating requirements on the size of the drone (larger drones regulated like fixed wing aircraft, smaller ones like helicopters).

The authors describe the history of technology and privacy starting with cameras that allowed instant shots instead of requiring the subject to pose. There was a law review published on the subject in 1890 formulating the legal theory of the right to be let alone. Balancing individual privacy with overarching social rights like freedom of the press poses a problem for the courts. Much of the privacy policy discussed is comprised of four rights that Dean William Prosser identified based on the case law surrounding the right to be let alone. Those are “(1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity which puts the target in a false light; and (4) appropriation of one’s likeness” (Dolan & Thompson II, 2013, p. 12).

Rules for enforcement of these rights would require a demonstrably “highly offensive” intrusion, repeated offense, intent, an objective standard of invasion of privacy that does not apply to idiosyncratic aversions, and some states require that “the intrusion must cause mental suffering, shame, or humiliation” (Dolan & Thompson II, 2013, pp. 12-13).
When drones are introduced into the privacy issue, their technological capabilities are the primary focus. They have “the ability to house high-powered cameras, infrared sensors, facial recognition technology, and license plate readers,” as well as thermal imaging (Dolan & Thompson II, 2013, p.10). The authors of the CRS report make the argument that, “while technology has increasingly shrunk other spheres of privacy in the digital age, the home is still accorded significant legal protection” (Dolan & Thompson II, 2013, p. 19). In a public space, privacy claims tend to be more difficult to uphold. The authors of the report recommended that Congress reconsider the principles proposed in the Privacy Protection Act of 1998 and the Personal Intrusion Act of 1998. Had those been passed, following someone to obtain their image would have been unlawful under a number if “the person had a reasonable expectation of privacy from such intrusion” or “the person feared death or bodily injury from being chased” (Dolan & Thompson II, 2013, p. 20). The variation in possible claims means liability would be determined by the particulars of each case. As regards public opinion on privacy and drone surveillance, the authors bring up the excellent point that “it is not clear, however, whether knowledge of being surveilled makes the monitoring more or less offensive” (Dolan & Thompson II, 2013, p. 19). A potential resolution presents itself in a bill introduced in the 112th Congress would “prohibit the FAA from issuing a license to operate a drone unless the application for such use included a ‘data collection statement’”(Dolan & Thompson II, 2013, p. 17). The statement would include as much information as possible to protect the privacy of the general public.

Ryan Calo also discusses privacy in relation to drones in his article “The Drone As Privacy Catalyst.” He suggests that drones may actually be visible enough to provoke more of a desire for privacy from the general population. He brings up that privacy violations are a bit
different in the context of current technology. With email lists being sold and shared and the
government connecting disparate bits of data about individuals, things aren’t always visible. Calo
also mentions the technological specifications of various drones with regards to their privacy
implications, stating that they can be equipped with “high-resolution cameras and
microphones,… thermal imaging and the capacity to intercept wireless communications” (Calo,
2011, p. 30). They can also easily be used to fly in patterns searching for suspicious activity, or
they can hover and perform surveillance.

Calo predicts that drones will become more and more prevalent because of their potential
use to police, firefighters, maintenance technicians, and physical scientists for a start. One reason
he claims drones are a privacy catalyst is that “privacy statutes tend to respond to specific
incidences or abuses,” and so legislation seems never to be caught up (Calo, 2011, p. 29).
However, drones may spur the type of incident that may pave the way for the laws to be
changed. He also suggests the idea of Privacy by Design, so that privacy standards aren’t slapped
on to the technology as an afterthought. His example is that “just as a dog might sniff packages
and alert an officer only in the presence of contraband, so might a drone scan for various
chemicals or heat signatures and alert an officer only upon spotting the telltale signs of drug
production” (Calo, 2011, p. 31). Privacy would be protected because the minimum intrusion is
enforced while keeping in mind the law.

In looking at drone legislation, it seems that legislation is really just beginning to be
implemented that will regulate drone use. In Allie Bohm’s (2013) *ACLU* article, “Drone
Legislation: What’s Being Proposed in the United States?” she claims that “the good news is that
the vast majority of the bills require a probable cause warrant in order for law enforcement to use
drones to collect information to use against someone in court” (Bohm, 2013). There is quite a bit of variation in the bills proposed and how far they got in the legislation process. Some points of legislative distinction are the weaponization of drones, “special protections from aerial surveillance for farmers or ranchers,” the requirement of “reporting on law enforcement agencies’ drone usage so the legislature can find out how drones work in practice,” and the requirement of “law enforcement to justify to their city councils or other local governing body their need for a drone before acquiring one” (Bohm, 2013). The states that adopt these legislations are listed in a table in the article. Some states are mentioned in particular for their legislation. The article specifies that “Georgia’s bill allows drone use only to investigate felonies—not misdemeanors and that Rhode Island’s… requires that incidentally collected data be deleted within 24 hours” (Bohm, 2013). Other states take completely the opposite approach and explicitly allow data to be kept and used in court. Additionally, “there are bills, like Montana’s, that prohibit private use of drones, or like Texas’s, that prohibit drone photography, raising First Amendment concerns” (Bohm, 2013).

In Cyrus Farivar’s arstechnica article, “DOJ calls for Drone Privacy Policy 7 years after FBI’s First Drone Launched,” he notes that the “steps to formulate a policy come seven years after the FBI launched its first drones… Right now, federal agencies essentially can make up their own standard operating procedures when it comes to drones and apply their own appropriate privacy policies as they see fit” (Farivar, 2013). While it seems likely that there will still be delays in legislation in the future, I see this push for privacy as one of many that may actually prompt representatives to take a stance on the issue. The more transparency there is
about the technical capabilities of law enforcement tools in particular, the more scrutiny will be placed on how they are used.

**How Technologies Embody Values**

Langdon Winner’s (1988) “Do Artifacts Have Politics?” discusses “good reasons to believe that technology is politically significant in its own right,” and describes the importance of assessing the “social circumstances of their development, deployment, and use” (p. 21). Winner presents a variety of examples of technologies and the biases that went into their design, creating a set of affordances, or features that allow for a specification. This theory of technological politics “suggests that we pay attention to the characteristics of technical objects and the meaning of those characteristics” instead of reducing “everything to the interplay of social forces” (Winner, 1988, p. 22).

Two ways technologies can display political properties are mentioned in the Chapter. The first is when the “invention, design, or arrangement of a specific technological device or system becomes a way of settling an issue in the affairs of a particular community,” and the second is what Winner describes as “‘inherently political technologies,’ man-made systems that appear to require or to be strongly compatible with particular kinds of political relationships” (Winner, 1988, p. 22).

According to the authors of “Embodying Values in Technology: Theory and Practice” Flanagan, Howe, and Nissenbaum (2008), Values in Design is a field in which the ideal is that “technologies promote not only instrumental values such as functional efficiency, safety, reliability, and ease of use, but also the substantive social, moral, and political values to which
societies and their peoples subscribe” (p. 322). The authors assign responsibility to designers, asserting that they should take these values into account.

Rubinstein and Good also discuss how specific design approaches can impact the embodiment of values in design. They state that “waterfall or similar top-down approaches are well suited for regulatory compliance (including security and privacy requirements), whereas most agile and lightweight development approaches tend to be more feature focused” (Rubinstein & Good, 2012, p. 18). The agile approach is characterized by “allows small teams to make changes very quickly and measures iterations in days or hours, not years or months” (Rubinstein & Good, 2012, p. 18). According to the authors, designers who use this process tend “to overlook security and privacy requirements at the outset and address them only over the course of several iterations, and sometimes neglect them entirely” (Rubinstein & Good, 2012, p. 18).

