Data and Privacy in a Quasi-Public Space: Disney World as a Smart City

Madelyn Rose Sanfilippo[1][0000−0002−7705−6753] and Yan Shvartzshnaider[2,3][0000−0001−5954−916X]

[1] University of Illinois, Champaign IL 61820, USA
madelyns@illinois.edu
[2] NYU, New York, NY 10012, USA
[3] York University, Toronto, ON M3J1P3, Canada
yansh@yorku.ca

Abstract. Disney World has long been at the forefront of technological adoption. Walt Disney theme parks implement emerging technologies before other consumer or public spaces and innovates new uses for existing technologies. In contrast to public contexts with representative governance, Disney World is both a prototype and a functioning quasi-public smart city, wherein a private actor controls ICT adoption and data governance. As cities increasingly partner with private corporations in pursuit of smart systems, Disney provides a glimpse into a future of smart city practice. In this paper, we explore normative perceptions of data handling practices within Walt Disney World and discuss contextual differences from conventional cities. We consider what can be learned about privacy, surveillance, and innovation for other public applications, stressing the limitations of and potential social harms from Disney as a model for public services.

1 Introduction

Over the years, Walt Disney World (WDW) has innovated and employed emerging and futuristic technology to realize the "great big beautiful tomorrow, shining at the light of every day" [2]. Walt Disney envisioned the Experimental Prototype Community of Tomorrow (EPCOT) as the first smart city, though that label did not yet exist [16]. He envisioned that "[EPCOT] will take its cues from the new ideas and new technologies that are now emerging from the creative centers of American industry. It will be the community of tomorrow, that will never be completed" [5].

With the adoption of emerging technologies in WDW and other public spaces, critics have raised a number of privacy concerns.

Privacy is often rhetorically positioned in false trade-offs with efficiency and convenience, and thus sacrificed in favor of commercial over human interests. This results in potentially serious social repercussions and inequities [10], both within and between smart cities. Some smart cities' governance is purely public,

drawing on community feedback and preferences through processes that incorporate many stages of revision, such as Seattle [1]. Other cities, such as Toronto [9], increasingly contract private partners to implement smart systems with varying degrees of transparency and consistency. It is difficult to predict outcomes for any specific smart city. Each path brings different governance models and decision-makers, in addition to local values, norms, harms, and benefits.

As cities pursue smart systems, in partnership with private companies, they evolve into quasi-public spaces. As an early adopter of numerous technologies, WDW provides useful perspective on the interplay among technology, people, and institutions in a context that narrowly represents the economic interests of private decision-makers and consumer preferences. In this context, individuals are pervasively quantified and surveilled, without consideration for broader social norms, rights, equity, or human autonomy.

In this paper, we examine WDW as a case study to explore both normative and institutional information governance challenges associated with: pervasive location monitoring, facial-recognition, data integration across contexts, and the seamlessness of smart experiences and interactions. Our analysis of WDW highlights a number of challenges, identified in terms of normative disagreement over particular smart systems between Disney and consumers, as well as with the general public. We discuss implications for technological adoption, including facial recognition, biometrics, and smart transportation systems, emphasizing that respecting privacy norms is important to retaining rights in smart urban environments. Further, we highlight the importance of feedback mechanisms on privacy norms and seamlessness in sociotechnical systems.

2 Background

An emerging body of scholarship employs institutional analysis to explore technology governance in public space, as way to complement existing legal and normative frameworks [8]. The governing knowledge commons (GKC) framework, built on institutional analysis approaches originating with Ostrom, facilitates descriptive and structural analysis of complex, layered, localized, and hybrid governing institutions around data, information, and technology. To address questions around privacy relative to public technology, recent studies integrate GCK with the contextual integrity (CI) framework [22], considering privacy as an appropriate flow of personal information [17], in order to address questions around privacy relative to public technology.

In this section, we provide an overview of: 1) governance of technological systems in public and quasi-public contexts, 2) privacy and security in smart cities, and 3) WDW as a smart city and a comparatively early adopter.

2.1 Technology Governance in Public

Privacy in public is essential to: individual autonomy, the relative invisibility of being one among many, safety in numbers, and the possibility of disinhibition within collective behaviors or experiences.

US law makes relatively clear distinctions between public spaces and the home, as a private space, dating back to *Bell v Maryland*, there is also a grey area. Quasi-public contexts, such as malls, airports, and amusement parks are privately owned and open to the public, as legally defined hybrid contexts [3]. Increasingly, these quasi-public contexts are privately policed and subject to significant surveillance, without public oversight or protections [3].

Quasi-public spaces raise numerous governance questions about the legitimacy of institutions, decision-making, and information flows in public-private partnerships in smart cities. As these technologies and systems are deployed, the implications of governance, relative to privacy, in public and quasi-public spaces, are becoming ever significant, particularly around questions of transparency. Important elements of governance in public spaces include: accessibility, understandability, and representativeness of the interests of the general public, both normatively and democratically [11,13]. The visibility and invisibility of these systems, which we discuss in the next section, is important relative to public expectations [6,17].

