ENTER THE WORLD OF YESTERDAY, TOMORROW AND FANTASY: WALT DISNEY WORLD'S CREATION AND ITS IMPLICATIONS ON PRIVACY RIGHTS UNDER THE MAGICBAND SYSTEM

Kaitlyn Stone*

I. Introduction

In 2015, over 54 million people visited the Walt Disney World resort.[1] In 2014, approximately half of guests to Walt Disney World participated in Disney's MagicBand and MyMagic+ systems.[2] These systems allow for smoother and more personalized guest experiences by having guests wear the wristbands to serve as their park ticket, room key, and credit card for purchases in the park.[3] Disney advertises these systems as a benefit for the guests, but most visitors

* J.D. Candidate, Suffolk University Law School, 2018.

[1] *See* THEMED ENTERTAINMENT ASSOCIATION, TEA/AECOM 2015 THEME INDEX AND MUSEUM INDEX: THE GLOBAL ATTRACTIONS ATTENDANCE REPORT 35 (Judith Rubin ed., 2016) (listing the attendance numbers for global amusement and theme parks).

[2] *See* Daniel Wolfe, *Magic Bands Used by Half of Disney World Guests*, PAYMENTSSOURCE (Aug. 5, 2014), *archived at* https://perma.cc/86NG-4NJM (highlighting the success that the MagicBand program experienced after its initial launch).

[3] *See FAQs: How do I use my MagicBand?,* DISNEY HELP CENTER (Oct. 18, 2017), *archived at* https://perma.cc/3XCW-U2GH (illustrating the various ways that MagicBands can be used); *see also* Wolfe, *supra* note 2 (explaining how the MagicBand program has improved guest experience while also increasing revenues for Disney).

 ISSN 1536-7983.

to the park do not realize the company is gaining large amounts of detailed information about individual guest behavior.[4]

Critics of this system believe that it is akin to the National Security Agency ("NSA") and "Big Brother."[5] Still, most guests do not mind the "creepiness" of someone tracking their every move when it is a company that will provide them with lasting family vacation memories rather than the government.[6] This distinction makes sense until you consider one fact: Walt Disney World ("Disney World") has its own government.[7] By establishing their own government structure in order to allow for easier innovation and less government red tape, Walt Disney World has blurred lines between the public and private spheres.[8] This makes it difficult to establish how exactly to apply privacy law to the MagicBand system.[9]

Additionally, as more and more companies and industries find ways to integrate technology like the MagicBand system into their

[4] *See* Cliff Kuang, *Disney's $1 Billion Bet on a Magical Wristband*, WIRED (Mar. 10, 2015), *archived at* https://perma.cc/4N29-FA6F (explaining how the information collected by Disney through the use of MagicBands helps the company anticipate the needs of their guests).

[5] *See* Eliana Dockterman, *Now Disney Can Track Your Every Move with NSA-Style Wristbands*, TIME (Jan. 2, 2014), *archived at* https://perma.cc/SNB8-S2RR (suggesting the dangers of the MagicBand system in a post-Snowden world).

[6] *See* Kuang, *supra* note 4 (distinguishing how Disney tracking users' data is motivated by creating consumer benefit); *see also* Wolfe, *supra* note 2 (citing that ninety percent of MagicBand users are satisfied with the experience and thus willing to participate in the program).

[7] *See* Herb Leibacher, *Reedy Creek Improvement District- Disney's Own Government?*, WORLD OF WALT (May 28, 2012), *archived at* https://perma.cc/9BY7-3YT7 (describing how and why Walt Disney World created its own government); *see also* Joshua Shenk, *Hidden Kingdom: Disney's Political Blueprint*, THE AMERICAN PROSPECT (Mar. 1995), *archived at* https://perma.cc/U5VF-QNYE (noting Disney's use of dummy corporations, cooperative individuals, and lobbying campaigns to segregate the land from local regulatory authorities).