Rubinstein and Good describe the process of software design as an idea, and claim that “Through a series of brainstorming sessions, analysis of feedback, requirements and iterations, this idea achieves some concrete form, which depends on the user goals and the technical processes relied upon to realize them” (Rubinstein & Good, 2012, p. 16). They describe the early design stages as “lists of requirements, flow diagrams, wireframes and related concepts” (Rubinstein & Good, 2012, p. 16).

Friedman et al. provide a different view of values in design in their article. They claim that, “Value Sensitive Design is an interactional theory: values are viewed neither as inscribed into technology (an endogenous theory), nor as simply transmitted by social forces (an exogenous theory)” (Friedman, Kahn, Jr., & Born, 2006, p. 13). Instead, the interactional
position is context based, asserting that “while the features or properties that people design into
technologies more readily support certain values and hinder others, the technology’s actual use
depends on the goals of the people interacting with it” (Friedman, Kahn, Jr., & Born, 2006, p. 13).

Batya Friedman and Helen Nessenbaum provide another perspective for my research in
their discussion of types of biases and where they come from. They also look at how to identify
biases in systems, and suggest ways to minimize them in their article “Bias in Computer
Systems.” They discuss several types of biases, including preexisting bias, technical bias, and
emergent bias (Friedman & Nissenbaum, 1996, p. 333).

Preexisting biases generally “exist independently, and usually prior to the creation of the
system” (Friedman & Nissenbaum, 1996, p. 334). This type of bias has “roots in social
institutions, practices, and attitudes,” and may spring from individual bias, which “originates
from individuals who have significant input into the design of the system” (Friedman &
Nissenbaum, 1996, p. 334). The authors state that preexisting bias can be built into a system
consciously, but it can also be implicit and unintentional (Friedman & Nissenbaum, 1996, p. 334).

The authors describe technical bias as being based in “technical constraints or technical
considerations” (Friedman & Nissenbaum, 1996, p. 334). They discuss a variety of potential
manifestations, including limitations inherent in “Computer Tools,” “Decontextualized
Algorithms,” “Random Number Generation,” and the “Formalization of Human Constructs”
(Friedman & Nissenbaum, 1996, p. 334). They define the formalization of human constructs as
“Bias that originates from attempts to make human constructs such as discourse, judgments, or intuitions amenable to computers” (Friedman & Nissenbaum, 1996, p. 334).

Emergent bias is contextual, and “typically emerges some time after a design is completed, as a result of changing societal knowledge, population, or cultural values” (Friedman & Nissenbaum, 1996, p. 335). One of their examples being a change in the user base that would make the interface more difficult to use (Friedman & Nissenbaum, 1996, p. 335). In Clark, Wroclawski, Sollins, and Braden’s (2005) article, “Tussle in Cyberspace: Defining Tomorrow’s Internet,” the authors address the idea of designing with the idea of emergent biases in mind. They suggest designers make the choice “not to impose a rigid form to the design, but to design for choice at a later time, at run time” (p. 466). However, they acknowledge that “Providing this sort of choice has a drawback—it adds to the complexity of configuring and using a service” (Clark et al., 2005, p. 467).

Rubinstein and Good describe how values, the example being privacy, can be embodied in a technology. For example, “encrypting PII in transit and in storage and/or the use of anonymity services that delink users from all traces of their online activity, or of user-centric identity management systems that enable anonymous or pseudonymous credentials” (Rubinstein & Good, 2012, p. 24). They mention other ways technologies come to embody certain values through the design process as well, which provides a foundation for my analysis.

The values that are embodied in a technology can be assessed based on its capabilities, or conversely the intentionally imposed limitations on those capabilities. Langheinrich discusses how certain principles can be implemented by default by a technology. His examples are that,
given the proper protocols: limiting the number of communication hops any message can travel enforces locality; creating simple proximity behavior for personal devices prevents unwanted surveillance; and devising communication protocols that use temporary, random IDs can provide some base-line anonymity. (Langheinrich, 2001, p. 16)

For law enforcement drones there will definitely be different criteria for assessing the values embodied in the design. Among other things, it is vital to look at how they collect and transfer data to ascertain what values they embody as related to privacy.
CHAPTER II
METHODS

My analysis will build on the idea that values are embodied in technology through technical investigations, and will identify and assess these values. There are many approaches to values in design research, most of which overlap. I take parts from many of these methodologies to frame my analysis. The approaches I will address in this thesis include computer ethics, reflective design, participatory design, value sensitive design, and social informatics. The scope of this section is too narrow to give more than a brief overview of these, or even to include all approaches to values in design. In fact, many values in design researchers take an approach that hybridizes these fields. My approach falls most closely under the category of Social Informatics, but it is also a bit of a hybrid. After I describe how I will incorporate aspects of these fields in my analysis, I will address Rubinstein and Good as well as Shilton et al. as two examples of applied values in design research. Moving into my analysis, I will compile the relevant principles I use and describe what my technical investigation will entail.

Computer Ethics

James Moor’s (1985) influential definition of the computer ethics method is that “the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology” (Moor, 1985). Friedman and Kahn (2003) describe the goals of computer ethics in “Human Values, Ethics, and Design,” one of which is to “utilize existing moral theory to bring clarity to issues at hand, and at appropriate times – to proscribe norms of behavior,” and a second goal that “builds on the innovations of the technology itself” (p. 1183). The authors assert that, “The strength of this type
of philosophical contribution is that it helps translate moral abstractions into crisp working conceptualizations that HCI professionals can use,” and that computer ethicists focus on computer technologies because they are “interested in understanding how such innovations extend the boundaries of traditional ethical concepts” (Friedman & Kahn, Jr., 2003, p. 1183).

One important example of how these boundaries can be extended is that computer technologies posses what Moor calls “the invisibility factor” (Moor, 1985). He claims that because “Most of the time and under most conditions computer operations are invisible,” there are often “policy vacuums about how to use computer technology” (Moor, 1985). One kind of invisibility is “invisible abuse” (Moor, 1985). Using computers to perform surveillance falls into this category. Moor also discusses “invisible programming values” and “invisible complex calculation” (Moor, 1985).

**Reflective Design**

Reflective design as an approach to values in design, according to Sengers, Boehner, David, and Kaye (2005), relies on “critical reflection, or bringing unconscious aspects of experience to conscious awareness, thereby making them available for conscious choice” (p. 2). The authors claim that, “without it, we unthinkingly adopt attitudes, practices, values, and identities we might not consciously espouse” (Sengers, Boehner, David, & Kaye, 2005, p. 2). To address this, they create a “set of design principles and strategies that guide designers in rethinking dominant metaphors and values” in their paper, “Reflective Design” (Sengers et al., 2005, p. 9).

However, the authors are adamant that reflection be an iterative process and not an analysis of a preexisting technology. This thesis will take a different approach and address the
values embedded in law enforcement drones by analyzing their societal response through case studies as well as delineating their capabilities through an analysis of their technological specifications.

**Participatory Design**

Friedman and Kahn also discuss the development of Participatory Design in their paper. Strong Norwegian labor unions in the early 1970’s led to a national agreement that “entitled workers along with management to determine which technologies are introduced into the workplace,” and “fundamentally sought to integrate workers’ knowledge and a sense of work practice into the system design process” (Friedman & Kahn, Jr., 2003, p. 1186). The focus of the approach has primarily stayed on technologies in the workplace, and as noted by Flanagan et al., “has built a substantial body of theory as well as a record of application” (Flanagan et al., 2008, p. 330). The authors list the following five important methods that are associated with Participatory Design,

1. **Identifying Stakeholders**
2. **Workplace Ethnography**
3. **Future Workshops**
4. **User Participation in Design Teams**
5. **Mock-ups and Prototypes** (Friedman & Kahn, Jr., 2003, p. 1186).