2.2 Privacy, Surveillance, and Smart Cities

Smart cities are arrangements between people, technology, and institutions. Smart cities are shaped by aspirational futurism and through socio-technical engineering, pursuing innovation, with little time dedicated to issues of privacy, socially normative expectations, or governance [7,15,26]. We define smart cities as public, semi-public, and quasi-public spaces in which information technologies provide feedback mechanisms or services enhanced beyond delivery.

Local trends in governance are just as important as trends in technological innovation, both to understand what is possible and what ought not to be replicated [20]. Privacy localism [21,20] manifests as governance or practices at the levels of states or regions, broadly, as well as in individual cities or neighborhoods. Notions of contested privacy in specific neighborhoods–as individuals negotiate how far the privacy of one's home extends and the extent to which neighborhoods are public or private [18] –illustrate the complexity and nuance of context.

The way we govern privacy, personal data flows, and data within social spaces illustrate the significance of learning from micro-level cases. This is particularly true around quasi-public spaces, where large populations of people interact, and in densely-populated urban areas that rush to transform into "smart-er" cities [26]. The notion of "Urban privacy," which integrates privacy in public with the normative frame and expectations of urban spaces [19] can help address the challenges of privacy governance in these spaces.

2.3 WDW as a Smart City

Immersive Disney spaces embrace techno-futurism, embedding innumerable data collection points throughout engaging experiences and pedestrian spaces. WDW has adopted many technologies and smart systems in a quasi-public space, prior

to other applications in public. WDW was one of the earliest commercial applications of CCTV digital multiplexing to scale [4]; CCTV represents one of the first technical applications of pervasive surveillance in both Disney stores and parks. Before diving into the case study, we articulate the ways in which WDW is a smart city and the ways in which it compares to purely public smart cities or other conventional public spaces.

First, WDW is a quasi-public place, in which a private actor controls a large space open to consumers from the general public. Second, Disney is a quasi-public smart city that employs numerous digital technologies and multiple networks of sensors to enhance services and experiences, as well as to provide feedback. Under our definition, the relationships between people, technology, and institutions within Disney spaces constitute a quasi-public smart city, yet there are many contextual differences that clearly delineates appropriate conclusions from this study. In comparison to fully public contexts or public-private partnerships in other smart cities, WDW is distinct not only in private control and decision-making, but also due to normative distinctions, differences in objectives, and the unique history of Disney as a planned space.

Normative differences are rooted in context and interests; cities address social needs of local populations, while Disney is a commercial purveyor of entertainment. Intentional and planned spaces are also distinctly different from other public and urban spaces. Disney is similar to other quasi-public spaces and intentional communities, such as Irvine, CA which was thoroughly planned and engineering in pursuit of normative values that have shaped development and human interactions over time [12]. Governance implications for adoptions of parallel systems, in other, non-WDW, contexts and for distinct purposes, come with significant caveats. Despite status as an early adopter and characterization of WDW as a prototype smart city, outcomes and benefits may not compare between quasi-public spaces and conventional cities.

3 Methodology

The case study of WDW, as an early adopter of new technologies, examines implications of public-private partnerships in emerging smart cities. We empirically explore: cross-context data integration in practice at WDW, data collection and processing, social perceptions of privacy practices, and lessons about practice and governance from Disney.

We frame our privacy analysis of WDW information handling practices in terms of the contextual integrity (CI) framework. The CI framework captures information flows and norms using 5 essential parameters: senders, subjects, receivers of the transmitted information, type of information and transmission principle, which specifies the constraints imposed on the information flow.

We structured our analysis of norm formation, divergence in preferences among community members, and governance in effect, using the governing knowledge commons (GKC) framework [8]. GKC applies institutional analysis, includ-

ing an underlying grammar to structure coding of strategies, norms, and rules, to the context of data, information, and technology as resources [22].

3.1 Empirical Assessment of Privacy Polices

Guided by the CI framework, we annotate words in each privacy statement matching CI parameters that prescribes information exchange and handling practices, as proposed in [24]. We then list all the prescribed information flow by a given statement. For example, the statement:

> We collect information using analytics tools, including when you visit our sites and applications or use our applications on third-party sites or platforms

prescribes a number of potential information flows. We can observe "Disney" as a recipient of the information, however, the statement omits several relevant parameters, namely, the type and subject of the information, and the sender of the information. The statement does include transmission principles, i.e. the two conditions under which the information is facilitated, which results in multiple potential information flows: when users visit the sites, when users using the apps, when users browse third party sites, and when users visit third party platforms. In our analysis, we compare each of the possible information flows to existing institutions to identify potential privacy violations or non-conformance to established practices.