[8] *See* Shenk, *supra* note 7 (outlining the ways in which Walt Disney World has combined aspects of a private entity and public government). *See also Walt Disney Company,* BLOOMBERG MARKETS (Oct. 31, 2017)*, archived at* https://perma.cc/W8AZ-3ZGL (establishing that while Disney is a publicly traded company, some decisions are left entirely behind closed doors).

[9] *See Shenk, supra* note 7 (suggesting that Disney's control of both land and community has facilitated its ability to operate solely as a corporation).

business structures, conflicts with privacy law will arise more frequently.[10] Both private industries, such as fashion retailers and department stores, as well as public entities, such as states' departments of transportation have started to implement Radio Frequency Identification (RFID) technology in their respective industries.[11] While implementing RFID technology can have tremendous benefits for the organizations that choose to make use of it, its use also poses an array of privacy concerns.[12] Attempts to address these concerns through technology-specific legislation have been relatively unsuccessful.[13] Users of RFID technology need to implement their own policies in order to protect the privacy of average consumers and protect themselves from invasion of privacy litigation.[14]

---

[10] *See* John Foreman, *You don't want your privacy: Disney and the meat space data race*, GIGAOM (Jan. 18, 2014), https://perma.cc/QA4U-8TRZ (detailing different ways that other businesses are implementing similar technology and how this presents increasing privacy issues).

[11] *See id.* (noting that the use of technology and data collection are now the main focus of marketing strategies for many companies); *see also* Ava Farshidi, *The New Retail Experience and its Unaddressed Privacy Concerns: How RFID and Mobile Location Analytics are Collective Customer Information*, 7 CASE W. RESERVE J. L. TECH. & INTERNET 15, 19 (2016) (highlighting the use of RFID technology in retail stores as a more efficient way of keeping track of merchandise compared to barcodes); Noah R. Bombard, *Free Ride: New Mass. Pike tolling system will allow you to bypass tolls in Springfield, Worcester*, MASSLIVE (Aug. 22, 2016), *archived at* https://perma.cc/A2TK-A2BW (explaining the Massachusetts Department of Transportation's new RFID-equipped highway tolling system currently being implemented in order to eliminate physical stops at the toll booth).

[12] *See* James Thrasher, *How is RFID Used in Real World Applications*, RFID INSIDER (Aug. 23, 2013), *archived at* https://perma.cc/J9UD-2R9M (listing thirteen uses and benefits of RFID technology); Quentin Archer & Gisèle Salazar, *RFID: a threat to privacy?*, COMPUTER WEEKLY (Apr. 2005), *archived at* https://perma.cc/9H3M-SQ5R (articulating the myriad of uses of RFID technology that could exceed its current legislative regulation in the future).

[13] *See Radio Frequency Identification (RFID) Privacy Laws,* NAT'L CONF. OF ST. LEGISLATURES (Mar. 30, 2017), *archived at* https://perma.cc/6KJG-BNWD (illustrating that only 19 states have implemented legislation addressing the privacy concerns of RFID legislation, and where legislation has been implemented, it is not comprehensive, but rather addresses individual concerns).

[14] *See GS1 Guidelines On the Use of EPC/RFID For Consumer Products*, GS1 (Mar. 30, 2017) [hereinafter, *GS1 guidelines*], *archived at* https://perma.cc/Q2V9-RS6C (outlining that in order for companies to successfully implement RFID technology the consumers must be fully informed and aware that the technology is being used).

This Note will attempt to resolve some of these legal ambiguities by analyzing the unique problem posed by Disney World's MagicBand system. First, this Note will discuss when a private entity may qualify as a state actor. This note will then look to the evolution of privacy laws both in the state actor context and under the tort of invasion of privacy. Second, this Note will present the unique history and development of Disney World's form of government. Then, this Note will illustrate the intricacies of the MagicBand system and how it presents various privacy concerns. Next this Note will analyze whether Walt Disney World should be classified as a state actor. Finally, this Note will discuss how privacy law should be applied to the MagicBand system in light of the state actor classification.

