These Aren't the Autonomous Drones You're Looking for: Investigating Privacy Concerns Through Concept Videos

Richmond Y. Wong, Deirdre K. Mulligan
School of Information, University of California, Berkeley

Regulators and privacy advocates increasingly demand that privacy be protected through the technical design of products and services, as well as through organizational procedures and policies. Privacy research by computer scientists and engineers are producing insights and techniques that empower a new professional in the technology sector—the privacy engineer. Despite great enthusiasm for this approach, there has been little effort to explore if and how this new direction in privacy protection is influencing the design of products. Understanding how design is being used to protect privacy requires analysis of sociotechnical systems, not de-contextualized technical artifacts. We analyze how privacy concerns in public policy debates about drones are raised and addressed in two concept videos from 2013 and 2015 developed by Amazon that depict fictional scenarios involving its future automated drone package delivery service. Drawing on design and communications methods we find that the concept videos reveal increased attention over time to privacy concerns. Our findings offer some evidence that privacy concerns are influencing Amazon's product and service design. Representations about the service offered in the 2015 video shape consumer expectations about how it addresses privacy concerns. While the videos reviewed do not represent an existing product, we discuss the shifting role such concept videos might play when Amazon's drone delivery service comes to market. As consumer facing representations of product functionality, concept videos, like other public statements, if misleading could form the basis of a deceptive statements claim by the Federal Trade Commission or state consumer protection agency. Finally, reflecting on our review, we suggest that concept videos are a useful tool for engaging regulators and other stakeholders in contextually specific considerations of when and how to enlist product and system design to protect privacy.

Keywords: privacy, drones, concept videos, privacy by design, design

Introduction

In December 2013, Amazon announced its desire to deliver packages to customers by automated drone through a service called Amazon Prime Air and released a concept video of footage showing what such a service might look like. Amazon released a second concept video in November 2015, offering an updated vision of the service. During the interim two year period, a vigorous public debate about the privacy risks posed by drones emerged in the U.S. This debate spurred multiple regulatory responses. The Federal Aviation Administration adopted a drone operator registration requirement, numerous states adopted laws prohibiting various drone uses

Authors retain copyright and grant the Journal of Human-Robot Interaction right of first publication with the work simultaneously licensed under a Creative Commons Attribution License that allows others to share the work with an acknowledgement of the work's authorship and initial publication in this journal.

Journal of Human-Robot Interaction, Vol. 5, No. 3, 2016, Pages 26-54, DOI 10.5898/JHRI.5.3.Wong

such as surreptitious surveillance of individuals, and the Department of Commerce convened a multi-stakeholder working group to develop voluntary drone operator best practices to address privacy concerns.

These piecemeal regulatory activities to address drone privacy issues occurred during a period when regulators globally were calling on companies to systematically integrate privacy into the design, engineering, and deployment of products, systems, and services. Understanding the potential privacy impact of Amazon's future drone delivery service requires attention to both the changing regulatory landscape and the affordances for (or against) privacy built into the drone delivery service. Efforts to push privacy into design will only succeed if privacy protective designs are acknowledged and accounted for in public debates about privacy protection.

Analyzing these concept videos we find some evidence that over time Amazon increasingly acknowledges and responds to privacy concerns animating public debate by presenting changes in the design of their drone delivery system. Given that the service has not yet launched, and only a subset of relevant privacy concerns are addressed within the videos, we cannot speculate on how well the ultimate service will address privacy. However, if the evolving approaches to privacy represented in the videos play out in practice, Amazon could address several privacy concerns through its design choices. The concept videos reviewed currently represent a fictional product; however, when Amazon's automated drone delivery service is available to the public, the videos take on new legal significance. Like television commercials, these videos may shape consumers' expectations about material aspects of the service—including privacy-related features. If the videos make misrepresentations about material privacy issues to the public they could provide the basis for a deceptive acts and practices action by the Federal Trade Commission or an action under similar state laws by a State Attorney General. We conclude with a reflection on the potential value of concept videos as a tool for engaging regulators and other stakeholders in deliberations about building privacy into product and system design.

The Drones and Privacy Discourse

The popular press and policy debates around drones have been rife with privacy concerns. Drones offer a physical manifestation of privacy violation in a way that other data collection technologies—on the internet, through embedded sensors, or through everyday financial and communication transactions—do not. Due at least in part to their physicality, drones appear to produce more emotional and visceral reactions from the public. These reactions are evident in phenomenal feats of self-help—with home owners literally shooting drones perceived to be privacy violators out of the sky like clay pigeons (Cummings, 2015; Goldman, 2014)[1]—public sentiment is in support of such extreme self-help measures (Reason-Rupe, 2013)[2], state bills are being introduced that would immunize such behavior (Okla. S.B. 492, 2015), and researchers are exploring similarly effective, if less violent, responses inspired by falcons and Super Heroes (Goodrich, 2016).[3] Some scholars have suggested that the physicality of drones may be a particularly potent "catalyst" for privacy reforms (Calo, 2011).

[1] For example, William Merideth shot down a drone he thought was capturing images of his 16-year-old daughter sunbathing. Subsequent to being arrested and charged with first-degree endangerment and criminal mischief charges, a Bullitt County District Court Judge dismissed all charges against Merideth. For a video of the court proceedings, see
http://www.wdrb.com/story/30354128/judge-dismisses-charges-for-man-who-shot-down-drone

[2] In this survey, 47% of respondents agree that they should have the right to destroy a drone flying over their property without permission.

[3] Goodrich describes a drone developed by an engineering professor that can net another drone from as far as 40 feet (12 meters) away, bag it up, and carry it away.

During the 2013–2015 period, policymakers responded to drone-related privacy concerns with a range of new laws and policy initiatives. During 2015 alone, forty-five states considered drone related bills. Twenty of those states adopted new laws (National Conference of State Legislatures, 2016). States also launched committees and commissions to study various drone-related concerns. While several bills were introduced in Congress,[4] none were adopted. The key federal actions during the period between the Amazon videos' release (2013–2015) were at the Federal Aviation Administration (FAA), which began allowing commercial unmanned aircraft vehicle (UAV) activities on a case-by-case basis under the existing regulatory framework and adopted a streamlined online registration requirement for small UAVs (sUAVs),[5] and the National Telecommunications and Information Administration (NTIA), which kicked-off a multi-stakeholder process aimed at developing best practices for privacy, accountability, and transparency issues regarding private unmanned aircraft systems (UAS).

In addition to drone specific privacy activities, the period between Amazon's videos (2013–2015) also saw increased interest in the concept of "privacy by design"—in brief, considering privacy concerns during the design phase of products and services, and embedding privacy in technical and organizational measures—as to proactively address privacy concerns (Rubinstein, 2012). Building on a long line of academic research showing both that social values are embedded in technology, and that the creation of artifacts or the making of technical decisions have social effects—both intended and unintended (e.g., Cranor & Reagle, 1997; Friedman & Nissenbaum, 1996; Latour, 1992; Winner, 1980)—the privacy community at large has sought to encourage technical designs that express and protect privacy. Technical decisions can regulate (using the term in a broad sense) in combination with other forces, such as law, social norms, and markets (Lessig, 2006). Just as automobile speeds can be regulated by distinct combinations of these modalities—a policeman can enforce speed limits, a speed limit sign can be posted, a speedbump can be built into the road, or a vehicle can be built so that it cannot go over a certain speed (Latour, 1992)—so too can privacy. For example, one can rely on legal rules and courts to limit government access to private communications, or one can rely on encryption systems in which individuals control access to their own keys. The choice of modalities influences how strictly something is enforced, at times collapsing policy and enforcement, eliminating the violability of the rules (Surden, 2007), as well as the relatively capacity for the exercise of discretion: For example, the policeman can choose whether or not to stop a speeding motorist, a speed bump causes nearly everyone to choose between slowing down or damaging their vehicle, and a car incapable of exceeding the speed limit simply makes speeding impossible.[6] Scholars in the human-robot interaction (HRI) community emphasize privacy, among other values, as an important benchmark in creating humanlike robots (Kahn, Ishiguro, Friedman, & Kanda, 2006). Other HRI research tacitly acknowledges the ways technical design and algorithms may encode values, such as the privacy implications of using robots to conduct gender recognition (Ramey & Salichs, 2014) or studying video manipulation techniques to obscure images and preserve privacy in robotic systems (Hubers et al., 2015). Technology is already in use to address privacy and other issues related to drone use. For example, NoFlyZone[7] maintains a database that drone operators can use to avoid flying over or collecting data around specific areas—in effect creating a "geo-fence." Advocates have recommended that drones broadcast a signal identifying themselves to those below—a digital "license plate" (Hall, 2013).

[4] For example, companion bills focused on privacy were introduced in the House and Senate: H.R. 1229 Drone Aircraft Privacy and Transparency Act of 2015; and, S. 635: Drone Aircraft Privacy and Transparency Act of 2015 on March 3, 2015.

[5] Those weighing less than 55 pounds and more than 0.55 pounds.

[6] Of course different vehicles are differently at risk of damage from speeding over speed bumps, and technical skill may make circumventing the speed regulator in the automobile a self-help possibility for some portion of the population.

[7] See https://www.noflyzone.org

During 2013–2015, regulators in particular intensified the pressure on the private sector to use the distinct attributes of code and technical systems to harden privacy's protection. This highlights the growing recognition, particularly among policymakers, of the power of technology to not only implement, but also to settle policy through architecture, configuration, interfaces, and default settings (Mulligan & King, 2012). While domestic legislation requiring federal agencies to systematically attend to privacy within the design and use of technical systems was adopted in the U.S. in 2002[8], and privacy by design became a consensus policy position of data protection regulators in 2010[9], a range of policy activities escalated the focus on privacy by design during the relevant period. The Obama Administration's *Consumer Data Privacy Framework and Bill of Rights* issued in 2012, the Federal Trade Commission's (FTC) *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* issued in 2012, and the European Union's General Data Protection Regulation,[10] which was under debate during the 2013–2015 time period, all require organizations to take privacy into account in the design and deployment of technical systems. This period also saw FTC enforcement actions against companies for privacy harms caused by technical design choices.[11]

Accounting for (Privacy by) Design

Against this background, Amazon's concept videos invite viewers to step into "the not too distant future" and imagine using the automated drone delivery service. The videos are discursive objects, engaging the broader policy discourse surrounding privacy and drones. The focus on the role of *design* in addressing privacy motivated our examination of Amazon's *portrayal* of their Prime Air service. While laws and technical design can express and enforce values related to privacy, *representations and depictions* of technologies can convey the values—or at least a take on them—of a sociotechnical system. We use the lens of design research, which holds that imagined representations of the future—including concept videos—are values-laden, express points of view, and can take part in broader discourses, such as debates about privacy (Dunne & Raby, 2013; Pierce et al., 2015; J. Tanenbaum, K. Tanenbaum, & Wakkary, 2012; Wong & Mulligan, 2016).