3.2 Empirical Assessment of Surveillance and Perceptions

To empirically assess the prevalence and visibility of data collection within WDW, we systematically counted and categorized clusters of sensors that interact with apps and MagicBands, as well as cameras. We differentiate between visible sensors that visitors intentionally swipe their phones or MagicBands and those that are not transparently labeled or visibly identified. Sources for this analysis included official Disney blogs, coded and analyzed through content analysis, and the My Disney Experience app, through which we manually counted the sensors, identified by individual geo-located tags on embedded maps.

We evaluated stakeholder perceptions about technologies and information flows at WDW through sentiment analysis of text discussing privacy and data collection systems, as captured from blog posts. For this analysis, we differentiate between content: directly from Disney, endorsed by Disney, and Disney consumers and users of Disney systems. The first two categories were identified from Disney resources. To generate the third set of blogs, we identified the top 100 Google Page Rank results for "Disney blog", that: had at least 100 posts total, post at least once per month on average, and a disclaimer differentiating the blog from the Walt Disney Company. We examine these blogs as representations of Disney consumers and users of Disney systems, rather than as independent perspectives from the general public. A Python script collected a total of 12506

posts, from 112 blogs, that included keyword sets associated with systems of interest. This collection strategy included many false positives, which were then manually discarded by the investigators, as posts were further classified and tagged within NVivo.

Data were processed and modeled within R, using the packages: textclean, to normalize punctuation; tidytext, to format normalized posts in comparable units of analysis and assess word counts and frequency; SentimentAnalysis, to assess polarity, including in proximity to a custom dictionary that focuses on the technologies and information flows of interest; and sentimentr, to aggregate and compare sentiment measures. We measured the significance of differences in sentiment using Welch's t-tests, as the most accurate and effective measures given the characteristics of the blog post data set [23], and then noted confidence intervals for measures of polarity. For further reference, we included a table of reviewed blogs/posts considered in this study in this repository.

4 Analysis

This section: identifies key issues around information flows at WDW, presents an ontology of community members, analyzes their perceptions of specific systems, and examines WDW privacy policies and communications that inform consumer expectations.

4.1 Surveillance and Information Collection

User and behavioral data are critical information resources, from an institutional perspective. This is especially true at WDW, which employs a massive network of sensors and cameras across multiple systems to understand, predict, and influence consumers and throughout WDW. This includes documenting individuals': steps taken, time browsing shops, food and souvenirs purchased, lines waited in, and entertainment or attractions engaged with. Figures 1 and 2 illustrate the overall scale of this data collection across the four distinct theme parks within WDW, other public spaces at WDW, and WDW resorts as counts of the number of sensor clusters visitors actively connect with by categories of interaction.

Visible Collection. Highly visibile data collection at WDW includes ticket and security screenings at park gates. People knowingly wave their magic-bands over silver Mickey-shaped sensors when they enter the parks or their hotel rooms, which light up to indicate authentication. People actively scan their bands in the Fast-Pass system, have their picture taken, or make purchases. They download and engage with immersive apps to augment experiences throughout the parks. The aggregate scope of this visible, participatory data collection is immense and not always obvious. Many active interactions visitors have with sensors are unobtrusive, despite the transactional nature. Yet, many interactions are designed to seamlessly minimize visibility.

Seamless Collection. Seamless data collection includes step tracking and most security cameras, as well as complex cross-function and multi-use systems. The My Disney Experience and the former Shop Disney Parks apps make suggestions about things individuals looked at, but didn't buy, or where they could find souvenirs associated with favorite rides and characters. These recommendation systems connect digital platforms and the physical world, in real time.

MagicBands MagicBands and step tracking represent newer streams of data collection about visitors, with many similarities to fitness trackers. MagicBands collect location data both through active (e.g. point-of-sale) and passive interaction (e.g. sensors, triangulation) [25]. The integrated MagicBand systems function based on the same RFID technology as luggage tracking, representing the first deployment of wearable RFID for the general public. Embedding RFID within Disney spaces allowed the MagicBands to integrate relatively seamlessly with many existing systems.

MagicBand sensors are pervasive all over the resort and theme park spaces, some unobtrusive, or even invisible. Invisible sensors are used both for tracking and engagement; for example, many attractions identify individuals' names via invisible sensors to greet them or personalize interactions. Figures 1 2 illustrate data collection via MagicBands, in which information flows are visible to visitors through their active engagement with these sensors, yet these represent the tip of the data iceberg. Sensors are relatively equally distributed across parks and categories, with most MagicBand interactions within customer service or through guest services staff (Figure 1). However, there are significant differences between data collection within the amusement parks and other public contexts, including water parks or shopping areas, and hotels (Figure 2), where guest services have greater prevalence and some categories of MagicBand interactions are non-existent. Customers view the parks and hotels as different contexts.