All of these methods highlight a democratic element in the approach, and a focus on engagement throughout the course of the design process. Many other frameworks are related to Participatory Design, but put less of a focus on the workplace or don’t necessitate as much involvement over the entire course of the design process.
**Value-Sensitive Design**

Another approach, Value-Sensitive Design, was conceptualized by Batya Friedman, and features a “tripartite methodology, which involves conceptual, empirical, and technical investigations, employed iteratively” (Friedman, Kahn, P.H., & Borning, 2006, p. 3). The conceptual investigations entail posing questions such as,

- Who are the direct and indirect stakeholders affected by the design at hand? How are both classes of stakeholders affected? What values are implicated? How should we engage in trade-offs among competing values in the design, implementation, and use of information systems (e.g., autonomy vs. security, or anonymity vs. trust)? Should moral values (e.g., a right to privacy) have greater weight than, or even trump, non-moral values (e.g., aesthetic preferences)? (Friedman et al., 2006, p. 3)

Part of the basis of my analysis will involve conceptual investigations, but not to the extent of Value-Sensitive design, and will not include some of the same moral considerations.

The authors follow up with an explanation of the second part of their methodology, the empirical investigations. These typically follow conceptual investigations, and may include “observations, interviews, surveys, experimental manipulations, collection of relevant documents, and measurements of user behavior and human physiology” depending on the context (Friedman et al., 2006, p. 4). Some of the questions empirical investigations would focus on are, “How do stakeholders apprehend individual values in the interactive context? How do they prioritize competing values in design trade-offs?” and “How do they prioritize individual values and usability considerations?” (Friedman et al., 2006, p. 4). Another reason the authors include empirical investigations in their methodology is that they “are also often needed to
evaluate the success of a particular design” (Friedman et al., 2006, p. 4). This type of investigation is not present in my analysis, but is an important part of Value-Sensitive Design. I do, however, rely heavily on the third part of their methodology, the technical investigation. I will explain later in the chapter how I will make use of this method.

Social Informatics

My technical investigation of embodied values in design shares characteristics with the approach of Social Informatics, which, according to Batya Friedman and Peter H. Kahn, Jr. (2003), “has been successful in providing sociotechnical analyses of deployed technologies” (p. 1184). The proper definition the authors provide, the source being a National Science Foundation-sponsored workshop, is that “Social Informatics is the interdisciplinary study of the design, uses, and consequences of information technologies that takes into account their interaction with institutional and cultural contexts” (Friedman & Kahn, Jr., 2003, p. 1184). The approach has developed from an “emphasis on the social context of information technologies,” that the authors state has “appeared under many labels, including social analysis of computing, social impacts of computing, information systems, sociotechnical systems, and behavioral information systems” (Friedman & Kahn, Jr., 2003, p. 1184).

In response to assertions against the applicability of Social Informatics, “Human Values, Ethics, and Design” proposes that “Social Informatics can move in at least two directions,” one of which “leads to developing the sociotechnical analyses, and viewing this work as complimenting work in design (and other areas, such as Computer Ethics)” (Friedman & Kahn, Jr., 2003, p. 1185). This is the best way to describe the direction of my thesis. The authors mention another potential direction as well, which “leads to an expansion of Social Informatics
such that it fundamentally embraces design (and other areas) into its theoretical framework” (Friedman et al., 2006). However, this is a broader approach than I will take in my analysis.

**Values in Design Applications**

Here I give two examples of values in design research, one of which is a counterfactual analysis that makes use of these collective approaches and one which focuses more on the Participatory Design aspects of values studies.

**Counterfactual Assessment**

Rubinstein and Good’s method is to perform a counterfactual analysis of Google and Facebook privacy incidents and discuss how they may have been avoided. The authors approach the issue of values in design by presenting their own set of principles derived from FIPs and Ann Cavoukian’s Privacy by Design principles. However, they continue on to emphasize the execution of their principles by following through in design and engineering, claiming that “FIPs must be translated into principles of privacy engineering and usability” (Rubinstein & Good, 2012, p. 9).

One aspect of the method they used to approach the issue was “to review the relevant technical literature and distill the findings of computer scientists and usability experts” (Rubinstein & Good, 2012, pp. 9-10). They argue that because FIPs are “not self-executing,” that “privacy by design requires the translation of FIPs into engineering and design principles and practices” (Rubinstein & Good, 2012, p. 9). The authors then performed a counterfactual analysis of several specific privacy incidents as related to Google and Facebook and concluded that, “privacy engineering and usable privacy design were highly relevant to evaluating and
overcoming a range of privacy problems including emergent issues those affecting social networking services” (Rubinstein & Good, 2012, p. 72).

The steps they took in their analysis were to collect as much information as possible surrounding their chosen case studies in order to “have a reasonably clear idea of what happened as well as how and why the firms responded as they did (for example, by modifying certain features or even withdrawing a service entirely)” (Rubinstein & Good, 2012, p. 5). Following this, they state that they “need to identify a baseline set of design principles that will inform our discussion of alternative outcomes” (Rubinstein & Good, 2012, p. 5). While my analysis will not focus on offering alternative outcomes of the case studies I present, the way they structure their study, identify and explain the principles they reference, and analyze case studies provides a model for my approach.

**Participatory Approach**

In “How to See Values in Social Computing: Methods for Studying Values Dimensions,” Katie Shilton et al. identify the “struggle to specify whether privacy is a value of a person or group, a value intentionally embedded within a technology by designers, or a value materialized by a technology’s affordances through human interaction” as an issue in performing their analyses (Shilton, Koepfler, & Fleischmann, 2014, p. 1). However, even though social computing studies addressing privacy as it is designed into a system encounter these struggles, the authors create a framework that identifies the “dimensions” of a value by identifying the sources and attributes of values on a scale (Shilton et al., 2014). With these dimensions identified, the authors “illustrate how using the six dimensions can unpack values investigations in social computing” (Shilton et al., 2014, p. 3). They suggest that, “Researchers can look for the
values at their sources, examine attributes of values themselves, or both,” and offer as an example that “a social computing study on privacy could use these dimensions to specify whether privacy is an intended goal of a technology, a core value of an individual or group, or some combination of the two” (Shilton et al., 2014, p. 3).

The authors provide figures and descriptions of these dimensions, starting with the first source dimension, which “describes the Unit from which values are elicited, moving from values of an individual to a collective,” followed by the second, which “describes the Assemblage of the source, moving from values of homogenous to hybrid human and technological actors,” and the third, which “describes the Agency of a source, moving from object to subject” (Shilton et al., 2014, pp. 2-3).

With the source dimensions concluded, the authors move on to the attribute dimensions. The first of which, “Salience, is a continuum from peripheral to central values,” and this dimension “depends upon the source of the values” (Shilton et al., 2014, p. 3). The next attribute dimension is “Intention,” and it “describes the degree to which a designer or system intends to materialize a value on a continuum from accidental to purposive values” (Shilton et al., 2014, p. 3). The authors describe purposive values as “those intentionally built into a technology’s affordances and policies by its designers,” and accidental values as “unintentional features or biases embedded in a technological system” (Shilton et al., 2014). Lastly, the third attribute dimension, “Enactment, is the degree to which values are enacted within a sociotechnical system. The Enactment dimension highlights a continuum between potential and performed values” (Shilton et al., 2014, p. 3). These dimensions can be used in conjunction with many of the other methods listed by anyone from researchers to values advocates.
**Technical Investigations**

The primary method of analysis in this thesis will be a technical investigation of the embodied values in drones. This method features prominently in Value-Sensitive Design as a part of its tripartite methodology, and Friedman et al. describe its distinction from empirical investigations specifically by stating that, “Technical investigations focus on the technology itself. Empirical investigations focus on the individuals, groups, or larger social systems that configure, use, or are otherwise affected by the technology” (Friedman et al., 2006, p. 4). The authors note that technical investigations have two forms. The first form is that “technical investigations focus on how existing technological properties and underlying mechanisms support or hinder human values,” and the second is that they “involve the proactive design of systems to support values identified in the conceptual investigation” (Friedman et al., 2006, p. 4).