We were interested in whether the portrayal of Amazon Prime Air changed in response to the privacy concerns raised by the public and policy makers. While concept videos do not provide technical details or may not address all possible issues, they provide some insight into how a company is conceptualizing a product or service and the extent to which privacy is influencing its design.[12] Paying attention to representations and depictions of a system's design throughout the design process is essential to the success of the privacy by design agenda. Such representations

[8] See the E-Government Act of 2002.

[9] See Resolution on Privacy by Design by the Data Protection and Privacy Commissioners.

[10] The E.U. General Data Protection Regulation, Article 23 states, "the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

[11] For example, see TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (complaint), available at https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter (insecure internet connected cameras left homes vulnerable to surveillance by third parties); for an earlier action see, FTC v. Frostwire, LLC, No. 11-cv-23643-CV-GRAHAM, at 13–16 (S.D.Fla. Oct. 12, 2011) available at http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111012frostwirestip.pdf (Peer-to-peer file sharing apps whose unfair design caused consumers to unwittingly expose sensitive personal files).

[12] Concept videos traditionally serve audiences within a company or group in order to provide a concrete representation of a potential design idea or build shared understandings of design concepts. They can also be shared with other audiences, such as the public, sharing some similarities with advertisements. However, they differ from advertisements in that their main purpose is not to sell a specific product but rather to convey a story or set of ideas about a possible design.

offer a useful tool for considering the privacy impact of a specific artifact in a relevant context of use. They offer the opportunity for a situated, contextual understanding of the way in which technical, organizational, and other forces may combine to afford (or not afford) privacy.

We now turn to consider whether and how Amazon's construction of their future service appears to respond to the privacy issues raised in this voluminous, at times quite heated, discourse of words and images.[13] We first explain our method of video analysis and then closely investigate two concept videos created by Amazon.

Methods for Analyzing Visual Signs

We use and adapt Gillian Dyer's techniques for analyzing visual advertising materials (Dyer, 1982) to facilitate our analysis of the concept videos. We analyze the visual signs—objects and concepts in the video—to unpack their meaning, implications, and significance. These analysis techniques draw upon semiotics, positing that visual objects signify ideas in relation to broader systems of meaning; structured relational languages of codes allow people to interpret objects as signifying certain ideas (Rose, 2007). To acknowledge that technological artifacts—particularly robots—act in the world, we extend Dyer's technique to consider technological artifacts as both props and autonomous agents. Other scholars have argued that technological artifacts in general have some form of agency, existing in sociotechnical systems where the human and technical cannot always be easily separated, such as Actor Network Theory (Latour, 1992). Although we focus on the autonomous drones—and extend Dyer's technique in response to the literal autonomy of these artifacts—in our analysis, our use of the term "agents" encompasses both of these meanings.

Dyer denotes five categories of visual signs in videos with human subjects: the physical appearance of people; people's expression and emotion; people's behavior and activity; props and artifacts; and setting and place. To address the agency of drones we modify our analysis of visual signs to look at the physical appearance, expressions, and behaviors of *agents* both human and technological. We further follow Dyer by analyzing visual camera techniques, such as camera angle, camera focus, lighting, and color. We also analyze the relationship between the spoken narrative and the visual representations.

Our goal is to present a method that can be used to systematically consider how the presentation of systems and artifacts relates and responds to public discourse around their introduction into society. Our goal is not to argue that our interpretation is the only "correct" reading. Viewers do not passively receive videos but rather interpret it based on their own social experiences and beliefs. Looking at concept videos as design fictions focuses our attention on the possible social and technical futures they represent, and how those futures dialogue with broader discourses around privacy.

We follow the method presented above to investigate themes in the two Amazon Prime Air videos, in particular paying attention to signs that may signify privacy-related issues. We note features of each video, followed by a discussion of how the representations in the video relate to privacy concerns articulated by stakeholders and a conclusion with some broader thoughts about the uses of concept videos.

---

[13] For example, see fdnyfish, What can my drone see?, Aug 1, 2015, https://www.youtube.com/watch?v=76P2Zr0yG_0 (showing what is visible at various heights from a personal drone, without specifying the drone's capabilities); Aeroworks Productions, Drones and privacy: the real truth, Aug 1, 2015 https://www.youtube.com/watch?v=GC85qvEhbLA (providing images of what is visibility at various levels using three specific drones); Soldier knows best, Amazon Prime Air: Will it work, Dec 3, 2013, https://www.youtube.com/watch?v=R8CorDkAsws

Features of the 2013 Amazon Prime Air Video

Amazon's first video introducing "Amazon Prime Air" was published on YouTube in December 2013.[14] The video opens with a person ordering a skate tool from Amazon on a tablet and selecting the "Prime Air 30 Minute Delivery" option. It cuts to an Amazon fulfillment center, where we see a worker place the boxed skate tool into a yellow plastic Amazon box. The box is sealed and placed on a conveyor belt with other similar boxes. At the end of the conveyor belt, an Amazon drone grasps the yellow box, takes off by itself, flies an unspecified distance, and lands outside the patio door of a house. It then detaches the yellow box and takes off again by itself. A man comes outside, picks up the box, and goes back into the house.

Agents' physical appearances. In this video, the primary agent is the drone itself. The drone has eight rotors and looks like other eight-rotor drones that might be used to hold camera equipment for aerial photography or video purposes (Fig. 1). Instead of carrying camera equipment, the drone uses clamps underneath it to grasp and release yellow Amazon boxes holding customers' items. Most of the drone's components are made out of black material or unfinished metal, giving it an industrial look. Furthering this look, the drone's wires are exposed and the rotors are open, unobstructed and unguarded.

Humans are barely seen (Fig. 2). While a human places the order and another human packages the item, only their hands are visible to the camera. At the very end of the video, we see a middle aged Caucasian male pick up the package from the backyard while a male child watches from the house, both wearing casual clothes, although their time on screen is very short.

Figure 1: The 2013's depiction of the drones, from the side (left) and close up (right) as it prepares to clamp onto a package. The inner workings of the drone, such as its wires, are visible (right).

Figure 2: Humans are barely present in the video. When they are, only their actions are focused on, such as preparing a package (left) or picking up a package (right).

[14] Viewable at https://www.youtube.com/watch?v=98BIu9dpwHU

Agent emotion. This video has little in the way of emotion. Humans appear briefly, but the focus is on their actions rather than feelings. The drone is not heavily personified. When picking up the package at the end, the man looks serious, while the child looks happy to see the package.

Agent behavior. Human behavior in this video is limited and is largely subsumed by the importance of the drone's behavior. Humans take on a largely ancillary role, pushing a button to order, helping load the package, and picking up the package after it is delivered. The drone, however, exhibits more behavior. It uses clamps to pick up the yellow delivery box while inside the warehouse. It then takes off by itself, flies across the sky and over farmland, touches down on the backyard patio, releases the yellow box, and then takes off again (Fig. 3).

Other artifacts. Aside from the drone, the main artifact in the video is the yellow Amazon shipping container. It appears small, perhaps the size of a shoebox, and several of them appear going down the conveyor belt in the warehouse. The yellow color makes the container highly visible against the black and metallic drone. The multitude of yellow containers in the warehouse allows the viewer to imagine that Prime Air is a widespread and common service, not just limited to a single drone, but likely a fleet to deliver the packages.

Settings. There are three main settings in this video. The first is the warehouse of the Amazon fulfillment center, where the drones start. It is shown as a wide, expansive space with almost no humans. The drone sits at the end of a conveyor belt near a large door, ready to pick up packages. A large circle is painted on the ground around the drone, perhaps denoting a landing zone or safety radius (Fig. 1, left). The second setting is outdoors. It is not clear how far the drone flies, but several shots depict the drone flying against a blue sky and over an open field. The third setting is the backyard patio where the drone lands, unclamps its package, and then flies off again. This implies that the service is for locations where people can afford single-family homes with yards (Fig. 3).

Visual techniques. Visually, the video foregrounds the Amazon drone as the central focus, while it places humans in the background. When the package is ordered, we only see a finger tapping on a tablet in the visual frame. In the warehouse, we only see parts of human workers' bodies as they interact with the broader technical system, such as their hands as they pack the delivery. Other humans are seen in the background, but they are small and out of focus. By only showing parts of humans in frame, or showing them out of focus, they are largely interchangeable and ancillary to the drone itself. The drone, however, is always shown in focus. Close up shots of the drone in the warehouse make it appear larger than life, even within the large expansive warehouse space. While flying, the drone is still the center of the image, as the camera looks up at the drone from the ground or looks at it horizontally from the sky. Even though a human is seen in focus picking up the package at the end of the video, by this point, the drone has been established as the central character.

Figure 3: The drone shown flying in the air (left) and landing in a backyard (right).

Narration. This video lacks any narration. It is silent except for the sound of the drone's rotors. The high speed, high-pitched sound of the drone may imply that it is small, fast, and potentially dangerous if the rotors came into contact with something. The lack of narration allows users to interpret and imagine details about the drone's actions, and what animates them, as there is no explanation of actions such as how the drone navigates, how far and high it flies, or if it is able to take pictures of people and houses it flies over.

Features of the 2015 Amazon Prime Air Video

Amazon's second video entitled "Amazon Prime Air" was published on YouTube in November 2015.[15] While the overall concept of Prime Air is similar to the 2013 video, the 2015 video includes narration, a greater focus on the customer's experience with the service, and several significant design changes. The video starts by presenting an onscreen narrator, Jeremy Clarkson, host of the BBC television show *Top Gear*. He explicitly asks the viewer to step into Amazon's view of the proximate future, saying, "This is a story from the not too distant future." We are shown and told about a family that lives in a suburban home. The family's bulldog tears up the daughter's soccer shoes, which is problematic as she has a soccer match later that day. The mother orders a new pair of shoes from Amazon. We then see an Amazon warehouse, as a worker packages a pair of shoes that is then automatically loaded into an Amazon drone. The drone then takes off on its own, flies to the family's house, lands by itself in their backyard, and deposits the package before departing again. Inside the house, the mother takes the new pair of shoes out of the Prime Air box and gives them to Millie, the daughter, while Stuart, the bulldog, gets a new chew toy.