II. History

A. When is a Private Entity a State Actor?

Whether or not a private entity is considered a state actor will determine how privacy law is applied to a given situation.[15] The Constitution only protects an individual from the infringement of rights by a state actor, not individual citizens or private organizations.[16] Therefore, in asserting a violation of a constitutionally protected right, the court must first establish whether the alleged violator is a state actor.[17] This determination generally rests on how closely intertwined the government and private actors are in light of the particular

[15] *See* Sheldon Nahmod, *Know Your Constitution (8): What is State Action?*, NAHMOD LAW (Feb. 19, 2015), *archived at* https://perma.cc/CKC4-PDHC (providing examples of how private individuals cannot violate your constitutional rights and establishing the state action analysis as a "gate keeper" to constitutional challenges).

[16] *See* Julie K. Brown, *Less is More: Decluttering the State Action Doctrine,* 73 MO. L. REV. 561, 562 (2008) (explaining that the Equal Protection Clause of the Fourteenth Amendment only protects individuals against actions taken by state actors).

[17] *See* Brown *supra* note 16, at 563 (stating that the determination between whether the defendant is a state actor and subject to constitutional restrictions, or a private entity and immune from these restrictions is essential to many constitutional claims).

facts of the case.[18] While there have been many theories on the best way to consolidate the precedent on state action, as John Niles, Lauren Tribble and Jennifer Wimsatt articulate, the doctrine can generally be broken down into three basic steps.[19]

The first step in any state action analysis is to identify what conduct is at issue and who is the actor responsible for the conduct.[20] This step is normally the easiest step because it requires little analysis beyond the identification of the conduct that is at issue in the complaint.[21]

The next step is to analyze whether the nature of the actor is public or private.[22] If the actor is public in nature, then the conduct is subject to constitutional scrutiny.[23] However, if the actor is private in nature then the conduct is only subject to constitutional scrutiny when the state has sufficiently encouraged the conduct.[24] The nature of the

[18] *See* Brown *supra* note 16, at 564 (noting that while the Supreme Court has used many different tests in the state actor analysis, the central factor remains how involved the actor is in traditional government actions).

[19] *See* John D. Niles et al., *Making Sense of State Action*, 51 SANTA CLARA L. REV. 885, 898 (2011) (delineating the different approaches to state action analysis and how they may be consolidated into a manageable standard).

[20] *See id.* at 898 (establishing the first step in any state actor analysis as determining who the alleged state actor is and with what conduct they allegedly violated the Constitution).

[21] *See* Niles et al., *supra* note 19, at 899 (asserting that the first step is usually the easiest to establish in the state actor analysis). For example, the authors provide an example of a case in New York where a family filed a complaint against a warehouseman who stored their belongings after a city marshal evicted them from their apartment. *Id.* The complaint alleged that the warehouseman threatened to sell the family's belongings if they did not pay him for the storage, even though their belongings were placed in storage against their will. *Id.* The family asserted that this violated their due process rights, necessitating a determination of state action by the court. *Id.* The court used the complaint to determine that the conduct at issue was the threatened sale of the family's belongings and the actor was the warehouseman, not the city marshal. *Id.*

[22] *See* Niles et al., *supra* note 19, at 901 (stating the premise for the second step in state actor analysis).

[23] *See* Niles et al., *supra* note 19, at 901 (detailing the importance of the determination of the nature of the actor in determining whether the conduct violates the Constitution).