Friedman et al. also suggest heuristics for technical investigations, the first of which will be helpful for me to take into account in my analysis, while the last two apply more to their framework since they focus on the design process. Below I’ve listed excerpts of each of their bullet points.

- We have found it helpful to make explicit how a design trade-off maps onto a value conflict and differentially affects different groups of stakeholders.
- Unanticipated values and value conflicts often emerge after a system is developed and deployed. Thus, when possible, design flexibility into the underlying technical architecture so that it can be responsive to such emergent concerns.
We suggest that underlying protocols that release information should be able to be turned off (and in such a way that the stakeholders are confident they have been turned off).

(Friedman et al., 2006, p. 19)

**Technical Investigations of Values in Drone Design**

My technical investigation draws on the computer ethics approach because the drones I analyze, like computers, “provide us with new capabilities and these in turn give us new choices for action” (Moor, 1985). Even the “invisibility factor” focused on by Moor is related to drone technology, since drones can easily collect information without being seen (Moor, 1985). However, computer ethics focuses on “proposing conceptual frameworks for understanding ethical problems involving computer technology” (Moor, 1985). This thesis will not address overarching ethical issues in this manner, but present a retrospective analysis of drones for embodied values.

The following chapter will be devoted to case studies detailing the use of the three drone models by law enforcement agencies and a technical investigation of the features of the technology, and a discussion chapter will follow. I will touch on each principle, focusing more heavily on some than others. I will address the principles in the order Cavoukian presents them:

1. Proactive not Reactive, Preventative not Remedial;
2. Privacy as the Default Setting;
3. Privacy Embedded into Design;
4. Full functionality – Positive Sum, not Zero Sum;
5. End-to-end security – Full Lifecycle Protection;
6. Visibility and Transparency – Keep it Open; and

In addition, I will consider the technical aspects relevant to the 4th Amendment and legislation.

Following this section, Chapter III will feature case studies of the MQ-9 Predator B, Falcon, and Aeryon Scout, to further explicate not only what they are capable of, but the manner in which they are used by law enforcement agencies. The chapter also consists of technical investigations, focusing on four features. These include: (1) size, (2) data collection sensors, (3) autonomous capabilities, and (4) altitudinal and geographic restrictions. These features provide a consistent framework for me to break down and delineate the capabilities of each drone. My discussion in Chapter IV will draw on those features and assess the extent to which privacy is an embodied value in the drones by using PbD as a standard. I will address each principle individually and indentify to what extent the drone models reflect the intent of the principles focusing on the four feature categories above.
CHAPTER III

CASE STUDIES AND TECHNICAL INVESTIGATIONS

In this section, I will employ technical investigations to analyze the MQ-9 Predator B, Falcon, and Aeryon Scout drone designs in order to uncover and identify their embodied values. For each model, the case study will include an example of the drone’s use as reported from a variety of news sources. This will be followed by a delineation of its technical characteristics including size, data collection sensors, and autonomous capabilities, as well as its altitudinal and geographic restrictions. My analyses will expand on how each of these features implicates privacy by addressing each Privacy by Design principle in the discussion following this chapter.

Predator B

As reported by Brian Bennett of the LA Times, the MQ-9 Predator B was utilized in Nelson County, ND by Sheriff Kelly Janke and his department in an investigation surrounding six missing cows, each valued at $1,000. When officers followed up by obtaining a warrant to search the neighboring Brossart family farm, they were threatened off with rifles. The police department followed up by dispatching the Predator drone the following morning. Bennett notes that “sophisticated sensors under the nose helped pinpoint the three suspects and showed they were unarmed,” enabling the police to make “the first known arrests of U.S. citizens with help from a Predator” (B. Bennett, 2011). The specific features mentioned in the article that enabled the arrest are “live drone video and thermal images of Alex, Thomas and Jacob Brossart — and their mother, Susan,” which they watched both “on a hand-held device with a 4-inch screen,” and in the Sheriff’s office on a “password-protected government website called Big Pipe” (B. Bennett, 2011).
While drones most definitely have their place in law enforcement, Bennett quotes the head of the local police SWAT team Bill Macki as saying, “‘We don't use [drones] on every call out,’’ and that for callouts in town, ‘‘like an apartment complex, we don't call them’” (B. Bennett, 2011). The reason for this is not mentioned in the article, but it is an example of privacy protection in the form of policy as opposed to the value being inherent in the design. However, the baseline capabilities of the Predator B are worrisome to privacy advocates, who claim that “Predators are simply more effective than other planes” that may legally be used for surveillance, because while operating “out of earshot and out of sight, a Predator B can watch a target for 20 hours nonstop, far longer than any police helicopter or manned aircraft” (B. Bennett, 2011).

Related to the drone’s privacy implications, Bennett quotes Ryan Calo as stating that “‘Any time you have a tool like that in the hands of law enforcement that makes it easier to do surveillance, they will do more of it,’’ which privacy advocates take a step further, claiming that “drones help police snoop on citizens in ways that push current law to the breaking point” (B. Bennett, 2011).

Size

The size of the drone being used in law enforcement impacts its endurance, low altitude visibility, and payload capacity for data collection sensors. General Atomics publishes the features and capabilities of their designs, and the Predator B is stated to have “an endurance of over 27 hours, speeds of 240 KTAS, and has a 3,850 lb (1746 kg) payload capacity that includes 3,000 lb (1361 kg) of external stores” (“Predator® B UAS,” 2014). This is enabled by its “flight-certified and proven Honeywell TPE331-10 turboprop engine, integrated with Digital Electronic Engine Control (DEEC), which significantly improves engine performance and fuel efficiency, particularly at low altitudes” (“Predator® B UAS,” 2014).
Data Collection Sensors

The primary privacy concern surrounding drones is centered on how they collect, store, and transfer data. The LA Times reports that “Proponents say the high-resolution cameras, heat sensors and sophisticated radar on the border protection drones can help track criminal activity in the United States” (B. Bennett, 2011). Additionally, the payload of the Predator B is capable of carrying the following: “Electro-Optical/Infrared (EO/IR), Lynx® Multi-mode Radar, multi-mode maritime surveillance radar,” and Electronic Support Measures (ESM), which is primarily for the purpose of threat recognition (“Predator® B UAS,” 2014).

Autonomy

The Predator B can either be remotely piloted or fully autonomous, and is capable of featuring systems that make the drone semi-autonomous as well. According to General Atomics, “it is equipped with a fault-tolerant flight control system and triple redundant avionics system architecture,” and is “engineered to meet and exceed manned aircraft reliability standards” (“Predator® B UAS,” 2014). They also list that it is “C-130 transportable (or self-deploys),” and can be controlled via C-Band line-of-sight data link control or Ku-Band beyond line-of-sight/SATCOM data link control.

In a 2013 Gizmag article, Francis Govers wrote about the General Atomics Sense and Avoid (SAA) system prototype. He states that the system “allows a UAV to operate safely around other aircraft in flight” (Govers III, 2013). He reports that the drone “has successfully completed the first of several flight tests,” and that this prototype “marked the first time the entire system – consisting of a radar, transponder, and traffic alert system – worked together as a
‘system of systems’ to detect the various types of aircraft it might encounter in the air” (Govers III, 2013).