Apps. Apps provide another major means of data collection about park visitors, as well as the wider population of Disney customers. In addition to individual apps tailored to each Disney Park worldwide, the My Disney Experience app, and a Disney transportation app, there are various consumer directed apps like Disney+, Play Disney Parks, and a Shop Disney app. Data from these apps are integrated with other systems to assess traffic and interaction with various features in and across the parks.

Overall there are fewer location-based interactions via app than via MagicBands. Apps' location-based interactions are either enabled through smart phones' GPS capabilities or through proximity-based Bluetooth. The Play Disney Parks app directly integrates location data and behavioral data about children, as a protected population, with data from other sensors and systems within the park. Yet, this app does not have a unique privacy policy, despite its target population and leveraging permissions the following permissions: camera (take pictures and videos); approximate location (network-based); precise location (GPS and network-based); storage and photos/media/files (modify, delete, or read USB contents); view Wi-Fi connection information; download files without notification; receive data from Internet; view network connections; prevent

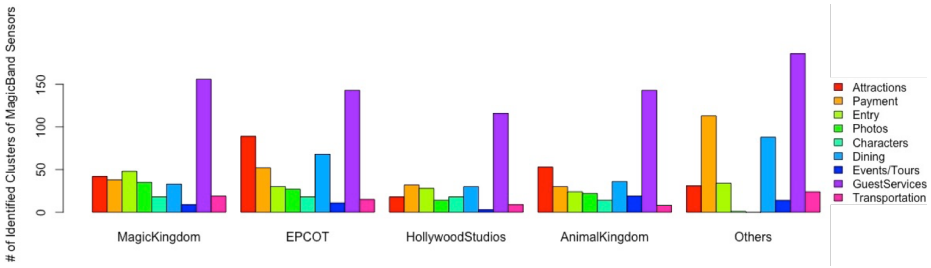

Fig. 1. Active Engagement MagicBand Sensors in 4 Disney Theme Parks and Other Quasi-Public Spaces at WDW

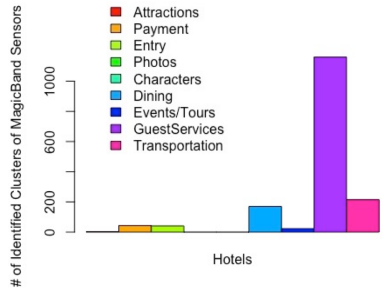

Fig. 2. Active Engagement MagicBand Sensors within Disney Hotels

device from sleeping; read Google service configuration and check Google Play license; run at startup; pair with Bluetooth devices and access Bluetooth settings; full network access; toggle sync on and off; use accounts on the device; control vibration; and connect and disconnect from Wi-Fi.

Cameras. An extensive network of cameras facilitate a major means to collect data resources within WDW. Specifically, in addition to CCTV surveillance, there are a number of other unobtrusive cameras in quasi-public spaces, including those on rides or within attractions to capture the "action" and visitors at play. Some of these unobstrusive cameras are considered "automatic photographer machines." Automated photographers are distinct both from human photographers with cameras, who roam the parks, and surveillance cameras, for which footage and images are not distributed to visitors via any of their photography packages, such as PhotoPass, or accounts. The Disney Parks app does provide maps indicating how widely distributed these cameras are throughout the parks and where these systems are located, yet these cameras cannot be identified without searching the map.

Further, there are also visible cameras that document visitors during character interactions or photo opportunities that consumers knowingly choose to interact with. Sometimes, these cameras are accompanied by photographers or other humans in the loop, who link photos to individuals via their MagicBands. In other instances, however, photos are connected with individuals' accounts via facial recognition, to varying degrees of success.

4.2 Community Member Ontology

Relevant community members and stakeholders in the WDW case have distinct relationships to and with Disney, as well as interests associated with governance issues. Despite individuals' unique preferences, stakeholder groups' consensus on particular values and objectives are reflected in governance processes and outcomes.

Within the Disney organization diverse role-based groups–including approximately 70,000 union, salaried and non-union hourly employees at the Disney Parks without decision-making roles–span: interns, imagineers, cast members, musicians, a business office, and management roles, as well as many Disney subsidiary organizations. A major proportion of those hourly, non-unionized employees–who number approximately 43,000 employees–include veterans who fill security roles within the Disney parks.

Outside of the Disney organization, there are two distinct groups: (1) individual visitors and (2) business and organizational partners. First, among visitors, different stakeholder groups are represented, including: those associated with conferences and events, families with children, multi-generational families, local visitors versus tourists, adults without children, individuals with disabilities, techno-futurists, and military families. Second, businesses and organizations that partner with Disney, provide services or in supply chains, have very distinct interests and influence privacy and surveillance practices. Given the limited transparency about some of these relationships, their outsize influence on and role in data governance is likely to be surprising to many visitors. Third parties, completely distinct from the multifaceted Disney organization, include: Lyft, TSA, the Orlando International Airport (MCO), and the City of Orlando, who partner to provide smart transportation solutions and safety throughout transit; various hotel chains in and around Disney parks, specifically including joint properties with Marriott and the Four Seasons; and consumer products and retailers, including Ziplock, Target, AppleMusic, and ACE.