Agents' physical appearances. There are several human agents in the video. The main group consists of a Caucasian family of three: father, mother, and daughter. The parents are dressed in casual clothes, while the daughter is dressed in a soccer uniform. The narrator, Jeremy Clarkson, appears several times in the family's home speaking directly to the camera, wearing a dress shirt. In some shots, a male Amazon worker is briefly seen at a warehouse, though few details about him are visible.

The autonomous Amazon Prime Air drone is the agent in the video that receives the most attention (Fig. 4). Described by the narrator as "a miracle of modern technology" when it first appears on the screen, the drone displays bright shiny colors, covered in blue, yellow, and white, emblazoned with the Amazon logo, rather than the common plain-black consumer drones. Furthermore, there are panels on the sides of the drone that enclose the inner workings. The blades and rotors are barely visible, and any digital technologies, such as cameras or sensors, are non-apparent. Similarly, the package that the drone carries is placed into an enclosed compartment and cannot be seen from the outside. In many ways, it looks like a colorful flying enclosed box or frame when it is in the air.

Agent emotion. While the main agent in the video is the drone, the family displays emotion before and after interacting with its services. After the family finds that their dog ate their daughter's soccer shoe, they appear somewhat frantic, worried, and frustrated. The mother orders a new pair of shoes on a tablet, appearing serious. Once the autonomous drone delivers the package, the mother and daughter appear both relieved and happy once again (Fig. 5).

Agent behavior. The human agents are relatively passive in this video, and they never directly interact with the drone. The mother orders the shoes on Amazon's website using a tablet and receives notifications once the package has been delivered. The mother only goes outside to

[15] Viewable at https://www.youtube.com/watch?v=MXo_d6tNWuY

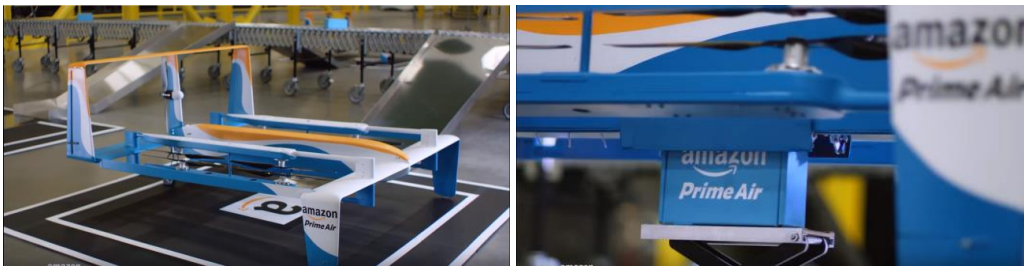

Figure 4: Depiction of the drone's physical appearance in the 2015 commercial (left) and close up as the delivery box is loaded into a compartment (right).

Figure 5: The mother orders products from Amazon using a tablet with a serious expression (left) and delivers the replacement pair of shoes to her happy daughter (right).

retrieve the package after it is delivered. Her interactions are primarily with the service enabled by the drone, more so than direct interaction with the drone. Similarly, an Amazon worker is seen putting the shoes into an Amazon Prime Air box, but the box is automatically delivered to the drone via a conveyor belt.

The autonomous drone, however, is an active agent moving through several stages of action. First, the Prime Air box with the shoes is loaded into the drone, and the drone takes off. The narrator describes this as "taking off, like a helicopter, to nearly 400 feet" (Fig. 6). Second, the drone then switches into a horizontal flying mode, which the narrator describes as a "streamlined

Figure 6: A static camera shot depicts the drone's vertical flight as it lifts off. About 2 seconds pass between these two images as the drone moves vertically upward.

Figure 7: The mother interacts with the drone via tablet, confirming that it can land (left). She then picks up the delivered package and landing mat after the delivery (right).

and fast airplane." Its behaviors are also personified, as the narrator speaks, "it knows what's happening around it," because it will "sense" and "avoid" obstacles. Third, the drone goes back into "vertical mode" as it lands in the backyard of the family's house. Fourth, the drone's internal compartment opens, and the package falls gently to the ground. Last, the drone takes off again and "flies straight back up to altitude."

Other artifacts. Two other key artifacts appear in the video. First is the delivery box. This box is a light blue cardboard box, which looks like a large shoebox, with the words "amazon PrimeAir" printed in white. The second artifact is a landing mat (Fig. 7, right). At the warehouse before the drone takes off, it is sitting on top of a mat with an Amazon "a" logo in the center. The drone lands on a similar "a" logo mat when it delivers the package. A shot from the video annotates the area surrounding the family's mat with the words "Delivery Zone," (Fig. 9, right) implying that the drone knows where to land based on the placement of the Amazon mat—suggesting that it "sees" or otherwise senses the mat. The mother also picks up this mat when she picks up the package, presumably bringing it back into the house.

Settings. The main setting of the video is in a suburban single-family home. The interior furnishings indicate that the family is financially comfortable. The family stays inside the home the entire time, except for the mother who goes into the yard to pick up the package once it is delivered. In contrast, the drone is seen flying in the open air outside in the sky, over farmland, forest, and neighborhoods. Several shots also take place within an Amazon warehouse. In this location, the viewer never sees the face of a worker, nor is the full body of a worker ever in focus. However, the drone is first revealed in the warehouse, with its full body visibly in focus (Fig. 4, left).

Visual techniques. The lack of focus on human workers in the Amazon warehouse—only showing parts of their bodies like their hands or showing one worker out of focus walking away from the camera—deemphasizes and de-individualizes them. In contrast, the appearance of the drone in full size, color, and focus emphasizes it as a major agent in the video. The family is also portrayed in full size, color, and focus. Thus, the video focuses on the drone itself and the experience of the customer end users interacting with the drone service but not warehouse workers or other classes of people who may experience the drones (Fig. 10). For example, we never see bystanders on the ground whose images may be captured by the drone, or how gift delivery via drone would work.

In many scenes in the home, the narrator is placed in the foreground and appears larger, while the family action occurs in the background. This visual placement provides the narrator with greater authority.

Many scenes also use camera angles that are meant to show the viewer the drone's point of view. When the drone is flying over houses in horizontal flight mode, the camera perspective is straight ahead (Fig. 8). This is overlaid with sample flight data such as speed (55 miles per hour), elevation (367 feet), compass direction, and time to delivery. It senses, identifies, and avoids obstacles in the sky, such as a hot air balloon, but does not seem to be sensing and identifying lower-level objects, such as trees or buildings.

However, when the drone begins landing in vertical mode, the drone's point of view changes to a camera angle facing directly downward (Fig. 9). Annotations on the screen imply that the drone is scanning and identifying obstacles, such as trees, building corners, and driveways, while the narrator says that it "scans the landing area." However, the image shown is confined to the recipient family's property—the top-down image does not look into and scan other people's properties.

Narration. The narrator begins the video by stating, "This is a story from the not too distant future." This places the concept video well into the realm of design fiction. By stating that it is both a story and it is in the future, the viewer is encouraged to suspend disbelief and imagine what the world would be like if Amazon Prime Air and its autonomous drone delivery system existed. By calling it the "not too distant future," viewers are encouraged to interact with and think about the video in new ways—what the video depicts is not pure fiction, but could be real. It is a design representation of the proximate future. Thus viewers can imagine how the system might work, how people might interact with it, and what the implications of those might be. The narrator also

Figure 8: First-person view from the drone in horizontal flying mode. Flight data mimics that of an airplane. The drone identifies a hot air balloon in the sky as a potential hazard.

Figure 9: First-person view from the drone in vertical flying mode identifying hazards and the landing zone. Only property owned by the package's recipient is in camera view.

says, "In time there will be a whole family of Amazon drones—different designs for different environments." This also invites the viewer to imagine the world beyond what is depicted in the video and imagine alternate scenarios with different agents in other settings.

The narrator also says that "you could yell angrily [at the dog, or]… much better to act like a rational human being," by ordering using Amazon Prime Air, which will deliver in 30 minutes or less. This language normalizes the idea of Amazon Prime Air, making it seem that choosing delivery by autonomous drone is both normal and rational. This language helps the viewer imagine the world where this is a regular occurrence. Viewers can then take the next step by asking what implications exist in a world where these actions are normal and seen as rational—where families of automated agents are at your beck and call to perform innocuous yet herculean tasks.

Figure 10: The foregrounding and large size of the narrator (left side of the left image) in the family's home emphasizes that this video presents a narrative or scenario. While family members are seen in whole (right side of the left image), Amazon workers (right) are only partially seen.

Representing Privacy in the Amazon Prime Air Videos

The word "privacy" is not used in either video. Yet, several changes from the first to second video read against the volatile privacy discourse can be interpreted as efforts to conceptualize and address privacy concerns.

The Prime Air videos were an explicit part of the public discourse. While not a central focus of this investigation, in prior work we found that news media organizations interpret, critique, and report on corporate concept videos in order to anticipate and speculate about future possibilities (Wong & Mulligan, 2016). The Prime Air videos were viewed and discussed by the media, contributing to a sociotechnical imaginary (Jasanoff & Kim, 2009) about the drone system. Amazon's drone delivery service and its 2013 video were featured in a segment on news program *60 Minutes*.[16] General news, business news, and technology news publications all reported on both the 2013–2015 concept videos, pointing out the boundaries where the service may work or not, looking at potential regulatory hurdles, and discussing the future possibilities that Amazon might explore.[17] Individuals also responded to the concept videos, speculating about how the drone might work technically and even creating parodies to critique aspects of the service.[18]

[16] See CBS, Amazon unveils futuristic plan: Delivery by drone. Dec 1, 2013. http://www.cbsnews.com/news/amazon-unveils-futuristic-plan-delivery-by-drone

[17] For example, see Gregory McNeal, Amazon testing drones for 30 minute delivery using service called Amazon Prime Air VIDEO, Forbes, Dec 2, 2013. http://www.forbes.com/sites/gregorymcneal/2013/12/02/amazon-testing-

Between 2013 and 2015, drones and privacy were debated in multiple venues. Twenty-seven states passed drone-related legislation in that time period, and forty-five states considered over 150 drone-related bills in 2015 (Karol, 2015; National Conference of State Legislatures, 2016). Each state and each bill took a slightly different approach. In February 2015, the Federal Aviation Administration (FAA) announced proposed rules regarding the operation of small, unmanned aircraft systems (sUAS).[19] The proposal includes rules about the operation of drones, such as: operating only in daylight conditions and within a visual line of sight, and flying under 500 feet and less than 100 miles per hour. It also includes rules about operator certification and drone registration. A public comment process preceded the issuance of the final rules. While privacy was outside the scope of the proposed rules, several commenters nonetheless raised privacy concerns.