The parameters of the test included “40 pre-planned encounters with other air traffic, including some not being tracked by Air Traffic Control” (Govers III, 2013). The technology enabling this system “does not rely on optical detection, and would be able to operate in any weather” (Govers III, 2013). The whole system is comprised of “three integrated systems – the BAE Systems’ AD/DPX-7 Identification Friend-or-Foe (IFF) transponder with Automatic Dependent Surveillance – Broadcast (ADS-B) receiver; the GA-ASI-developed Due Regard Radar (DRR); and Honeywell’s TPA-100 Traffic Collision Avoidance System or TCAS” (Govers III, 2013).

The system is only partially autonomous, as the “onboard software fused the data into a single set of tracking information that was relayed to the Conflict Prediction and Display Systems (CPDS) in front of the Predator’s ground-based pilot” (Govers III, 2013). However, it is the system itself that is able to “track two participating ‘intruder’ aircraft that acted as targets for the exercise” using “its radar to see these targets” (Govers III, 2013). The system is able to interact with traditional aircraft that use “transponders to tell aircraft apart on radar as each aircraft has its own code that it responds to” and is generally utilized by the Traffic Collision Avoidance System (Govers III, 2013). However, due to possibility that modern aircraft may not have a traditional transponder, and may instead feature “a current-style radar transponder, or a new, modern ADS-B radio (or some combination thereof),” General Atomics designed their Sense and Avoid System to use “all three techniques to detect other aircraft” (Govers III, 2013).

Altitude and Geographic Restrictions
Not taking into account any regulations, the drone can operate at up to 50,000 feet (“Predator® B UAS,” 2014). Its ability to be pre-programmed for automated routes is not limited. Only policy regulation could prevent the Predator from entering certain restricted airspace. However, visibility affects the drone’s usefulness with regards to geography. For instance, the farmlands in ND provided an ideal environment for the use of the Predator B. The power source for the drone is “significantly improves engine performance and fuel efficiency, particularly at low altitudes,” making it more versatile than its predecessor, the MQ-1 Predator, an A-series drone (“Predator® B UAS,” 2014).

**Falcon**

The Falcon is a fixed wing UAV, but due to its size it has different capabilities and applications than the Predator B. This model has been adopted by the Mesa County Sheriff’s Department for use in investigations, search and rescue operations, and potentially for observation during wildfires (Mortimer, 2012). This specific model has received “an FAA Certificate of Authorization (COA) in conjunction with the Mesa County Sheriff’s Office (MCSO) for flight operations covering all 3300 square miles of the MCSO jurisdiction” (“Falcon UAV Information,” n.d.).

The creators of the drone, Falcon UAV, also volunteered its use during the flooding in Colorado in September 2013. However, as reported by Evan Ackerman for *IEEE Spectrum*, “Falcon (which was providing valuable services for free) was, for whatever reason, prevented from helping,” although they had already coordinated with Boulder Emergency Operations Center (EOC) to arrange the use of the drone (Ackerman, 2013). Ackerman explains that “there was a serious breakdown in communication somewhere along the line, although it's not entirely
clear whether it was between FEMA and Boulder EOC or Boulder EOC and Falcon” (Ackerman, 2013).

In this instance, law enforcement was potentially a part of the confusion. Ackerman states that “the Denver Post reported that it was a sheriff’s reserve volunteer that contacted Falcon UAV, telling them “‘to cease-and-desist by order of the sheriff and the incident commander,’” reportedly due to concern that the drone could interfere with other aircraft operations (Ackerman, 2013). However, Falcon pointed out that “they had already worked successfully with Boulder EOC on coordinating flights, and part of the point of using a drone is that drones can fly when and where manned aircraft cannot” (Ackerman, 2013).

Size

Due to its size, it is much easier to coordinate the launch of this drone and to transport it to its intended launch site. It does not require a rail launcher, and can be hand or bungee launched (“Falcon UAV Information,” n.d.). The drone weighs 9.0 lbs excluding payload (limited to 2-3 lbs), and can be transported in a backpack or ruggedized case (“Falcon UAV Information,” n.d.). Its flight endurance is 60-90 minutes at a speed of - 55 mph (22 - 49 knots), and its smaller size also lends to a lower maximum altitude than the Predator B (“Falcon UAV Information,” n.d.). The wing span of the Falcon is 96 inches, and it measures 50 inches long (“Falcon UAV Information,” n.d.).

Data Collection Sensors

The Falcon features the 10x zoom Sony block camera, kept horizontal to the drone with a pivoting support, as well as a thermal infrared camera, and its glider style design is intended to provide stability for “improved image quality versus foam flying wings” (“Falcon UAV Information,” n.d.).
Mapping,” n.d.). Its video range is 1 - 6 miles, and is link / antenna dependent. The primary application for this drone is surveying and mapping. Falcon advertises that their UAV “can cover map between 1-2 square miles to less than 1 inch pixel resolution,” primarily due to their Sony NEX 7 24.1 MP DSLR mapping payload (“Falcon UAV Mapping,” n.d.). Data processing is done after landing, when the “imagery is collected and processed using Photoscan” (“Falcon UAV Mapping,” n.d.). The drone’s images “may be outputted in any number of datums and formats,” which include “geo-rectified mosaics, digital elevation models, point clouds, 3D models, and Google Earth KMZ files among many others” (“Falcon UAV Mapping,” n.d.).

**Autonomy**

This UAV can be preprogrammed with GPS waypoints or be controlled manually with a stabilized joystick control. Gary Mortimer of *sUAS News* reported on Mesa County’s Falcon purchase, and stated that it “is most useful and efficient on autopilot, allowing its operators to type into a computer where they want the plane to fly” (Mortimer, 2012). Heather Benjamin, the sheriff’s spokesperson, was quoted as stating that, “You tell it where to go, and it will continuously fly over those parameters you set for it” (Mortimer, 2012). However, its endurance limits its autonomous use to an hour.

**Altitude and Geographic Restrictions**

There are no geographic restrictions by design on the Falcon, so any GPS coordinates can be input when it is flying autonomously, and there aren’t any restrictions for manual control either. The drone features “parachute recovery in rugged and constrained operations,” and so is able to operate over a broader variety of terrain. Mortimer reports that the Mesa County Sheriff’s department “also has a remotely controlled helicopter, but it costs more to fly, cannot stay aloft
as long and is more vulnerable to bad weather” (Mortimer, 2012). While the drone would be effective at night, the department only “has FAA permission to fly the drone anywhere in Mesa County in daylight hours” (Mortimer, 2012). It has an altitudinal range from 300 – 1500 ft, making it potentially very difficult to see depending on conditions (Mortimer, 2012).

**Aeryon Scout**

The Scout is a quadrotor UAV that Aeryon Labs promotes “as one of the most advanced vertical take-off and landing devices in the world” (“Halton Police Drone: High-Tech Surveillance,” 2013). Aeryon labs is based in Waterloo, and the Scout has been used by Halton Police in several investigations, one of which found “$744, 000 worth of marijuana growing in a Milton farmer’s field” (“Halton Police Drone: High-Tech Surveillance,” 2013). This case study is unique because the police use it focuses on is international, but my analysis will focus on the technological capabilities of the drone in this context and not offer an assessment of Canadian regulations.

Aeryon discusses the values embodied in the design of the Scout in asserting the usefulness of the system for law enforcement, and it is important that privacy is not mentioned. Their focus is primarily on “Having safety built into the system allows the operator to focus on the job of collecting the information at the scene” (“Considerations in Selecting a Small UAV for Police Operations,” 2014). According to Aeryon’s website, their drone contains integrated features that support safe operation. These include:

- The ability of the system to know when the power source is running low, inform the pilot, and if necessary fly home.
• Reporting when wind speed is excessive and the vehicle should return to the ground or the ability to set user imposed max range fencing in which the vehicle is allowed to fly. This reduces the pressure the pilot may feel to fly when he/she is unsure of the safety of the conditions.
• Not permitting the vehicle to fly if any of the onboard systems had detected a fault.
• Intelligent response if communication is lost between the aerial vehicle and the operator. (“Considerations in Selecting a Small UAV for Police Operations,” 2014).