[24] *See* Niles et al., *supra* note 19, at 901 (illustrating how a private actor's conduct can still be considered state action through the involvement of the state). The authors give examples how passing various forms of legislation could make a constitutional violation by a private actor more likely to occur, and therefore the state can be found to encourage the conduct of a private actor. *Id.* at 911-14.

actor can be said to be public if (1) the actor is a governmental entity; or (2) the actor acted in a public capacity during the conduct in question.[25] The third and final step in the state action analysis is to determine when the action of a non-governmental actor that is participating in private conduct can become attributable to the state for purposes of constitutional scrutiny.[26]

The bulk of the state actor analysis deals with determining when a non-governmental entity becomes a state actor by acting in a public function.[27] The basics of the public function doctrine involve determining whether the conduct at issue is "traditionally, exclusively reserved to the state."[28] In *Marsh v. Alabama*,[29] the Supreme Court addressed whether a company-owned town was a state actor by analyzing whether the conduct was of the kind that is traditionally reserved for the state.[30] The town was owned by Gulf Shipping Corporation, a shipbuilding company, but had all the characteristics of a normal town or municipality, including residential buildings, public roads, sewer systems and a post office.[31] The State argued the company had the ability to regulate the residents of the town in the same way that a homeowner has the ability to control the conduct of his houseguest.[32] The Court determined that because the company was

[25] *See* Niles et al., *supra* note 19, at 901 (outlining the ways in which an entity can become a state actor for purposes of constitutional analysis). A government entity can be the entities that make up all levels of government including legislatures, courts, agencies and their employees. *Id.* at 902. However, they also include entities that are controlled by governmental entities. *Id.*

[26] John D. Niles et al., *Making Sense of State Action*, 51 SANTA CLARA L. REV. 885, 910-11 (2011) (establishing the final step in the state action determination).

[27] *See id.* at 904 (introducing the intricacies of the precedent that exists in the public function doctrine).

[28] *See id.*, at 905 (stating the most basic standard for applying a public function analysis).

[29] Marsh v. Alabama, 326 U.S. 501 (1946) (questioning whether a state can criminally punish someone on a company owned town, contrary to the wishes of the towns management).

[30] *See id.* at 502 (inferring that the main issue of the case was whether a company owned town that restricted the distribution of religious materials was in violation of the Constitution).

[31] *See id.* (detailing the aspects of the town that were operated as a municipality, in the traditional sense).

[32] *See id.* at 504-05 (outlining the State's argument that the shipping company's right to control the inhabitants of the municipality is the same as a homeowner's right to control the people in his house). The corporation asserted that because legal title to the town belonged to Gulf Shipping, they had the power to limit freedom

operating the town in the same way that any non-corporate owned town would be run, they could not infringe upon the constitutional rights of the residents of the town.[33]

The Supreme Court has also addressed whether providing a public service can classify a private company as a state actor.[34] In *Jackson v. Metropolitan Edison Company*,[35] the Court addressed whether the fact that a private company is subject to state regulation can support a finding that the private company is a state actor.[36] The utility company was privately owned, but was subject to many state regulations.[37] The Court established that it is not only an evaluation of the company being subject to state regulations, but rather whether there is "a sufficiently close nexus between the state and the challenged action… so that the latter may be fairly treated as that of the state itself."[38] Subsequently, the Court determined that merely because the utility company provided a public service and was heavily regulated by the state, it did not establish a nexus close enough to operate as a state actor.[39]

If the actor is determined to be nongovernmental and acting in a private nature, then the final step in the analysis is to determine

---

under the theory that it was private property. *Id.* The court ultimately denied this argument. *Id.* at 505.

[33] *See Marsh*, 326 U.S. at 508 (highlighting the fact that many Americans live in company-owned towns and that does not mean that they have somehow given up their constitutional rights).

[34] *See* Jackson v. Metropolitan Edison Company, 419 U.S. 345, 351 (1974) (setting up the situation for the court to address whether holding a certificate of public convenience issued by the state classifies a company as a state actor).

[35] 419 U.S. 345 (1974).

[36] See *id.* at 349 (detailing that the main issue in the case was whether the utilities company's actions were private or state action).

[37] *See id.* at 349-50 (establishing the public and private elements of the utility company). The Metropolitan Edison Company was privately owned but held a certification of public convenience from the Pennsylvania Public Utilities Commission that subjected it to extensive regulation by the commission. *Id.* at 346.