In February 2015, President Obama called for the National Telecommunications and Information Administration (NTIA) to create a multi-stakeholder engagement process to develop a framework for privacy, accountability, and transparency for commercial and private unmanned aircraft systems. The multi-stakeholder process, in which Amazon participated, produced a final Best Practices document in May 2016 (NTIA, 2016)[20]. These voluntary Best Practices address the collection of personally identifiable information by commercial and non-commercial UAS, and flying over and within private property.[21]

Drawing on these policy debates, new laws, and frameworks, we explore changes between Amazon's 2013 and 2015 videos to consider whether and how they are adjusting the portrayal of their service in response to privacy concerns.

Trespass and Constructive Trespass as Privacy Harm

Concerns about drones trespassing on the air space over private property[22] to view activities or individuals are a staple of the policy discourse. The Center for Democracy and Technology (CDT)

---

drones-for-30-minute-delivery-using-service-called-amazon-prime-air; Matt McFarland, Amazon has a new drone delivery video. Here are 8 details worth noting. *Washington Post*. Nov 30, 2015 https://www.washingtonpost.com/news/innovations/wp/2015/11/30/amazon-has-a-new-drone-delivery-video-here-are-8-details-worth-noting; Tiffany Kelly, Amazon shows off prototype drone for future delivery service in new video. *ArsTechnica*, Nov 29, 2015. http://arstechnica.com/business/2015/11/amazon-shows-off-prototype-drone-for-future-delivery-service-in-new-video;

[18] For example, see Soldier knows best, Amazon Prime Air: Will it work, Dec 3, 2013, https://www.youtube.com/watch?v=R8CorDkAsws (speculating on how the drone service works); Team legit, Amazon Prime Air parody, Dec 6, 2013 https://www.youtube.com/watch?v=ViqsDpTvRdk (parody suggesting packages might get stolen or shot down, with Amazon responding by selling customers "Prime Insurance"); Michael Stusser, Amazon Prime Air launches new ad campaign (parody) https://www.youtube.com/watch?v=FsZ0Y1qL-GI (parody that suggests drones may crash, go to the wrong location, or be used for surveillance in neighborhood watch programs).

[19] These are defined as a small unmanned aerial vehicle (sUAV) under 55 pounds, and the equipment necessary for the safe and efficient operation of that aircraft.

[20] The Best Practices document was updated in June 2016 with additional background information, but the recommendations remain the same. The June 2016 version is cited here.

[21] The Best Practices document expressly does not apply to newsgatherers and news reporting organizations as to not raise potential First Amendment issues. The document states, "Newsgatherers and news reporting organizations may use UAS in the same manner as any other comparable technology to capture, store, retain and use data or images in public spaces" (NTIA, 2016).

[22] The precise bounds of private airspace are uncertain and vary. It lies between the publicly navigable airspace secured for air travel by Congress (49 U.S.C. § 40101(c)(2) (2012)) and the "immediate reaches of the air space next to the land" protected against trespass under tort law (RESTATEMENT (SECOND) OF TORTS § 159(2)(a) (1965)); its contours are filled in by state statutes. The recently adopted final rules for *Operation and Certification of Small Unmanned Aircraft Systems* set a maximum altitude of 400 feet above ground level, but no minimum. Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed.

discusses the potential for drones to surveil individuals by peering into the windows of people's homes or areas immediately outside the home (CDT, 2015). Both CDT and the Future of Privacy Forum (FPF) comments in the NTIA proceedings suggest that geofencing technologies and other technical mechanisms may be used to preserve privacy by allowing homeowners to prevent drones from flying near their person or over their private property (FPF, 2015). The final NTIA voluntary Best Practices state that operators should minimize UAS operations over or in private property without the property owner's consent (NTIA, 2016). [23]

Legislatures have responded to this privacy threat. In Texas, the state code now makes it illegal to "uses an unmanned aircraft to capture an image of an individual or privately owned real property . . . with the intent to conduct surveillance on the individual or property…" (Texas Code Sec. 423.003, 2015). In California, a state law defining the physical invasion of privacy was amended in 2015 to include entering "…airspace above the land of another person without permission or otherwise commits a trespass in order to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or familial activity and the invasion occurs in a manner that is offensive to a reasonable person" (California Code Sec. 1708.8, 2015). Concerns about increasingly powerful telephoto lenses were addressed years earlier through the creation of a cause of action for a "constructive invasion of privacy" defined as "capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or familial activity, through the use of any device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the device was used" (California Code Sec. 1708.8, 2015)

The 2015 Amazon video elaborately explains the drone's flight behavior in a manner that reduces concern about capturing images of private homes and human activity on private property. In the 2013 video, the drone delivered the package by flying from the Amazon warehouse to the recipient's house. There was no description of the drone's flight pattern or visual field. In 2015, the flight pattern is broken down into three distinct flying phases, and each is shown and described in detail: a vertical helicopter-like take off phase; a horizontal airplane-like phase; and another vertical landing phase.

In takeoff mode, the narrator compares the drone to a helicopter, describing it flying straight up to 400 feet. This suggests that the drone will be high enough as to not surveil and look closely at people in their homes or on their property. The visual images of the drone show it flying up next to an industrial warehouse, and the vertical takeoff (instead of a horizontal plane-like takeoff) indicates that it will not fly over homeowners' private property until it reaches an altitude of 400 feet.

The video then describes the horizontal flight mode, which the narrator compares to an "airplane." While airplanes fly above private property, people on the ground are generally not concerned that airplane passengers are violating their privacy. By drawing on people's experiences

---

Reg. 42064, 42097 (June 28, 2016). For a thorough description of the challenges of defining private airspace in relation to a trespass claim, see Froomkin, A. M., & Colangelo, P. Z. (2015). Self-defense against robots and drones. *Connecticut Law Review*, *48*, 1.

[23] The questions of who regulates activity in the airspace at different altitudes, what limits the First Amendment places on the regulation of video and audio recordings from public places, and what both mean for privacy interests are beyond the scope of this discussion, which is interested in how Amazon is shaping its service based on privacy concerns regardless of whether those concerns could be addressed through state or federal legislation. However, these are significant questions that others have explored; see Kaminski, M. E. (2013). Drone Federalism: Civilian drones and the things they carry. *4 California Law Review Circuit 57*.; McNeal, G.S. (2014). Drones and aerial surveillance: Considerations for legislators. *Brookings Institution: The robots are coming: The project on civilian robotics, November 2014; Pepperdine University Legal Studies Research Paper No. 2015/3*.

of flying in airplanes, the video abates concerns about visual surveillance of private property and activity on it.

The 2015 video reveals that the drone has some type of camera or visual recognition device. However, the only object it identifies during its horizontal flight is a hot air balloon, a high level object. The video does not show it identifying other potential hazards like trees and rooftops, which are closer to the ground. This suggests that the drone only looks toward the horizon during the horizontal flight phase, not down toward the ground and people and buildings. While houses are visible at the bottom of the image, they appear far away and details are not visible. The horizontal camera image is overlaid with flight data including time to destination, height, speed, and direction. The use of iconography and phrasing familiar to the data and display of an airplane's flight tracker further reinforces the airplane metaphor, situating the drone in a familiar context that evokes a particular understanding of the drone's view of the environment in which it acts in a manner that is tightly connected to its purpose and presents limited concerns with the privacy of those on the ground.

In the vertical landing phase, the drone-view camera switches to look directly down, so it can identify the landing site and potential hazards. The video looking directly down only shows the house and property of the package recipient. The framing of this part of the video, the narrator's disclosure that it "scans" while landing, and the narration that it "flies straight back up to altitude," also serve to convey the sense that the drone is only looking down and visually scanning the land of the package recipient. The drone does not appear to scan or see the neighbors' yards and other adjacent areas.

The video implies that the drone searches for an Amazon landing mat on the package recipients' property. The mother picks up the mat after retrieving the package, implying that customers have some control and agency in determining the drone's landing site. This artifact was not present in the 2013 video, suggesting the drone had complete freedom to choose its landing site. The 2015 video's inclusion of the moveable mat presents a scenario where humans exercise control over an important safety-related aspect of the autonomous system.

The emphases on vertical takeoff and landings, the nearly 400-foot flying altitude, and the use of airplane-like iconography to orient viewers to the drone's view of the environment in the 2015 video speak to the privacy concerns about surveillance of private property and human activity on it—and the related concern of entering low airspace over such private property. The vertical landing and takeoff imply that any downward facing images will only be of the recipient's property, who presumably consents by using the service, thus not peering into neighbors' property or entering the airspace directly above it at a low altitude. Amazon reveals potentially privacy-invasive affordances but proactively suggests how privacy concerns are addressed through the service's design.

Privacy Harm as Non-Consensual Data Collection

Both CDT and FPF raised concerns about the types of data drones can collect without individuals' knowledge or consent. Drones can carry a variety of sensor equipment, including cameras, audio-visual sensors, high-powered zoom lenses, infrared and thermal cameras, biometric recognition technologies, and other sensing technologies. Each of these sensor types can potentially collect personal information about individuals without their knowledge or consent. Furthermore, at present, while some states are enacting laws to limit the collection of data by drone operators, aside from prohibitions on eavesdropping, there is weak and inconsistent privacy protection from such sensors. The NTIA's best practices document recommends informing individuals whose personally identifiable data may be collected by providing prior notice and a privacy policy,[24]

[24] The document states that UAS operators need only use "practical and reasonable effort" to provide prior notice. The document also recommends that this notice inform individuals of a general timeframe and area where a UAS may collect identifiable data (NTIA, 2016).

avoiding the collection of information that identifies particular people where they have a reasonable expectation of privacy, and avoiding "using UAS for the specific purpose of persistent and continuous collection of covered data about individuals" (NTIA, 2016).