4.3 Stakeholders Perceptions

In order to understand the current state of governance around surveillance and personal data at Disney, it is important to have a sense of how goals and objectives diverge among stakeholders. We analyzed the perceptions of (a) visitors and Disney enthusiasts, (b) bloggers endorsed by Disney, and (c) the Disney organization on key governance issues around privacy and surveillance. Figure 3 illustrates perceptions of specific technological systems as polar sentiment expressed, noting significance via confidence interval error bars.

Perceptions of specific systems vary across these three stakeholder categories, with the greatest consensus demonstrated through comparably positive language employed to discuss apps, smart transportation systems, and voice recognition. Those individuals whose blogs are endorsed by Disney, unsurprisingly, generally frame their views more similarly to official Disney accounts, than to consumers.

The most notable disagreements fall in framing of biometric technologies and facial recognition in WDW. Additionally, while endorsed blogs and official Disney blogs frame MagicBands and Smart Locks in similarly positive ways, mimicking the common divide between these groups and the broader population of users and visitors. Endorsed blogs describe recommendation systems and smart planning tools in similarly somewhat positive language to consumers, while Disney officially frames these technologies using more positive language.

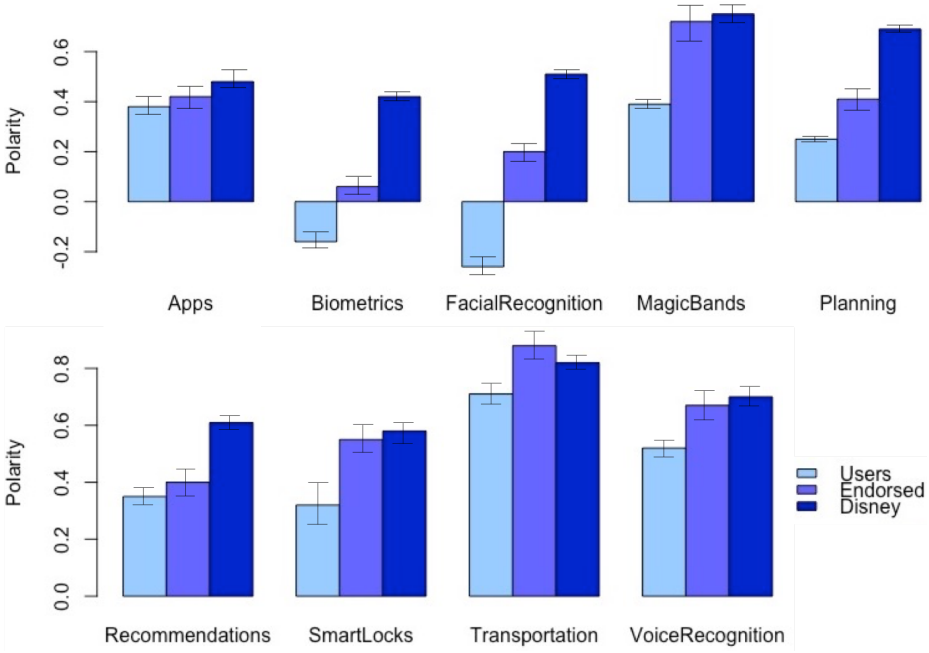

Fig. 3. Community Member Perceptions of WDW Smart Systems

The dataset did not include any posts expressing concerns about privacy or data governance associated with the application of facial and voice recognition technology in engaging and interactive attractions geared toward children, though there were blog posts analyzing and articulating the technological design. In contrast, some blogs about immersiveness, seamlessness, and recognition technologies outside of attractions express hesitation and concerns about whether people understand "concern over privacy," particularly with MagicBands outside of rides. This suggests a distinction between rides and more general experiences at WDW, within the minds of visitors.

Official Disney dialogue prioritizes security over privacy. Disney offers compelling and well packaged arguments about safety and security, while assuring visitors and readers, in vague terms, that biometric and surveillance data will

be "secure." They do not discuss privacy or trade-offs made, leading to the very positive polar sentiments documented in Figure 3. Language used around safety and security is also very assertive and positive in tone to communicate why visitors should trust them and need not worry.