[38] *See id.* at 351 (highlighting the test that the Court uses in their determination of the case). In order to establish a "sufficiently close nexus," the party claiming state action must be able to show some connection between the State and the allegedly infringing conduct so that the conduct may be treated as that of the State itself. *Id.*

[39] *See Jackson*, 419 U.S. at 354-59 (articulating the court's holding that the utility company's termination of service could qualify as state action simply because the company received licensing and authorization from the state).

whether the private conduct can be attributed to the State.[40] Niles, Tribble, and Wimsatt highlight the different levels of state involvement, which include prohibition, discouragement, permission, encouragement, and mandate.[41] Private conduct becomes attributable to the state when the state involvement crosses from permission to encouragement.[42] This determination is made based on the subjective and objective intent of the state.[43]

The Supreme Court addressed this step specifically when they asked whether a city-owned and publicly funded parking facility had encouraged the actions of a privately owned restaurant located within the parking garage in *Burton v. Wilmington Parking Authority*.[44] While the case was ultimately dismissed, the Supreme Court decided to address the important constitutional question under the state actor doctrine.[45] The Court determined that based on the parking facility's status as a building for "public uses," that it was built using public funds and that the parking authority in charge of the facility was able

[40] *See* Niles et al., *supra* note 19, at 910-12 (elaborating that the final way state action can be found is when the State is found to be involved in the private conduct in such a way that the conduct may be attributed to the State itself).

[41] *See* Niles et al., *supra* note 19, at 912-13 (illustrating the different types of state involvement that can exist to encourage the actions of private entities). The different levels of state involvement begin with prohibition, where the state specifically limits or punishes certain actions, and progress across the spectrum to mandate, where the state specifically requires or orders a certain action to take place. *Id.*

[42] *See* Niles et al., *supra* note 19, at 913-14 (analyzing at what point the state involvement becomes sufficient enough to cause the conduct to be subject to constitutional scrutiny). The authors explain that in order for a State to encourage private conduct there must be more than merely permitting the conduct to happen by failing to take action or pass legislation. *Id.* at 913. Instead the state must affirmatively take action that encourages the conduct, such as passing legislation that makes the deprivation more likely. *Id.*

[43] *See* Niles et al., *supra* note 1919, at 914 (giving the basis for the differentiation between permission by the state and encouragement by the state).

[44] *See* Burton v. Wilmington Parking Authority, 365 U.S. 715, 716 (1961) (providing background and setting forth the main issue of the case). The Parking Authority was created by the city in order to deal with the public parking crisis. *Id.* at 717. The Authority constructed a parking facility and leased space in the facility to supplement the cost of construction. *Id.* at 718-19. Eagle Coffee Shoppe leased the space and received certain benefits from the Parking Authority such as maintenance costs and a tax exempted status. *Id.* at 719-20. Eagle later denied service to the appellant on the basis of his race. *Id.* at 720.

[45] *See id.* at 716-17 (discussing the reason for granting the motion to dismiss and why the Court ultimately chose to evaluate the state actor question, treating the appeal instead as a petition for a writ of certiorari).

to perform "essential governmental functions," the parking facility could be determined to be a state actor.[46] Furthermore, based on the relationship between the restaurant and the parking facility—namely that the restaurant relied on the facility to provide a place of business and other benefits, while the parking authority relied on the income generated from leasing the space—the Court recognized a " degree of participation and involvement in discriminatory action, which the it was the design of the Fourteenth Amendment to condemn" and held the parking authority responsible.[47]

Together, the preceding cases illustrate ways in which private actors that exhibit characteristics typically attributable to public entities can complicate the state actor determination.[48] This determination is essential to the outcome of many cases dealing with the constitutionality of the actions of private actors and the steps outlined by Niles, Tribble, and Wimsatt, and illustrated by the aforementioned cases help to navigate the complex area of state action.[49]

B. Privacy and the Fourth Amendment

Now that a conceptual framework for establishing whether a private actor is a state actor has been defined, it is necessary to analyze

[46] *See Burton*, 365 U.S. at 723-24 (listing various reasons why the parking authority could be viewed as a state actor).