The 2013 video provides no specific sense of what data the drone might collect. In contrast, the 2015 video strongly implies that the drone is equipped with several cameras and sensors that measure altitude and geographic location, and detect or sense potential obstructions. Sensed data is overlaid on the horizontal in-flight view (Fig. 8). However, the drones could be equipped with a variety of other sensing technologies that are not suggested by the video, such as thermal imaging or heat sensing as well as the capacity to transmit photos and videos in real time (Wingfield & Sengupta, 2012).

Timothy Takahashi (2012) offers a description of sensors, with which small UAV drones can or could soon be equipped, as well as some of the implications of using these sensors. With current technology, enhanced imaging techniques can be deployed for operation in low-light conditions and at night, using the same technology as night vision goggles or infrared sensing. Drones with conventional microphones or laser optical microphones could collect audio samples, potentially within as much as a 1000-foot range. Molecule and chemical sensors could conceivably detect cannabis burning or perfume scents (Takahashi, 2012). Takahashi further speculates that a number of sensors not widely available for civilian drone use could soon be implemented, due to technical advances or relaxations of military restrictions. Imaging radar can produce images through smoke and haze, and can also detect objects through walls. Technological advances have miniaturized this technology, making it possible for a drone to use it in the near future. Military-grade imaging can detect individuals from 10,000 feet in the air, suggesting that people on the ground will be highly visible to small UAV operations at 400 feet. Linking sensors and data from multiple sources, such as ground-based sensors and existing databases, would enable drones to identify and track individuals whom they sense.

It is not clear, in the 2015 video, whether the drone's behavior is regulated by technical design or policy. For instance, the drone-perspective camera only looks vertically downward when landing and taking off, and the image only shows the recipient's property, thus addressing concerns about trespassing and taking photographs on private property. However, that action could be constrained in several ways. There could be a physical constraint on the camera because a single camera swivels between vertical and horizontal mode, limiting what the drone can observe at a point in time. Or the downward facing camera might capture neighbors' property but crop it out before images are processed. Or the downward camera may be constantly on but only process the data while in vertical mode. Or, the drone may be capable of 360˚ imaging but limited by policy to a narrower field of view.

The 2015 video shows some types of data the drone might collect, indicating some increased sensitivity to privacy implications and concerns. However, the use of sensors beyond regular cameras, and the specific mechanisms that may serve to limit data collection were not directly addressed in the 2015 video. While the video suggests that drones will not collect personal data, it does not convey the technical or policy limits on such data collection.

Privacy Harm as Unwanted and Unknown Data Use

Related, but separate from concerns about data collection, are concerns about data being used in ways that are unknown or unwanted by the people whom the data is about (CDT, 2015; Electronic Privacy Information Center, 2015; FPF, 2015). Privacy advocates suggest that images collected by drones may be unknowingly used to identify people using facial recognition, license plate scanning technologies, or behavioral analysis technologies. Sensors may collect sensitive information, but limits on processing, retention, or sharing can mitigate privacy risks. The NTIA's Best Practices recommend limits on the use and sharing of personally identifiable data, including

not using the data for employment, credit, and healthcare eligibility, and not using identifiable data for advertising without consent.

The 2015 Amazon video suggests that data collected will be used only for the process of delivering a package. But the issue is not directly addressed and the absence of data reuse from the video does not necessarily mean that use and sharing are limited.

Privacy Harm as Lack of Transparency

CDT and FPF note the need for transparency about who is operating a drone to enable individuals to protect themselves against privacy invasions (CDT, 2015; FPF, 2015). The overriding concern is being able to identify the operator of a visible drone. The ability to identify the operator is heightened if the drone is capable of collecting, storing, or sharing images or other data about people. CDT and FPF suggest that every drone should broadcast a unique identification signal (akin to a license plate), which would be tied to a database record containing the name of the owner and operator, and other information such as the privacy policy. Drone flight tracking tools could be created to track these identification signals, similar to airplane flight trackers today. The FAA's rule requires registration of sUAS and their operators.

Amazon changed the appearance of their drones in a manner that facilitates easy identification. Both the 2013 and 2015 videos show a drone with the word "Amazon" on the side. However, the 2013's black color and common 8-rotor design would make it more difficult to distinguish Amazon's drone from other owners' drones, particularly when viewed at a distance. The 2015 video shows the Amazon drone with a unique and bright color scheme, and a unique square-like shape. The design changes increase the identifiability of Amazon's drones from a distance. While this likely has marketing and brand benefits, it also addresses transparency concerns arising in the privacy discourse. The 2015 video's updated design allows people on the ground to easily identify a drone as belonging to Amazon. Presumably an interested individual could then go to Amazon's website to learn about their data collection and use policies.

Privacy Harm as Lack of Security

The Electronic Privacy Information Center (EPIC), in public comments to the FAA, points out the need for cybersecurity measures to be implemented in drones (EPIC, 2015). If drones and their surveillance equipment are hacked, unauthorized access to these tools could facilitate additional surveillance and surreptitious monitoring. The NTIA Best Practices recommend that operators take measures to secure collected data, following common security frameworks and standards (NTIA, 2016).

Amazon's concept videos do not discuss any security measures related to the data that the drone uses or collects. However, the use of the package recipient placing a landing mat for the drone in the 2015 video perhaps suggests a way to protect the physical security of a recipient's package (i.e., without the recipient physically placing the landing mat on the ground, the drone is unable to deposit the package).

Privacy as Fair Information Practices

We note that the policy debate is heavily influenced by the Fair Information Practices (FIPs). Originally articulated in 1973, the FIPs identified five principles to protect individuals' privacy in government databases:

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

(2) There must be a way for a person to find out what information about that person is in a record and how it is used.

(3) There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

(4) There must be a way for a person to correct or amend a record of identifiable information about the person.

(5) 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 precautions to prevent misuses of the data.

The FIPs exist as principles, not laws. However, the principles have been incorporated into some sector- or context-specific laws in the U.S., such as the Health Insurance Portability and Accountability Act (HIPAA) privacy rule and the Children's Online Privacy Protection Rule. Other versions of the FIPs exist as regulatory guidelines. For instance, the principles were restated in the FTC's 2000 *Report on Online Privacy* (in part leading to the pattern of website privacy policies today). In this version, sites are called on to (1) provide *notice* to consumers about a site's information practices; (2) provide consumers *choice* about how their data is used; (3) provide consumers *access* to review or delete information collected about them; and (4) protect the *security* of consumers' information. The FTC published similar restatement of the FIPs in a 2015 report about privacy and the Internet of Things. While well-known problems exist with the FIPs, such as users' not reading or understanding privacy notices and privacy policies (Solove, 2013), it is a durable framework that has been repeated and implemented in many contexts (Gellman, 2015).

FPF directly calls for the FIPs to be used as a framework to address potential drone-related privacy concerns (FPF, 2015). Other concerns framed around the non-consensual collection of data, unknown uses of data, lack of data transparency, and lack of security reinforce a FIPs-based view of privacy in the context of autonomous drones.

Amazon also submitted a comment to the NTIA regarding Amazon Prime Air. Prime Air is described as "a future delivery system designed to get packages to customers in 30 minutes or less using small unmanned aerial vehicles" (Amazon.com, 2015a). They associate privacy with the need to maintain "consumer trust" and note that they will use information in a "responsible, appropriate, and secure manner" in order to protect users' privacy. However, the concept videos largely do not address the FIPs, as they do not provide enough specifics about the types of data collected, how they may be used, or how users can access that data.

Privacy as Contextual

Many of the state laws focus on limiting drone activity and data collection where individuals have a reasonable expectation of privacy. For example, Wisconsin law states "Whoever uses a drone, as defined in s. 175.55 (1) (a), with the intent to photograph, record, or otherwise observe another individual in a place or location where the individual has a reasonable expectation of privacy is guilty of Class A misdemeanor" (Wisconsin Statute 942.10, 2013). The concept of a reasonable expectation of privacy has deep roots in U.S. privacy jurisprudence. Formulated in the 1967 Supreme Court case *Katz v. United States*, to emphasize that privacy protected people, not places, the concept allows privacy to be protected in public as well as private places. A reasonable expectation of privacy is a normative and contextual approach to conceptualizing privacy.

The narrator in the 2015 video personifies the drone, which serves to build empathy and trust with the drone; he says that there will be a "family" of drones that can go different distances or operate in different environments (unlike the 2013 video, which contains no narration). The term "family" is a warm and affectionate description that replaces more standard terms such as fleet, army, squad, or swarm. Importantly, the notion of having different drones for different situations implies that drones will have different qualities appropriate to various contexts. This draws some parallels to contextual definitions of privacy, which hold that preserving privacy is dependent on following contextually determined social norms about information flow (Nissenbaum, 2009).

Amazon in the Policy Debate

Our analysis identifies several changes to the representation of the drone delivery service, between 2013 and 2015, that are responsive to privacy concerns. While our research does not allow us to attribute these changes to the public dialogue about drones and privacy, we note that Amazon participated in these debates and processes, participating in the NTIA's multi-stakeholder process (NTIA, 2015), submitting public comments to the NTIA, and providing Congressional testimony. While its testimony before the Senate Subcommittee on Aviation Operations, Safety, and Security, focused primarily on safety concerns,[25] Amazon's representative disclosed that the planned "future delivery system"[26] would use "sophisticated 'sense and avoid' technology," be automated, operate at distances of 10 miles or more and operate beyond an operator's visual line of sight, and acknowledged that there may be potential surveillance concerns (Amazon.com, 2015b). Amazon addressed these concerns by stating that "Prime Air is a future delivery service, not a surveillance operation, and we will respect the privacy of every person, with stringent privacy policies accessible to all" (Amazon.com, 2015b). Amazon's public comments to the NTIA on drone privacy suggest that issues of privacy, transparency, and accountability need to be considered together. The comments also frame privacy as an issue of consumer trust, which can be maintained if information is used in a "responsible, appropriate, and secure manner" (Amazon.com, 2015a).

A critical analysis of Amazon's concept videos provides a useful complement to these statements by providing a visceral sense of what their future system might feel like. Yet videos provide limited details about the drone's technical capabilities and specifications. To some extent, the ambiguity of concept videos is a "feature," not a "bug." One video cannot possibly demonstrate every element of a system, or every situation in which it may operate, even with multiple videos, as not every situation can be anticipated. Leaving some ambiguity provides viewers the ability to create multiple interpretations and ask further questions about the service (Sengers & Gaver, 2006), particularly early in the design process of the system. Amazon's framing provides a starting point for interpretation, imagination, extrapolation, and further questioning. However a lack of communication over the drone's full capabilities, and what that experience might be like for users, can be troublesome as the system or service approaches deployment and launch. One would expect more details about the drones' capabilities to be released as the service approaches commercial deployment to better determine how the design of the ready-to-deploy system addresses (or does not address) privacy.