Endorsed perspectives are similarly very positive overall; they communicate their trust in Disney and positive experiences, without interrogating trade-offs between privacy and security. Perspectives from parents and Disney youth and Disney marathon runners often continue to focus on their positive experiences, even when faced with questions about privacy or skepticism about public safety. For example, a question posed to the Disney Parks Moms Panel by a general visitor focused on biometric privacy: "Are fingerprints stored to your name or just to your MagicBand"? The response was framed in terms of safety and security; the only mention of privacy was in the link to the Walt Disney company's privacy policy.

The greatest disagreement between Disney and endorsed perspectives is about biometrics, when exploring these posts in aggregate. The general public frames biometrics and facial recognition as slightly negative, although their views of systems in aggregate are slightly positive, as depicted in Figure 3; their views on safety and security as broad action arenas are very fragmented. Safety and security objectives are meaningful and important, given that there are so many children in these spaces; these objectives are well met. This gives people a sense of safety and many blogs discuss the same incidents in which security and surveillance identified individuals with handguns and prevented them from entering the parks.

Yet, there are, sometimes explicit, questions about whether there are more privacy preserving ways to manage these data flows. Many blog posts discuss or hint at privacy tensions, with most expressing uncertainty (e.g. "...though I don't know if..." or "I'm not really sure how..." data is stored or protected). While journalists have directly questioned data retention [14], bloggers suggest similar concerns in discussing long term tracking around MagicBands, including that they " don't expect to continue being watched... after [they] go home." Further, bloggers express greater trust in Disney than in privacy or security of technology in any context, including Disney technology. Similarly, consumers question the increasing presence of security personnel in these spaces, with third-party "back-up" from "more uniformed and plain-clothes police officers, security guards, and dogs patrolling the parks" at particularly busy times of year. In this sense, despite Disney's apparent trustworthiness, consumers don't necessarily trust Disney's third-party partners or understand the nature of those relationships around privacy and security.

4.4 Privacy Rules-on-the-Books

In this section, we present our analysis of information flows prescribed by the privacy policies and as explained to customers.

Given the large scope of the Walt Disney Company and diversity of subsidiaries, the privacy policy is highly generic and and lacks detail about data

handling practices. For example, what types of information are collected is never disclosed, much less in what context or through what system. Disney's privacy policy describes practices in a general sense, only offering more details on what information is collected, processed and shared while engaging with Magic+ services (including MagicBands) in a separate, non-contractually binding My Disney Experience – Frequently Asked Questions (FAQ) page [27]. Many WDW information handling practices are performed without any meaningful user consent or rules guaranteeing consistent practice.

Although the privacy policy states that Disney collects information from visitors/users during any interaction with their devices or services, such as purchasing products or surveys, it omits what type of information is collected or about whom. It is ambiguous whether data collected is about the user, the account holder, or any other associated accounts or relatives. Not only are children included on accounts or able to access services through their parents' accounts, but accounts are also linked by design, for family reunions or school field trips. The FAQ fills in some of the details: "Your interactions provide us with information about the products and services you experience in the Parks; your wait time for rides, restaurants and other attractions; and similar types of information." From this, non-binding, statement, the implication is that data collection extends far beyond account holders and pertains to all interactions users and visitors have with Disney platforms or parks.

Similarly, Disney collects information "whether or not [users] are logged in or registered." Pervasive surveillance is implied by the privacy policy; information is acquired from other sources to "to update or supplement the information provided." An FAQ expands: "We also collect certain information from you while you are at select locations throughout the Resort through means other than the My Disney Experience website or mobile app. When you use your RF Device at touch points (e.g., for Disney Resort room entry, park admission, FastPass+, and purchases at select Resort locations), we are able to record your transaction and, when necessary, make the appropriate adjustment to your account."

Aggregation is as pervasive as surveillance and notably crosses contexts. The Disney privacy policy mentions using information for: personalization, optimization, and improvement of their services, as well as for targeted advertising. The policy lacks details on what type of information is shared, with whom, or under what conditions. Again, FAQs provide further details: "We will only share information about you that is collected automatically when your MagicBand is read by long-range readers with third parties for their marketing uses if you elect that we do so." This implies opportunities for users to opt-in to marketing uses, without making clear how or when.

The WDW case illustrates how informed consent, in its current form, through privacy policies can be reduced to a meaningless artifact from the general public point of view and a power manipulation tool on behalf of large corporations, like, Disney. For a privacy concerned member of the community it is extremely difficult, if not impossible, to understand precisely what type of information flows, to whom, about whom or what, and under what conditions. To piece this

information together, the reader is expected to follow countless links, read length documents only to end up with an incomplete picture. The FAQ might seem to be a useful gesture on behalf of the company to help a concerned member, by providing more details and concrete scenarios, yet, it is not legally binding and is often as vague and incomplete as the privacy policy.

5 Discussion

In this section, we discuss potential implications of Disneyfication of smart cities. We identify lessons to be learned from WDW in comparison to adoption of new technologies, based on commercial interests and with private sector partners.