[47] *See id.* at 724 (highlighting the interdependent nature between the restaurant and the parking authority). The Court stated that, "the state has so far insinuated itself into a position of interdependence with Eagle that it must be recognized as a joint participant in the challenged activity." *Id.* at 725.

[48] *See* Niles et al., *supra* note 19, at 886 (illustrating the difficulty that the Supreme Court has had in drawing a line between private and state action). The authors explain that because the determination is fact dependent and made on a case-by-case basis, there exist many different standards and rationales that courts have used to find state action. *Id.* at 886-87.

[49] *See* Niles et al., *supra* note 19, and 887-88 (advocating that the Court adopt a simplified, conceptual approach to state action analysis in order to provide more guidance to lower courts).

when a state actor may violate the Constitution's privacy guarantees.[50] The Fourth Amendment of the United States Constitution establishes the first line standard for privacy from the government.[51] However, there have been significant adjustments made to the interpretation of the term "unreasonable" as national security and terrorism become important issues.[52] In an invasion of privacy analysis under the Fourth Amendment, a government search must enter into a place where one has a "reasonable expectation of privacy" in order to implicate constitutionally provided protections.[53] A determination of whether an individual has a reasonable expectation of privacy is entirely fact dependent and has been analyzed in many different contexts, including technological surveillance.[54]

The controlling case on establishing what constitutes whether or not a search has occurred is *Katz v. United States*.[55] In *Katz*, the Supreme Court analyzed whether someone had a reasonable expectation of privacy in a public phone booth such that, by placing a listening device on the outside of the booth, the police violated the individual's

[50] *See* Niles et al., *supra* note 19, at 898 (describing what is considered state conduct).

[51] *See* U.S. CONST. amend. IV (establishing the right to be protected from unreasonable searches and seizures). The amendment states, in relevant part: "The Right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated…" *Id.* *See also* STEVE C. POSNER, PRIVACY LAW AND THE USA PATRIOT ACT § 2.02 (Matthew Bender & Co. 2016) (explaining that the right to privacy is created through the use of many different clauses throughout the Constitution and their counterparts in state and local governments). Courts have held that the right to privacy can also be found in the First, Third, Fifth, Ninth and Fourteenth amendments. *Id.*

[52] *See* POSNER, *supra* note 51 (discussing how privacy rights can change over time to adapt to cultural and technological evolutions). Posner suggests that due to the fluid nature of the right to privacy, there is a potential for certain privacy rights to be lost over time, and possibly, overnight. *Id.*

[53] *See* STEVE POSNER, PRIVACY LAW AND THE USA PATRIOT ACT, § 2.05 (Mathew Bender & Co. 2016)(highlighting the importance of the "unreasonableness" analysis when determining if there has been an invasion of privacy under the Fourth Amendment).

[54] *See* POSNER, *supra* note 51 (listing important cases in which a reasonable expectation of privacy has been analyzed by a court).

[55] *See* Courtney Burten, Note, *Unwarranted! Privacy in a Technological Age: The Fourth Amendment Difficulty in Protecting Against Warrantless GPS Tracking and the Substantive Due Process and First Amendment Boost,* 21 S. CAL. INTERDISC. L. J. 359, 365 (2012) (highlighting the importance of the *Katz* case in establishing the elements of a Fourth Amendment violation).