Amazon's representations of Amazon Prime Air's design in the 2013 and 2015 videos suggest responsiveness to the privacy debates. Although the 2015 video did not address every privacy issue raised with regard to drones, it did respond to concerns about surveillance, drone use over private property, and operator transparency. The video was framed as to suggest certain actions and capabilities the drones have and do not have. It may be that Amazon's intended audience for the videos is not only consumers, but also policymakers, regulators, and advocacy groups. Indeed, the Future of Privacy Forum viewed and cited Amazon's Prime Air webpage in its April 2015 public comment to the NTIA, which contained a link to the 2013 concept video (FPF, 2015).[27] The

[25] Amazon was pushing for the FAA to examine operations beyond visual line of sight and calling for harmonization of rules within the U.S. through uniform federal rules (Amazon.com, 2015b).

[26] As of March 2015, Amazon had tested this system in several outdoor locations in non-U.S. countries and in indoor locations within the U.S. (Amazon.com, 2015b).

[27] See footnote 30 in FPF (2015) *Letter to the National Telecommunications and Information Administration*. The Internet Archive's Wayback Machine shows that on April 1, 2015, the Amazon.com webpage cited by FPF contained a link to view or download the 2013 concept video, Amazon's July 2014 letter to the FAA, and a short FAQ section.

changes between the 2013 and 2015 Amazon videos suggest that Amazon refined its vision and design of the Prime Air service, including design changes to potential privacy-infringing parts of the service.

Discussion

The preceding analysis shows that changes between Amazon's 2013 and 2015 video representations of Prime Air indicate that Amazon made design changes that addressed several privacy concerns raised in policy discussions. While Amazon was also involved in these debates, this analysis suggests that beyond written disclosures and policy comments, we can look to companies' actual designs and design representations, to see how they are addressing privacy concerns.

In this section, we note two further potential uses of the concept videos. First, we discuss the changing legal significance of video representations like these when a product comes to market. The concept videos we reviewed represent a fictional product; however, when Amazon's automated drone delivery service is available to the public, the videos take on new legal significance as representations of the product's functionality, including privacy-related functions. Second, we note a variety of ways that concept videos can be used to engage policymakers and other stakeholders in conversations about values.

Concept Videos as Material Representations

Concept videos provide a potentially potent way for companies to communicate the ways in which their products and services take account of privacy. The changes in Amazon's portrayal of the Prime Air service couple a simulated experience with their service with specific statements about the services operation (by the video narrator). Both the statements and the visual representation acknowledge privacy concerns raised in the broader policy discourse, although neither privacy nor personal information is mentioned. These visual and audio representations are likely shaping consumers' expectations about Amazon's drones and will inform consumers' understandings of the product when it goes live. Through representations of the service's design, the video communicates information about how Amazon's drones respect privacy and private property.

The concept videos shape consumers' understanding and expectation of the service. Like advertisements, they are a source of information about the service and its operation and may inform consumers' decisions about whether to use it. While the videos portray the service in a way that responds to some privacy concerns, the videos are silent on many other aspects of the service that raise privacy concerns. The videos omit information about what sensors are onboard, what they can and do record, how collected information is used, how long it is maintained, and whether it is shared with others. These omissions leave out information necessary for consumers to fully understand the privacy implications of the service.

Beginning in the mid-1990s, the Federal Trade Commission (FTC) has used its authority to police deceptive and unfair practices in the marketplace to protect consumer privacy. When evaluating deceptive practices, the FTC considers the practice from the viewpoint of a reasonable consumer and considers representations, omissions, and practices that are "material" to consumers (FTC, 1983). Express claims and representations are material, but omissions can be too. Marketing that provides incomplete information, for example, can be deceptive.[28] Importantly, the FTC's

[28] The FTC Act states: "False advertisement" means an advertisement, other than labeling, which is misleading in a material respect; and in determining whether any advertisement is misleading, there shall be taken into account (among other things) not only representations made or suggested by statement, word, design, device, sound, or any combination thereof, but also the extent to which the advertisement fails to reveal facts material in the light of such representations or material with respect to consequences that may

authority to police deception in the marketplaces covers deceptive commercial speech broadly, not just advertisements.[29]

When the FTC evaluates deception, they look at representations to the public in all forms. In the context of privacy, this may include terms of service, privacy policies, blog posts; advertising and marketing materials; and non-textual representations, such as online design and layout, configurations, and other settings (Hoofnagle, 2016). In other words, all relevant design choices, their implementation, and their representations can potentially cause consumers to be misled (Hoofnagle, 2016).

A statement is deceptive where it makes a material representation, omission, or practice that is likely to mislead consumers acting reasonably under the circumstances. The FTC's policy statement on deception further clarifies that a "…misrepresentation is an express or implied statement contrary to fact" and a "misleading omission occurs when qualifying information necessary to prevent a practice, claim, representation, or reasonable expectation or belief from being misleading is not disclosed." (FTC, 1983) When reviewing advertising, the Commission considers the "entire mosaic" (FTC v. Sterling Drug, 1963), considering the "visual and aural imagery of advertisements" to understand the overall impression on the consumer (FTC, 1983).[30] Thus, all representations—audio and visual, explicit and implied—are potentially relevant to the question of deception.

The FTC focuses on the viewpoint of a reasonable consumer, taking a "surprise" approach to omissions in privacy policies and focusing on consumers' expectations (Hoofnagle, 2016). Advertisements and practices are judged by their likelihood to mislead a reasonable consumer, not by the intents of the advertisements' authors. Material claims or omissions are those that would affect a consumer's choice of, or conduct, regarding a product. In the privacy context, as in others, misleading and false statements are considered material. Withholding information about uses of data that are more likely to be objectionable while highlighting appealing uses can be deceptive. In addition, one can implicitly create expectations about data collection and use. For example, by highlighting and talking about some uses but not others, users' expectations of a system's capabilities may be much narrower than the system's actual capabilities. Deception occurs if a system's data use upends expectations. If there is surprising, scary, or unexpected data collection or data use that is not disclosed to consumers, this can give rise to deception, because consumers may have made a different decision if the data collection or use had been disclosed. For example, Hoofnagle (2016) notes that "surprising" practices include: sale of personal information to third parties; collection location or other sensitive information; collection of information from a

---

result from the use of the commodity to which the advertisement relates under the conditions prescribed in said advertisement, or under such conditions as are customary or usual (15 U.S.C. 55(a)(1)).

[29] The Commission recently reaffirmed the breath of its authority to police deceptive statements in the marketplace. In re POM Wonderful, LLC, FTC Docket No. 9344, (Jan. 10, 2013), affd in relevant part, 777 F.3d 478 (D.C. Cir. 2015). While basing the finding of deception exclusively on advertisements, and not a set of interviews that had also been part of the initial complaint, it rejected an ALJ's narrow construction of their authority, stating, "We do not adopt the predicate for the ALJ's ruling–that the media interviews must be advertisements (rather than deceptive commercial speech more broadly) in order to form the basis for liability under Section 5 of the FTC Act." POM Wonderful LLC, FTC Docket No. 9344, at 46. The use of social media and other new approaches to advertise and promote products raise increasingly complicated questions about the interaction of the FTC's authority and freedom of expression guarantees. See, e.g., Bond, K. (2016). Tracing FTC's line on commercial speech: What makes an ad an ad and why does it matter. *Food & Drug LJ, 71*, 211.

[30] See FTC (1983) Policy Statement on Deception, citing American Home Products, 695 F.2d 681, 688 (3d Cir. Dec. 3, 1982). "The Commission's right to scrutinize the visual and aural imagery of advertisements follows from the principle that the Commission looks to the impression made by the advertisements as a whole. Without this mode of examination, the Commission would have limited recourse against crafty advertisers whose deceptive messages were conveyed by means other than, or in addition to, spoken words" (p. 4).

user's contact list or address book; transferring a unique identifier that leads to disclosure of personal information with third parties; changing settings in a way that degrades users' previous privacy protections; and default settings that cause users to inadvertently make files public from their computer.

At the time of writing, these concept videos of Amazon Prime Air represent a fictional product. However, when Amazon's automated drone delivery service becomes available to the public, these types of video representations take on new legal significance. Amazon's Prime Air videos make privacy-relevant representations—visual and audio—about the operations of the future service. Consumers viewing them will form impressions about the services impact on their and others' privacy. The images and narration create an overall impression that visual images of earth's surface—including the homes and activities of people—are not collected while the drones are in transit, and that the drone's field of vision is very tightly circumscribed on descent. Through different visual camera angles and airplane iconography, the video suggests that when the drone is flying horizontally, it is not surveilling people, and when travelling vertically to land or takeoff, it only captures images of the recipient's property near the owner-designated landing site. Although the video goes to great length—including narrator emphasis—to suggest limits on the visual field of the drones, it does not directly discuss its data collection capacity or practices.

As discussed above, the data collection capacity and practices of Amazon's drones are likely to be considered material to consumer decisions about whether to use the service. Being silent about the data collection performed by onboard sensors (those that assist on measuring altitude, identifying locations, sensing hazards, navigating and any others) may lead consumers to believe that no data about them or their neighbors is being collected. By highlighting and talking about some privacy-relevant aspects of the service but not others, the video may skew consumers' understanding of the system's capabilities, leading them to believe they are far more limited and benign. The contrast between the detailed information shared about flight patterns, and the dearth of information about data collection and use, creates a *prime* opportunity for consumer surprise. Given the potential impact of these hidden capabilities to undermine privacy expectations, as Prime Air comes closer to reality, Amazon should consider providing more information about the sensors and their collection and use of data to ensure that consumers more fully understand the privacy implications of the service. If there are sensing, data collection capabilities, or uses of personal data that would be unexpected by a reasonable consumer, they should be disclosed.