5.1 Lessons for Technological Adoption

As documented in Section 2, many of the technologies used at WDW, are ultimately integrated in smart cities and public spaces.

Facial Recognition. The use of facial recognition technologies is increasingly under public scrutiny. To address issues of concern to visitors, such as imprecision and bias, Disney maintains humans in the loop and triangulates against other data sets, such as to reunite children separated from their families. This illustrates a mechanism to address issues similar to those experienced in applications of facial recognition in quasi-public spaces, such as university campuses. However, humans in many contexts may provide other avenues for bias to creep in and claim justification through these systems. In this sense, an attempt to replicate this sociotechnical application of facial recognition would not translate to every context and would require critical evaluation of norms and expectations, prior to implementation.

Biometric Tracking. While Disney was first to employ biometric access for large public populations, the technology had long been perfected for access control to secure military bases and national laboratories. Yet the contexts have very different implications for stakeholder perceptions of appropriateness. Various blog posts analyzed were quick to explain that the data collected at the gates to Disney parks is not shared with law enforcement, unless legally obligated. These discussions reveal that Disney customers are more trusting of private corporations like Disney, with respect to their personal data, including fingerprints, than they are trusting of the government. There are significant issues of trust that must be overcome before employing fingerprint scanners in other public spaces and also appears analogous to trust issues associated with contact tracing.

Despite the parallel technological systems between urban public spaces and WDW as a quasi-public space, there are meaningful differences between private and public infrastructure with respect to: representation, inequality, values, and trust.

A major distinction between Disney and smart cities relates to community member perceptions of and trust in decision-makers by other stakeholders. Technologies do not operate in a vacuum, but rather are used and governed by people

with distinct interests, needs, and expectations in particular contexts. Systems are not transferable with parallel outcomes across contexts.

5.2 Seamlessness in Sociotechnical Systems

Ubiquitous data collection quickly and seamlessly became integral defaults at WDW, challenging norms in absence of meaningful alternatives. As so often happens in techno-socially designed systems, analog alternatives diminish the quality of experience and are presented as a less attractive option, with time consuming procedures, little information, and reduced priority. For example, one may opt for an analogue ticket or not to use an app, but then is ineligible for particular experiences or must wait in stand by lines. Disney follows a worrisome trend, presenting false trade-offs between information collection and quality of service. Given the relationships between Disney and guests, as well as the success of Disney nudges in numerous contexts, opt-in would also likely work as well. This should serve as a warning to smart city advocates that face a much more challenging task relative to "opt-in" options.

Another increasingly common practice is the use of social nudging. Based on our analysis of blog posts, consumers seem to be more comfortable with nudges from Disney than other commercial partners, yet these consumers do not represent the general public. Nudges to encourage opting-in, when made by cheerful Disney characters are likely to be perceived as much less sinister than those from police officers. However, opting-in to data collection at WDW versus by law enforcement, within smart cities, are more similar in effect, than individuals realize, given the relationships between law enforcement and Disney. The implications of these information flows are thus, similarly problematic, particularly in an age where mistrust of law enforcement is increasingly pervasive.

Overall, WDW and smart cities represent different contexts with distinct system functions, perceptions of systems, values, and stakeholders' trust in decision-makers. Disney's data handling practices, generally align with consumer expectations–whether organically or due to extensive marketing–yet, many of their practices are inappropriate for publicly-accountable smart cities. While WDW functions as a smart city, it reflects very distinct norms, patterns of decision-making, and consumer preferences, rather than public needs. Even as cities partner with private sector firms, they should not assume that they can imitate Disney. Instead, they should likely question if those partnerships are appropriate and consider what types of governance are necessary to engender trust in decision-makers, data, and practices.

6 Conclusions

This paper examines normative perceptions of privacy, surveillance, and innovation in a case study of an emerging smart quasi-public space. Using WDW as our prototype smart city, we empirically compare two possible modes of governance: WDW's quasi-public model and conventional cities' publicly accountable

model. We further identify the limitations and potential social harms of Disneyfication of conventional cities and the importance of contextual norms in cross-context data integration, data collection, and processing practices involving public-private partnerships. What is normatively appropriate for WDW is likely not appropriate for Oakland or New Orleans, just as what is appropriate for Atlanta is not necessarily right for Seattle.

Our institutional analysis shows the extent of data collection strategies in contrast with: normative customer perceptions and expectations; underlying trade-offs, marketing slogans, and corporate values; and privacy policies regarding data collection and sharing. While generalizability of this study is limited, by our focus on Disney and its consumers, as opposed to the general public, this highlights an important lesson: privacy is contextual. We also find that Disney illustrates two important procedural approaches to governance: the use of detailed social surveys to understand expectations, and a commitment to iterative reevaluation, including for negotiation of legitimate practices and information flows. Smart cities and other public contexts need to foster dialogue between all stakeholders even if they are not all involved in decision-making. Future studies of privacy governance in smart cities should explore feedback and evaluation mechanisms to better reflect local values and norms.