**Size**

The Scout weighs just over a kilogram, or about 2.5 lbs, can be carried disassembled in a case and put back together relatively simply by snapping the rotors into the body of the drone (Guizzo, 2013). It is able to “accept custom payloads weighing up to 0.4kg to meet the specific requirements of customers” (“Aeryon Scout Micro-UAV, Canada,” n.d.). Its vertical takeoff and landing (VTOL) configuration in conjunction with its size impacts many aspects of its performance, e.g. its ability “to fly effectively in confined environments that are unapproachable by fixed-wing UAVs” (“Aeryon Scout Micro-UAV, Canada,” n.d.). Aeryon also recommends this system because “VTOL systems require limited space for take off and landing, some as little as 5 m², while providing improved control of take off and landings” (“Considerations in Selecting a Small UAV for Police Operations,” 2014). This stands in comparison to fixed wing systems which, while they are able to “fly for longer distances and duration, they require space for take-off and landing and must keep moving,” without the ability to hover over a specific location (“Considerations in Selecting a Small UAV for Police Operations,” 2014).
The small military grade UAV is able to “conduct safe flight operations in wind speeds of up to 50km/h and gusts up to 80km/h,” and is “capable of flying in different operating temperatures ranging from -30°C to +50°C” (“Aeryon Scout Micro-UAV, Canada,” n.d.). Its endurance is “up to 25 minutes with payloads in a normal environment,” and the drone is “equipped with an electric motor powered by a battery” (“Aeryon Scout Micro-UAV, Canada,” n.d.). The Scout can be operated up to a range of about 3 km (Robinet, 2013).

**Data Collection Sensors**

The Scout is able to support payloads including but not limited to, “electrochemical and infrared imaging gas and liquid detectors, radiation detectors, field communications, acoustic detection and location payloads” (“Aeryon Scout Micro-UAV, Canada,” n.d.). The integrated payloads of the Scout are the “Photo 3S - three-axis stabilised high resolution camera, VideoZoom 10x - ten times optical video zoom camera, and Thermal FLIR - thermal infrared video camera,” but are switchable for the other compatible sensors (“Aeryon Scout Micro-UAV, Canada,” n.d.). According to Aeryon’s website, two perks of systems that feature an integrated camera is that they allow for the tagging of metadata with the image or video stream, and that the geographical metadata taken allows for images to be stitched together into a larger, still detailed, picture of the area (“Considerations in Selecting a Small UAV for Police Operations,” 2014).

The Sout’s VTOL configuration also “ensures the collection of detailed imagery for precise modelling and measurement,” because the internally stabilised gimbals help to assure the camera’s focus on any given target (“Aeryon Scout Micro-UAV, Canada,” n.d.). While its ability to hover is helpful in image capturing, this drone is able to keep locked on to a target even while moving (Guizzo, 2013). As compared to satellites and manned aircraft, as well as other
alternatives, the Scout system is reported to collect more accurate aerial imagery, and do so in a more timely and cost-effective manner (“Aeryon Scout Micro-UAV, Canada,” n.d.).

The Scout’s collected information “is integrated with an end-to-end GIS (geographical information system) solution delivering a range of image processing options,” including not only high resolution 2D “orthomosaic” images and maps, but “Digital Elevation Model (DEM) data in three-dimensions and GIS datasets” as well (“Aeryon Scout Micro-UAV, Canada,” n.d.). To create 3D models, the system utilizes pix4D integrated GIS software (“Aeryon Scout Micro-UAV, Canada,” n.d.). This information can be, and generally is, recorded for later access. However, systems like this are leaning toward more interactive models. Currently, as is the norm,” high resolution imagery and other on-board data can be accessed online while the vehicle is in flight” (“Considerations in Selecting a Small UAV for Police Operations,” 2014).

**Autonomy**

The Scout can fly preprogrammed routes while recording or streaming live video, and it also features advanced fly-safe controls (“Aeryon Scout Micro-UAV, Canada,” n.d.). These routes are “fixed by the operator through the selection of way-points on the map” and are able to “be replaced with unplanned path by simply clicking on the map” (“Aeryon Scout Micro-UAV, Canada,” n.d.). Once these waypoints are selected, the drone can be instructed to “search a given grid, and return to the site of takeoff at the push of a button” (Robinet, 2013). Additionally, if the system battery begins to run low, loses communications, or encounters unsafe weather conditions, the automated return-home-and-land routine in employed (“Aeryon Scout Micro-UAV, Canada,” n.d.).
When the Aeryon Scout is controlled directly by ground personnel, they use a “tablet PC-based interface integrating a touchscreen device,” on which the operator can point to an area on the “touchscreen's map to direct the UAV to that specified location” (“Aeryon Scout Micro-UAV, Canada,” n.d.). The map-based control ensures that the Scout can be controlled “beyond the line-of-sight and in low visibility conditions,” allowing for “response teams to gather high resolution imagery during day and night in any situation” (“Aeryon Scout Micro-UAV, Canada,” n.d.). The system is intended to make the job of the controller as intuitive as possible, and is therefore different from “typical model remote control aircraft” (“Aeryon Scout Micro-UAV, Canada,” n.d.).

Altitude and Geographic Restrictions

The Aeryon Scout can “operate at lower altitudes and slower speeds than manned aircraft” due to its VTOL configuration (“Aeryon Scout Micro-UAV, Canada,” n.d.). This along with its size “allows the UAV to fly effectively in confined environments that are unapproachable by fixed-wing UAVs” (“Aeryon Scout Micro-UAV, Canada,” n.d.). The only geographic restrictions of the Scout are the safety restrictions and the 3km operating range, it is otherwise very versatile.
CHAPTER IV

DISCUSSION

This chapter presents each drone again, and assesses the technical characteristics discussed in the previous chapter using the Privacy by Design principles as a standard. There are many shared features and capabilities between the drones I discuss, but within each analysis I will focus on their unique aspects. I will conclude by suggesting ways in which these drones may better reflect PbD standards, returning to the law enforcement’s need for a warrant before flying a drone.

1. Proactive not Reactive, Preventative not Remedial

According to Cavoukian, in order to ensure privacy protection for UAVs comes before their deployment, “a necessary first step is to consider the usage limitations associated with these technologies” (Cavoukian, 2012, p. 18). She states that such a system should clearly state the “location of equipment, and the personnel authorized to operate the system and to access the equipment” (Cavoukian, 2012, p. 18). Geographic and time of day restrictions are features of a system that can be assessed to determine its adherence to this standard. How the system collects and stores data, as well as the use, should also be considered before its deployment (Cavoukian, 2012, p. 18).

Predator B

For the Predator B, these features are currently regulated by the agencies using them instead of being built into the system. The Nelson County, ND police use their discretion for when to operate the Predator. As mentioned in my case study, Sheriff Kelly Janke states that for callouts in town, “like an apartment complex, we don't call them” (B. Bennett, 2011). However,
it can be manually controlled or pre-programmed to fly anywhere, only limited by its size and policy restrictions. The altitudinal range of this drone, up to 50,000 feet, is regulated by policy as well (“Predator® B UAS,” 2014). Access to its data is restricted to authorized personnel primarily by policy, but the government website that receives the video data stream is password protected (B. Bennett, 2011).

**Falcon**

The Falcon’s use is regulated by legislation, and my case study for this drone model demonstrates that breakdown in communication between agencies and multiple interpretations of laws can easily happen. There aren’t technical limitations for the flight paths or data collection of the Falcon. Law enforcement agencies rely on regulations to determine when it is acceptable to fly the Falcon, like the FAA authorization to fly only during daylight hours (Mortimer, 2012). This drone is easier to transport and launch than the Predator, and the overall usage restrictions are less stringent.