Given the current and future capacities of onboard sensors, one can imagine many data collection practices by Amazon's drones that would raise privacy concerns and some that would be material to consumers. For example, if Amazon Prime Air drones are collecting information about activities going on in consumers' yards and using the data for purposes other than avoiding hazards—such as for advertising—consumers may be quite reluctant to use the product. Omitting information about what the drone can see and record, while constructing a constrained picture of its sight through the video's images, iconography, and narrative, could mislead consumers about the services impact on privacy. The combination of information about the drones' flight patterns and omitted information about the drone's data collection capacity and usage policies make it difficult for individuals to fully evaluate the impact of the service on their, and the public's, privacy.

Concept Videos as a Resource for Engaging in Values

Through our analysis of Amazon's concept videos, we sought to explore the interaction between public privacy discourse and product presentation. The exercise highlighted the role of concept videos as a site of inquiry and discourse, and led us to consider their utility as a method for engaging stakeholders in conversations about the impact of a product on values.

Concept videos often depict a technology still in the prototyping, development, or design stage. They place the technology in a fictional yet plausible scenario, providing viewers a sense of

what it might do, how it might interact in the world, and how people might interact with it.[31] We believe these videos, similar to other design methods and practices, can help viewers imagine possible futures and reflect on the values implications of technological and system design.

Members of the HRI community use design methods and practices, such as speculative design (Auger, 2014; Fernaeus, Ljungblad, Jacobsson, & Taylor, 2009), to understand the values present in design and design representations (e.g., Gaver & Martin, 2000; Pierce, et al., 2015). Speculative design uses design to ask questions and surface social issues rather than to identify or design specific solutions (Dunne & Raby, 2013). Designs in this context reflect a *range of possibilities rather than predicting a specific future outcome*. Design fiction, a practice related to speculative design, is described as existing between science fiction and science fact, using yet-to-be-realized design concepts to understand, explore, and question possible futures (Bleecker, 2009). Importantly, these design concepts are "diegetic," that is, they exist in a *fictional world or narrative* (Kirby, 2010; Lindley & Coulton, 2015). The focus is not just imagining a technical artifact but embedding that artifact in a broader world, story, or fictional scenario to think about the social implications and relations of the technology. Thus, design fictions embody values and ideas (consciously and unconsciously) that may respond to or instigate broader discourses (Tanenbaum et al., 2012). Recent work uses the lens of design fiction to *analyze* practices and artifacts (Tanenbaum et al. 2012; J. Tanenbaum, Pufal, & K. Tanenbaum, 2016; Wong & Mulligan, 2016). We take publicly released corporate concept videos to be a type of design fiction.[32] Placing concept videos in the realm of design fiction frames the video as something that is not predicting a singular future but presenting a representation of a possible future. Because design fictions are discursive, such videos are best considered in dialogue with broader social and policy discourses, such as privacy discourses.

Another line of work shows that *representations* of technology affect broader perceptions, reactions, and debate. Collective processes of imagination are expressed through and facilitated in part by processes of cultural production. For instance, Harmon and Mazmanian (2013) investigate the ways commercials and news articles create sociotechnical narratives about smartphones and smartphone users. Wong and Mulligan (2016) show how broader publics, such as journalists, perceive and react to concept videos' representations of future augmented reality technologies. Bell and Dourish (2007) explore how imaginations and narratives of ubiquitous computing create a shared narrative of the "proximate future," or near future. This narrative is embedded, expressed, and reinforced through the actions and products of researchers and practitioners in the field, as well as through cultural expressions of the future, like science fiction (Dourish & Bell, 2013). Representations of technologies influence the way people imagine future technologies, build broader collective narratives about what technologies mean, and influence actual technological development and use. Work by Jasanoff and Kim (2009) shows how these broader collective narratives about technology affect science and technology policy decisions. This suggests that we should not look at the concept videos' representations of technology in isolation but in relationship to broader discourses.

As robot technologies increasingly become more commonplace and interact with humans, the role of design and design methods gain importance for surfacing, and addressing humanistic and social issues related to HRI. Because robots will move, mingle, and interact with humans, the systems-level—rather than artifact-level—considerations enabled by concept videos may be a

[31] Other examples of concept videos include videos of Google Glass (viewable at https://youtu.be/9c6W4CCU9M4), Microsoft HoloLens (viewable at https://youtu.be/aThCr0PsyuA), as well as the two Amazon Prime Air videos discussed above.

[32] Under some definitions (e.g., Lindley, 2015), concept videos would be considered "incidental" design fictions, as compared to other design fictions which exist purely as fictional objects, such as designs in science fiction films. However, we find using the lens of design fiction to describe concept videos useful to understand the types of work these video fictions can do in provoking conversations about policy issues.

particularly appropriate and useful tool for identifying and addressing social and political concerns that may otherwise undermine robotic systems' utility and adoption. Concept videos may be a promising way to engage stakeholders in values analysis.

There are known limits to this type of video analysis, such as the gaps between portrayal and actual capabilities that we described above. Furthermore, from a video alone, it is difficult to know what the regulatory mechanisms underlying the drone's actions are and how limits to the actions are assured. Finally, concept videos may serve to normalize values that others may think are problematic; some may interpret the Amazon video as normalizing a particular definition of surveillance.

However, concept videos' usefulness, like design fictions, comes from their ability to elicit multiple interpretations, reflections, and questions. In the same way that speculative design seeks to ask questions, concept videos' representations of technology should not be seen as final design solutions but as a work in progress still amenable to change. While concept videos can respond to the concerns of policymakers and advocacy groups, concept videos can also provide a starting point for policymakers and advocacy groups to ask further questions in order to affect the changes they seek. They present one possible version of the future that others can critique.

Concept videos offer a conception of the experience of using a technology, which is much more difficult to convey through text, code, or static images alone. Ryan Calo (2012), writing in the context of privacy policies and notice, uses the term "visceral notice" to describe when users learn about a systems' behaviors by understanding what it is like to experience the system rather than by reading a textual description of the system. Concept videos can act as a type of visceral notice to end users, as well as policymakers and advocacy groups. The idea of learning by visceral notice becomes even more important in HRI, because few people have firsthand experiences interacting with robots or have mental models to understand what that interaction might be like. Concept videos provide a way to ground people's understandings of what it would be like to interact with that technology, and implicitly, allow people to think about the potential values tradeoffs in using such a technology.

In order to systematically think about values related to a new system represented in a concept video, policymakers, advocacy organizations, and other stakeholders can identify and interpret video elements by using the method outlined above. After identifying those elements, a number of further questions can be asked in order to surface potential values issues. We note that the following is not an exhaustive list and is likely to grow as concept videos are used to identify policy concerns beyond privacy.

How are technologies portrayed? This includes asking what the technical affordances are by drawing on technologies' behaviors, appearance, and place of operation. Where and when are technologies used? What is regulating the system? This might be a company policy, a piece of code, a design limit, or a physical limit. What types of controls and limits are in place? This asks how much control and input humans have or what types of options humans have in the operation of the system.

How are humans portrayed? How do they interact with the technologies? How are users portrayed? This draws on factors like behaviors, appearance, emotion, and setting to see what types of people are imagined to be interacting with the technology. Who are non-users, or users who are not portrayed? For instance, while the Amazon videos show us the package recipients' experience, we do not get to see the experience of the neighbors watching a drone fly over their house.

How is the sociotechnical system portrayed? How do humans and technologies interact? Who or what has agency over what parts of the system? Do the interactions address potential policy issues?

How has the portrayal changed over time? If there are multiple videos, changes may indicate shifts in design or shifts in the way people are thinking about the systems.

What is not portrayed in the video? The video provides one possible scenario that viewers can use as a starting point to begin asking further questions, including "what if" questions that examine alternate scenarios. For instance, what if the scenario presented in the Amazon video took place in an urban environment? What if the neighbor used geofencing technology to prevent a drone from flying overhead? What if the drone used sonar instead of computer vision techniques to identify potential obstacles? Or, what does Amazon's drone control center look like?

Analyzing concept videos to elicit concerns about a technology's potential impact on privacy or other values is useful in several ways. First, concept videos can be created and shared while a technology is still in development. Ideally, they would be created and shared in early ideation and design phases of a project. This would allow potential privacy concerns to be raised and addressed proactively during the design process.

Second, concept videos can act as a shared language among multiple communities. This is not dissimilar to other design representations, which help externalize and communicate ideas during the design process. One does not need an extensive technical background to understand, analyze, or question the content of a concept video. This makes it useful to share among groups within an organization, such as engineers, designers, lawyers, and business teams, as well as with outside policymakers and advocacy groups. Given these benefits of concept videos, they would fit well into a "privacy by design" regime to address privacy concerns during the design phase of products and to communicate attention to privacy to people within and outside of the organization. While these videos have the power to inspire the public imagination by providing a visceral experience of new technologies, care should be taken so that these video representations do not mislead consumers about the product's data practices.

Conclusions

In our analysis of Amazon's concept videos for its future autonomous drone delivery service, Amazon Prime Air, we have found that their concept videos acknowledge and address some of the privacy concerns raised in policy debates. Concept videos, which are representations and depictions of technologies, are also capable of representing and depicting values associated with and embedded in those systems. Concept videos are meant to be unfinished and imperfect. The recognition that the depicted technologies are not yet finalized allows people to ask further questions about the technologies and allows the company to address these questions and iterate on the design. We provide a systematic way to analyze concept videos' elements and have begun to develop lines of inquiry for policymakers, advocacy organizations, and other stakeholders to ask when reviewing videos in order to elicit values-laden questions. Using concept videos as a communicative tool with stakeholders who have policy and regulatory concerns about robotic systems but may not have the prior experience, mental models, or technical knowledge to properly analyze them would be useful for designers, businesses, and the HRI community. However, as robotic systems shift from fictional design ideas to real consumer products, such video representations take on new legal meaning and must avoid misleading consumers about material aspects of product functionality, including those related to privacy. As robotic systems increasingly interact with consumers and collect various types of data about them, regulators will increasingly look toward the privacy implications of those systems. Makers of systems can use concept videos to convey efforts to address privacy through design, rather than exclusively through legal disclosures. This may be particularly useful within a regulatory system that calls for privacy by design.

Given the dual nature of drones, and many other technologies that raise privacy concerns, a consideration of their privacy impact must examine their technical features as well as the context and constraints on their deployment. Earnest consideration of how products and services attend to privacy may increase the motivation of designers and deployers to protect privacy through technical and service design.