In her book *Privacy in Context* [17], Nissenbaum warns us of the "Tyranny of the Normal." Without careful analysis and consideration of harms and benefits of these practices, by the time we detect resulting raptures in social and cultural values, it might be too late, because "the new normal may be comfortably entrenched, but far from comfortably accepted". In this sense, other smart cities and public contexts should take caution in learning from WDW before citizens, too, become products and local governance is delegitimized.

References

1. AlAwadhi, S., Scholl, H.J.: Aspirations and realizations: The smart city of seattle. In: 2013 46th Hawaii International Conference on System Sciences. pp. 1695–1703. IEEE (2013)
2. Allen, R.: There's a Great Big Beautiful Tomorrow. Walt Disney (1964)
3. Button, M.: Private security and the policing of quasi-public space. International journal of the sociology of law **31**(3), 227–237 (2003)
4. Coleman, R., Sim, J.: From the dockyards to the disney store: surveillance, risk and security in liverpool city centre. International Review of Law, Computers & Technology **12**(1), 27–45 (1998)
5. Disney, W.: Epcot / florida film (1966), `https://www.youtube.com/watch?v=sLCHg9mUBag`
6. Ekbia, H., Nardi, B.: Heteromation and its (dis) contents: The invisible division of labor between humans and machines. First Monday (2014)
7. Elmaghraby, A.S., Losavio, M.M.: Cyber security challenges in smart cities: Safety, security and privacy. Journal of advanced research **5**(4), 491–497 (2014)
8. Frischmann, B.M., Madison, M.J., Strandburg, K.J.: Governing knowledge commons. Oxford University Press (2014)

9. Goodman, E.P., Powles, J.: Urbanism under google: Lessons from sidewalk toronto. Fordham L. Rev. **88**, 457 (2019)
10. Heeks, R., Shekhar, S.: Datafication, development and marginalised urban communities: an applied data justice framework. Information, Communication & Society **22**(7), 992–1011 (2019)
11. Johnston, M.: Good governance: Rule of law, transparency, and accountability. New York: United Nations Public Administration Network (2006)
12. Kling, R., Lamb, R.: Bits of Cities: Utopian Visions and Social Power in Placed-Based and Electronic Communities. Rob Kling Center for Social Informatics (1996)
13. Kosack, S., Fung, A.: Does transparency improve governance? Annual review of political science **17**, 65–87 (2014)
14. Mangu-Ward, K.: Mickey mouse is watching you. Slate (2013), https://slate.com/technology/2013/01/magicbands-disney-ceo-bob-iger-gives-epic-smackdown-to-ed-markey-over-privacy-concerns.html
15. Martínez-Ballesté, A., Pérez-Martínez, P.A., Solanas, A.: The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Communications Magazine **51**(6), 136–141 (2013)
16. Mosco, V.: City of technology: Where the streets are paved with data. The Smart City in a Digital World (Society Now) pp. 59–95 (2019)
17. Nissenbaum, H.: Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press (2009)
18. Peel, M.A.: Between the houses: neighbouring and privacy. In: A history of European housing in Australia, pp. 269–286. Cambridge University Press (2000)
19. Rubinstein, I.: Urban privacy. Research Privacy Group, NYU (2020)
20. Rubinstein, I., Petkova, B.: Governing privacy in the datafied city. Fordham Urban Law Journal, Forthcoming (2019)
21. Rubinstein, I.S.: Privacy localism. Wash. L. Rev. **93**, 1961 (2018)
22. Sanfilippo, M., Frischmann, B., Standburg, K.: Privacy as commons: Case evaluation through the governing knowledge commons framework. Journal of Information Policy **8**, 116–166 (2018)
23. Sharma, R., Mondal, D., Bhattacharyya, P.: A comparison among significance tests and other feature building methods for sentiment analysis: A first study. International Conference on Computational Linguistics and Intelligent Text Processing pp. 3–19 (2017)
24. Shvartzshnaider, Y., Apthorpe, N., Feamster, N., Nissenbaum, H.: Going against the (appropriate) flow: a contextual integrity approach to privacy policy analysis. In: Proceedings of the AAAI Conference on Human Computation and Crowdsourcing. vol. 7, pp. 162–170 (2019)
25. Stone, K.: Enter the world of yesterday, tomorrow and fantasy: Walt disney world's creation and its implications on privacy rights under the magicband system. J. High Tech. L. **18**, 198 (2017)
26. Van Zoonen, L.: Privacy concerns in smart cities. Government Information Quarterly **33**(3), 472–480 (2016)
27. Walt Disney Travel Company: My disney experience – frequently asked questions (faq), https://www.disneyholidays.com/walt-disney-world/faq/my-disney-experience/