The Falcon’s flexibility of use and quality data collection sensors does not make it proactively protective of privacy, although Falcon UAV does identify the most ideal uses for the system in a proactive manner. They include: Agriculture (Multispectral imaging options available); Oil and Gas; Mining; Pipeline Monitoring; Powerline Monitoring; Wildlife Management; County / City Planning; Real Estate / Development Planning; Disaster Response (Oil Spills / Flood Mapping / Fire Mapping); Insurance / Damage Assessment; Law Enforcement / Military mission planning; and Research/Academia (“Falcon UAV Mapping,” n.d.). While this occasionally involves identifying individuals, generally in a search and rescue capacity, the
images it usually generates are on a different scale looking for landslide volume loss, vegetation stress, or landfill volume and area ("Falcon UAV Mapping Samples," n.d.).

**Aeryon Scout**

The Scout is not a system that proactively protects privacy. Its integrated camera system allows image or video stream metadata to be tagged, and the image data it provides is very detailed. There are also no technical limitations on the routes it can take, and its size combined with its vertical take-off and landing configuration make it a very versatile drone for law enforcement. The map based controls are also more accessible than most, and feature a touch screen display.

**2. Privacy as the Default Setting**

Cavoukian classifies a system as maintaining privacy as a default if “No action is required” to protect privacy (Cavoukian, 2012, p. 18). The standards of this principle can be applied to a system’s data sensors, autonomous capabilities, and altitude and geographic restrictions. The size of the aircraft is also applicable in relation to altitude restrictions, since almost all drones can reach altitudes at which they would be very difficult to see and vary in endurance.

**Predator B**

Officials need to take actions to protect privacy when using the Predator B. Its cameras and other sensors collect incidental data, and it can be manually controlled or preprogrammed without GPS restrictions integrated into the system. The endurance of the Predator B also contributes to the need for regulation in order to protect privacy. Without the limitations of a
warrant, the Predator is capable of staying in flight for over 27 hours (“Predator® B UAS,” 2014).

**Falcon**

While the primary use of this drone is mapping, and its endurance is limited to an hour, the Falcon may also collect incidental data that is generally retained for months or years. The data processing is done after landing, however, and if this restricts access to the data collected to authorized personnel, the system could be considered to protect privacy by default. Overall, however, actions would need to be taken to protect privacy; it is not an embodied value in the system.

**Aeryon Scout**

The Scout does not protect privacy by default, so it’s left to legislation to regulate its use. The type and quality of the data it collects is an important factor in this assessment, as is the fairly across the board issue of data retention. However, the drone can only fly for 25 minutes at a time, which makes it less useful for some of the surveillance operations the Predator B or similar drones are used for.

3. **Privacy Embedded into Design**

This principle essentially requires an iterative design process, so that “privacy becomes an essential component of the core functionality being delivered” (Cavoukian, 2012, p. 18). It is related to the first principle, “Proactive not Reactive, Preventative not Remedial,” because embedding privacy in design requires consistent reflection on the features of the technology and their impacts (Cavoukian, 2012, p. 18). In this instance, I cannot extrapolate the details of the design process of these drones, but I will discuss what values they embody based on their
features and capabilities. When applied to drones, all of the features analyzed in my technical investigations are relevant, particularly the data collection sensors and the altitude and geographic restrictions.

**Predator B**

Privacy is not embedded into the design of the Predator B. The performance of the system shows reflection on other features during the design process. For instance, there is a focus on collecting high quality data, making the system easier to operate by automating things like the detection and avoidance of other aircraft, and general system performance in order to improve flight endurance and other features. This is not to say the design is not able to support privacy protection, the technology simply does not embody privacy as a value currently.

**Falcon**

The features of the Falcon demonstrate that a primary focus when designing the system was in collecting a broad variety of high quality image data that can be displayed in a variety of ways (“Falcon UAV Mapping,” n.d.). It was also intended to be easily transportable and launched more quickly and efficiently than something like the Predator B, while still being as resistant as possible to weather. Privacy is not embedded in this design, although the use has consistently been non invasive.

**Aeryon Scout**

Some of the primary design focuses of the Scout include having safety integrated into the system, promoting ease of use, and the quality of the data collected (“Considerations in Selecting a Small UAV for Police Operations,” 2014). Aeryon’s website also states that the Scout will not operate if it detects a fault in any system, and it informs the operator when its battery is running.
low or if wind speed is unsafe. The variety and quality of the data collection sensors, imaging processing options, and live video streaming without any technical restrictions shows that overall, the Scout does not have privacy embedded in the design. However, the site does identify a feature that allows the operator to impose a max range on the drone.

4. Full functionality – Positive Sum, not Zero Sum

Full functionality in this instance refers to the avoidance of unnecessary trade-offs and false dichotomies (Cavoukian, 2012, p. 19). The example Cavoukian gives is privacy vs. security, arguing that it is very possible to have both (Cavoukian, 2012, p. 19). This principle is particularly applicable to drones used by law enforcement, since privacy protection seems to conflict with their surveillance applications. I can’t speak to the designers’ conscious trade-offs, but if privacy protection is not present in the system and it instead appears to favor other features, I will identify the system as supporting a false dichotomy for the purpose of this analysis. The data collection sensors, autonomous capabilities, and altitude and geographic restrictions of drones are relevant features.

Predator B

The Predator B’s design supports a potentially unnecessary trade-off between privacy and overall performance. Its uses are only limited by legislation and departmental regulations, but the system itself does not protect privacy. Instead, as mentioned in the previous section, it appears that the intention is to provide the best data collection, ease of operation, and general system performance.

Falcon
The Falcon appears to need some adjustments to align with this principle. There don’t seem to have been any conscious trade-offs in the Flacon design, but there are a few aspects of its use that may conflict with privacy protection as a value. The drone is not ideal for surveillance because it is unable to hover, and it generally is not used in that capacity, but the system would be capable of collecting and storing data irrelevant to its mission.

**Aeryon Scout**

In the last section I discussed some of the features seemed to be a priority in the design, but that functionality does not need to be traded for privacy protection. They do present a few apparently conflicting goals, but if privacy were put forward as a goal, it is reasonable for the Scout to be used without sacrificing features. Aeryon expresses the values embodied in their UAV design when they list why the Scout would be idea for police operations, and privacy is not mentioned ("Considerations in Selecting a Small UAV for Police Operations," 2014).

5. **End-to-end security – Full Lifecycle Protection**

For a system to have end-to-end security, Cavoukian states that privacy needs extend “throughout the entire lifecycle of the data involved, from start to finish” (Cavoukian, 2012, p. 20). The management of the data drones collect is currently regulated by state legislation, which generally sets a time limit for the amount of time the data can be held (Bohm, 2013). The management of the data is comparable across different systems, and is not specifically related to any features analyzed in the previous chapter.

6. **Visibility and Transparency – Keep it Open**

A system can be considered transparent if it is “operating according to the stated promises and objectives, subject to independent verification” (Cavoukian, 2012, p. 20).
Providing visibility and transparency is also the sole responsibility of legislators, who generally decree that the public should be informed of when and where UAVs are operated in some manner (Kennedy, 2014). All of the features of a system discussed here should be made transparent, with most of the public’s focus centered on the data collection capabilities and any geographic restrictions.

Cavoukian suggests that this principle can be adhered to without building transparency into the system in a technical sense. As such, the information reported to the public would vary between the specific models analyzed, but the manner in which they would report the information would be consistent. This standard is currently being met by any drone model operated in a state with legislation that requires the law enforcement agencies to inform the public of drone use, like Utah’s “Government Use of Unmanned Aerial Vehicles Act,” SB167 (Kennedy, 2014).