References

Amazon.com. (2015a). *Letter to Secretary Strickling re: UAS RFC 2015 – Docket No. 150224183-5183-01.* Retrieved from https://www.ntia.doc.gov/files/ntia/amazon_041915.pdf

Amazon.com. (2015b). *Hearing on unmanned aircraft systems: Key considerations regarding safety, innovation, economic impact, and privacy before the Subcommittee on Aviation Operations, Safety, and Security. Testimony of Paul Misener, Vice President for Global Public Policy, Amazon.com.* Retrieved from https://www.commerce.senate.gov/public/_cache/files/8711c6f8-cf1b-42b9-8ebc-26971c245f7f/0F6BCA396C06E03DC6750AD71F84B21D.amazon-misener-scc-testimony-032415.pdf

Auger, J. H. (2014). Living with robots: A speculative design approach. *Journal of Human-Robot Interaction*, *3*(1), 20-42. doi:10.5898/JHRI.3.1.Auger

Bell, G., & Dourish, P. (2007). Yesterday's tomorrows: Notes on ubiquitous computing's dominant vision. *Personal and Ubiquitous Computing*, *11*, 133–143. doi:10.1007/s00779-006-0071-x

Bleecker, J. (2009). *Design fiction: A short essay on design, science, fact and fiction.* Retrieved from http://drbfw5wfjlxon.cloudfront.net/writing/DesignFiction_WebEdition.pdf

California Code Sec. 1708.8 (2015). *Obligations imposed by law.* Retrieved from http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1708.8

Calo, M. R. (2011). The drone as privacy catalyst. *Stanford Law Review Online*, *64*, 29-33.

Calo, M. R. (2012). Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, *87*(3), 1027.

Center for Democracy and Technology. (2015). *CDT comments to NTIA on "Privacy, transparency, and accountability regarding commercial and private use of unmanned aircraft systems*." Retrieved from https://www.ntia.doc.gov/files/ntia/cdt_04202015.pdf

Cranor, L. F., & Reagle, J. (1998). Designing a social protocol: Lessons learned from the Platform for Privacy Preferences Project. In J.K. Mackie-Mason, D. Waterman (Eds.) *Telephony, the Internet, and the Media.* Routledge.

Cummings, R. (2015, Oct 26). Judge dismisses charges for man who shot down drone. *WDRB*. Retrieved from http://www.wdrb.com/story/30354128/judge-dismisses-charges-for-man-who-shot-down-drone

Dourish, P., & Bell, G. (2013). "Resistance is futile": Reading science fiction alongside ubiquitous computing. *Personal and Ubiquitous Computing*, *18*(4), 769–778. doi:10.1007/s00779-013-0678-7

Dunne, A., & Raby, F. (2013). *Speculative everything: Design, fiction, and social dreaming*. Cambridge, MA: MIT Press.

Dyer, G. (1982). *Advertising as communication*. London: Routledge.

Electronic Privacy Information Center (2015). *Comments of the Electronic Privacy Information Center to the U.S. Department of Transportation, Federal Aviation Administration*. Retrieved from http://www.regulations.gov/#!documentDetail;D=FAA-2015-0150-4314

Federal Trade Commission (1983). *FTC Policy Statement on Deception*. Retrieved from https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf

Federal Trade Commission v. Sterling Drug. 317 F.2d 669, 674. 2d Cir. 1963.

Fernaeus, Y., Ljungblad, S., Jacobsson, M., & Taylor, A. (2009, March). Where third wave HCI meets HRI: Report from a workshop on user-centred design of robots. In *Proceedings of the 4th ACM/IEEE International Conference on Human-Robot Interaction* (pp. 293-294). IEEE. doi:10.1145/1514095.1514182

Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems (TOIS)*, *14*(3), 330-347. doi:10.1145/230538.230561

Future of Privacy Forum (2015). *Letter to the National Telecommunications and Information Administration*. Retrieved from https://www.ntia.doc.gov/files/ntia/future_of_privacy_forum.pdf

Gaver, B., & Martin, H. (2000, April). Alternatives: Exploring information appliances through conceptual design proposals. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 209-216). ACM. doi:10.1145/332040.332433

Gellman, R. (2015). *Fair information practices: A basic history.* Retrieved from http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

Goldman, J. (2014, Sept 26). Man arrested after shooting down neighbor's remote control helicopter, cops say. *NJ.com*. Retrieved from http://www.nj.com/cape-may-county/index.ssf/2014/09/man_faced_with_gun_charges_after_shooting_down_remote_control_helicopter.html

Goodrich, M. (2016, Jan 7). Drone catcher: "Robotic Falcon" can capture, retrieve renegade drones. *Michigan Tech News.* Retrieved from http://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html

Hall, J. (2013, March 8). 'License plates' for drones? *Center for Democracy and Technology*. Retrieved from https://cdt.org/blog/license-plates-for-drones

Harmon, E., & Mazmanian, M. (2013). Stories of the smartphone in everyday discourse: Conflict, tension and instability. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1051–1060. doi:10.1145/2470654.2466134

Hoofnagle, C.J. (2016). *Federal Trade Commission Privacy Law and Policy*. Cambridge, MA: Cambridge University Press. doi:10.1017/CBO9781316411292

Hubers, A., et al. (2015, March). Video manipulation techniques for the protection of privacy in remote presence systems. In *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction Extended Abstracts* (pp. 59-60). ACM. doi:10.1145/2701973.2702048

Jasanoff, S., & Kim, S.H. (2009). Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva*, *47*(2), 119–146. doi:10.1007/s11024-009-9124-4

Kahn Jr, P. H., Ishiguro, H., Friedman, B., & Kanda, T. (2006, September). What is a human? Toward psychological benchmarks in the field of human-robot interaction. In *Proceedings of the 15th IEEE International Symposium on Robot and Human Interactive Communication (ROMAN).* (pp. 364-371). IEEE. doi:10.1109/ROMAN.2006.314461

Karol, T. (2015). *A compendium of state laws and proposed legislation related to unmanned aerial systems/drones*. Retrieved from https://www.ntia.doc.gov/files/ntia/publications/namic-ntia-drones_final.pdf

Kirby, D. (2010). The future is now diegetic prototypes and the role of popular films in generating real-world technological development. *Social Studies of Science*, *40*(1), 41-70. doi:10.1177/0306312709338325

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W.E. Bijker & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (225-258). Cambridge, MA: MIT Press.

Lessig, L. (2006). *Code version 2.0*. New York: Basic Books.

Lindley, J. (2015). A pragmatics framework for design fiction. *Proceedings of the 11th European Academy of Design Conference.* doi:10.7190/ead/2015/69

Lindley, J., & Coulton, P. (2015, July). Back to the future: 10 years of design fiction. In *Proceedings of the 2015 British HCI Conference* (pp. 210-211). ACM. doi:10.1145/2783446.2783592

Mulligan, D. K., & King, J. (2012). Bridging the gap between privacy and design. *University of Pennsylvania Journal of Constitutional Law*, *14*(4), 989.

National Conference of State Legislatures (2016, January). *Current unmanned aircraft state law landscape*. Retrieved from http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx

National Telecommunications & Information Administration. (2015, November 20). *Multistakeholder process: Unmanned aircraft systems.* Retrieved from https://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-unmanned-aircraft-systems

National Telecommunications & Information Administration. (2016, June 21). *Voluntary best practices for UAS privacy, transparency, and accountability*. Retrieved from https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford University Press.

Okla. S.B. 492, 55th Leg., 1st Sess. (2015). Retrieved from http://www.oklegislature.gov/BillInfo.aspx?Bill=SB492&Session=1500

Pierce, J., Sengers, P., Hirsch, T., Jenkins, T., Gaver, W., & DiSalvo, C. (2015, April). Expanding and refining design and criticality in HCI. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2083-2092). ACM. doi:10.1145/2702123.2702438

Ramey, A., & Salichs, M. A. (2014, March). Morphological gender recognition by a social robot and privacy concerns: Late breaking reports. In *Proceedings of the 2014 ACM/IEEE International Conference on Human-Robot Interaction* (pp. 272-273). ACM. doi:10.1145/2559636.2563714

Reason-Rupe (2013). *Public opinion survey: February 2013 topline results*. Retrieved from http://reason.com/assets/db/13620384648046.pdf

Rose, G. (2007). *Visual methodologies: An introduction to the interpretation of visual materials* (2nd ed.). London: Sage.

Rubinstein, I. (2012). Regulating privacy by design. *Berkeley Technology Law Journal*, *26*, 1409.

Sengers, P., & Gaver, B. (2006, June). Staying open to interpretation: Engaging multiple meanings in design and evaluation. In *Proceedings of the 6th Conference on Designing Interactive Systems* (pp. 99-108). ACM. doi:10.1145/1142405.1142422

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880-1903.

Surden, H. (2007). Structural rights in privacy. *Southern Methodist University Law Review*, *60*, 1605-1629.

Takahashi, T. (2012). Drones and privacy. *Columbia Science and Technology Law Review*, *14*, 72-114. doi:10.2139/ssrn.2035575

Tanenbaum, J., Pufal, M., & Tanenbaum, K. (2016, June). The limits of our imagination: Design fiction as a strategy for engaging with dystopian futures. In *Proceedings of the Second Workshop on Computing Within Limits* (p. 10). ACM. doi:10.1145/2926676.2926687

Tanenbaum, J., Tanenbaum, K., & Wakkary, R. (2012, May). Steampunk as design fiction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1583-1592). ACM. doi:10.1145/2207676.2208279

Texas Code Sec. 423.003 (2015). *Offense: Illegal use of unmanned aircraft to capture image*. Retrieved from http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.423.htm#423.003

Wingfield, N. & Sengupta, S. (2012, February 18). Drones set sights on U.S. skies. *The New York Times*, pp. A1. Retrieved from http://www.nytimes.com/2012/02/18/technology/drones-with-an-eye-on-the-public-cleared-to-fly.html?_r=1

Winner, L. (1980). Do artifacts have politics? *Daedalus*, 121-136.

Wisconsin Statute 942.10 (2013). *Use of a drone*. http://docs.legis.wisconsin.gov/statutes/statutes/942/10

Wong, R. Y., & Mulligan, D. K. (2016, June). When a product is still fictional: Anticipating and speculating futures through concept videos. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (pp. 121-133). doi:10.1145/2901790.2901801

R. Y. W., School of Information, University of California, Berkeley, USA. Email: richmond@ischool.berkeley.edu; D. K. M., School of Information, University of California, Berkeley, USA. Email: dkm@ischool.berkeley.edu