7. Respect for User Privacy – Keep it User-Centric

This principle is fairly comprehensive of the overall idea of PbD. Cavoukian claims that a system can “keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options” (Cavoukian, 2012, p. 20). There aren’t specific features that support this principle among my presented case studies, and if this principle were applied to drone use its broadness would most likely make it applicable to many different models.

A 4th am and Government Drone Use Legislation Based Design Assessment

This Privacy by Design assessment has been very general, because a broad framework not only allowed me to analyze multiple distinct drone models, but is applicable to other
technologies as well. The analyses are meant to stand alone, and do not come with suggestions for how to make the technologies adhere to the PbD principles. This section ties back into the legislation overview I provided earlier, and is specific to drone design.

For privacy to actually be implicated by the design of these drones, their functionality would need to be limited so they could not exceed legal standards. However, the performance of the drones could easily suffer if functionality was cut across the board. I present one suggestion as to how drones can remain useful to law enforcement while enforcing the requirements of the warrant issued for its use. Additionally, I present a second recommendation for how from the Center for Democracy and Technology on how drone design can adhere to Markey’s 2013 Drone Aircraft Privacy and Transparency Act using outbound signals. These suggestions are meant to build off of analyses of designs that may be found not to protect privacy by providing a practical extension to the earlier discussion.

One way that the principles could be met is to require the system to verify that there is a valid warrant for its use. A warrant verification system could be achieved by requiring a theoretical warrant code before the drone could be operated. While most legislation requires a warrant for drone use already, unmanned aerial systems themselves are unable to enforce that at this time. If this were a requirement, only authorized personnel would be able to use them, and the verification system could include specific mission restrictions that would set parameters to meet and not exceed the needs of the warrant. For example, the warrant could specify GPS restrictions and altitude restrictions if applicable. If called for, there could be a limit on the amount of time the drone would be able to collect data as well. Data retention policies could also be enforced through this system.
This would apply the first principle, proactive not reactive, to drone design. It considers usage limitations and enforces them through the technology itself. If this were implemented, it would also apply the second principle, setting privacy as the default. Extra steps would not need to be taken to protect privacy. To implement something like this would embed privacy in the design as well. The drones would still be very useful to law enforcement agencies, and would not lose functionality. Warrant verification could support end-to-end security as well, by enforcing data retention policies. When the verification is input, the system could post an announcement that would be publicly accessible to comply with legislation requiring law enforcement agencies to provide information to the public about their use of drones, maintaining transparency. With all these principles applied, the seventh would also be met.

The Center for Democracy and Technology summarizes Markey’s 2013 Drone Aircraft Privacy and Transparency Act, as referenced in the Protecting Privacy as a Value section of my literature review, and makes suggestions of their own for how drones can embody privacy as a value. They argue that the bill should “explicitly require the FAA to require licensed drones that co-occupy manned aircraft airspace to broadcast what is referred to as an ‘automatic dependent surveillance-broadcast out’ (ADS-B Out) signal — including an identifier, location, altitude and velocity” (Hans, 2013). This is a reasonable and implementable suggestion, and can be tweaked to allow law enforcement drones to share this information as publicly as required by policy. This discussion contains ideas that engineers and software developers would have to investigate further for their viability.
CHAPTER V

CONCLUSION

The values embodied in drones have a strong impact on the level of surveillance that law enforcement agencies are able to perform (B. Bennett, 2011). As privacy concerns continue to be discussed by journalists as well as academics, it becomes more urgent to assess our society’s approach to drone surveillance. While legislation will continue to be an important way to regulate drone use, I have discussed approaches to regulation in this thesis that can be integrated with the technology.

This research is founded in Values in Design, and provided a review of the literature in the field that most closely related to my research. I chose defining privacy as a value, focusing on types of privacy harm, as a starting point that transitioned into a broader focus on protecting privacy with electronic surveillance legislation. I then expanded on Privacy by Design, and discussed it as way to protect privacy as a value by looking at others’ applications of the principles, the limitations presented in the literature, and any recommendations for improvement of the framework. Following this, more specific legislation was presented in protecting privacy from drones, which introduced some of the difficulties and features that applied later in my technical investigations and discussion. The chapter continued to discuss how it is that technologies come to embody values before offering a comparative analysis of methods for approaching Values in Design in Chapter II.

My research in Values in Design approached this topic by applying Cavoukian’s Privacy by Design principles in a retrospective analysis to three drones, one each from different classifications. My method consisted of a case study, technical investigation, and discussion
applying PbD principles to each drone. The case studies discussed at least one instance of that drone model’s use and provided context for the technical investigations, which focused on four aspects of the technology: (1) size, (2) data collection sensors, (3) autonomous capabilities, and (4) altitudinal and geographic restrictions. In the technical investigations, I delineated the features and various capabilities of the technology, highlighting the differences between the three drones. This allowed me to apply the PbD principles after breaking down what features of the drones implicated privacy.

In my discussion section I contextualized the principles for this analysis by stating which features are most applicable to each principle. I then discussed those features for each system, describing how the system’s performance compares to the standards of the principle. My analyses showed that all three UAS designs do not currently meet the standards the Privacy by Design principles, drawing on the information from my technical analyses to make these conclusions. Also, importantly, the discussion section breaks down why these drones do not meet the standards based on context of use as discussed in my case studies. This analysis was applicable to three categories of drones, and is a consistent, repeatable method. I concluded this chapter with a short section that suggests a warrant verification system that fits with the PbD principles, which enables the technology to enforce regulations and embody privacy as a value.

One limitation of this research centered around the available information on the drones I analyzed. I was able to locate enough information on each to flesh out this framework, but I would have been interested in finding more details about the data retention and automated features in particular. There could be potential for further research there, and the method I used could still apply. The method could
also be adapted to other technologies, embodied or web based. I would also be interested in expanding the method. My primary interest aside from the work I did would be participatory design.

Values in Design is a field that very often focuses, unsurprisingly, on the process of design and its iterative nature. My approach to this field was to bring together different aspects of the most prominent methods to assess a deployed technology with social relevance and focus on its technological capabilities.
BIBLIOGRAPHY


Falcon UAV Mapping Samples. (n.d.). *Falcon UAV*. Retrieved from Agriculture (Multispectral imaging options available)


Hans, G. S. (2013). Drone Privacy Bills Attempt to Protect Americans from Governmental,
from https://www.cdt.org/blogs/gs-hans/0804drone-privacy-bills-attempt-protect-
americans-governmental-commercial-surveillance

Retrieved from http://blog.tenthamendmentcenter.com/2014/04/utah-governor-signs-bill-to-
restrict-drone-use/#.U0I6mqhdWSo

http://link.springer.com/chapter/10.1007/3-540-45427-6_23

http://www.cs.ucdavis.edu/~rogaway/classes/188/spring06/papers/moor.html

Retrieved from http://www.suasnews.com/2012/01/11/259/mesa-county-police-purchase-
fixed-wing-suas/


Podsiadla, A. (2013). What Robotics Can Learn from the Contemporary Problems of
Information Technology Sector. Privacy by Design as a Product Safety Standard -
Compliance and Enforcement. In We Robot: Getting Down to Business (pp. 1–51).

asi.com/products/aircraft/predator_b.php

purchase-of-unmanned-aerial-vehicle-2

and Facebook Privacy Incidents. New York University School of Law Public Law & Legal

O. Bouvin, P. G. Krogh, & M. Kyng (Eds.), Proceedings of the 4th Decennial Conference
on Critical Computing: Between Sense and Sensibility (pp. 49–58). New York, NY: ACM.
Retrieved from http://dl.acm.org/citation.cfm?id=1094569