privacy.[56] The Government asserted that no search had occurred because there was no physical intrusion into the phone booth.[57] The Court established that the case did not rest on the determination of whether there was a physical intrusion into a "constitutionally protected area," but rather whether the defendant had a reasonable expectation that his phone call would remain private.[58] Most notably, the Court held that a physical intrusion or trespass into an area is not necessary for a Fourth Amendment claim.[59] The Court concluded that the defendant did have a reasonable expectation of privacy due to the fact that people within a phone booth would expect that their conversations would remain private.[60] Through this case, the Supreme Court established the two elements of a Fourth Amendment cause of action: (1) that a reasonable expectation of privacy existed by determining whether the person had an actual expectation of privacy and whether society recognizes the expectation of privacy as reasonable; and (2) whether there was a violation of this reasonable expectation of privacy.[61]

The Supreme Court further explored what a "reasonable expectation of privacy" is by elaborating on the Third Party Doctrine in

[56] *See* Katz v. United States, 389 U.S. 347, 349-50 (1967) (stating the main issue on appeal). The defendant argued that the phone booth was a constitutionally protected area, and therefore, the government had infringed upon his privacy by listening in on his phone conversation. *Id.*

[57] *See id.* at 352-3 (articulating why the Government believed that they had not violated the Constitution). The Government sought to maintain the use of the trespass doctrine in determining whether a violation of the Fourth Amendment had taken place. *Id.* The trespass doctrine required that in order for a search to take place, there must have been a physical intrusion in to a protected area. *Id.* at 352.

[58] *See Katz*, 389 U.S. at 351 (noting that the Fourth Amendment protects people rather than just areas). The Court stated that, "What a person knowingly exposes to the public, even in his own home or office is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in areas accessible to the public, may be constitutionally protected." *Id.*

[59] *See id.* at 353 (explaining the previous trespass standard is no longer the exclusive test in an unreasonable search and seizure analysis).

[60] *See id.* at 352 (rejecting the idea that the expectation of privacy did not exist due to the public nature of the phone booth). The Court goes on to establish that because the Government's surveillance of the phone booth was limited to the purposes of their investigation of the defendant, it was not an unreasonable search and seizure and did not violate the Fourth Amendment. *Id.* at 354.

[61] *See* Burten, *supra* note 55, at 365 (outlining the two parts of a Fourth Amendment violation analysis established in Katz).

United States v. Miller.[62] In *Miller,* the Court was asked to determine whether obtaining an individual's bank records from the bank in order to establish a criminal charge against him was a violation of the Fourth Amendment.[63] While the Fourth Amendment provides protections for an individual's "papers and effects," and previous case law had established that this part of the Amendment protects against the "compulsory production of a man's private papers," the Court held that the bank account information at issue in the case would not be considered to be "private papers."[64] The Court determined that no "expectation of privacy" existed in the bank records because they contained information that was voluntarily given to the banks in the ordinary course of business.[65] Further, the Court explained that the Fourth Amendment does not protect an individual from the release of information they have revealed to a third party.[66] While *Miller* addressed financial records specifically, the reasoning used by the Court, is now known as the Third Party Doctrine, and has been extended to various other cases – such as the use of cell phone data in pinpointing an individual's location.[67]

---

[62] *See* United States v. Miller, 425 U.S. 435, 443 (1976) (explaining that the third party doctrine applies when the government obtains information that is voluntarily shared by an individual with a third party).

[63] *See id.* at 437 (articulating that the main issue on appeal is whether the defendant had a protectable Fourth Amendment interest). The respondent argued that because the bank records at issue were copies of his own personal records given to the bank for a limited purpose, a protectable Fourth Amendment interest existed. *Id.* at 442.

[64] *See id.* at 440 (stating that the "private papers" at issue are business records of the bank). The respondent argued that the Government effectively circumvented the Fourth Amendment requirement of probable cause. *Id.* at 441. This was because the bank was required to keep certain records under the law and the records were obtained through a subpoena. *Id.* at 442.

[65] *See Miller*, 425 U.S. at 442-43 (1976) (rejecting the respondent's assertion that the bank records were copies of his personal records).

[66] *See id.* at 443 (explaining that the Fourth Amendment does not extend to information revealed to third parties under the assumption that the confidence in the third party will not be betrayed). The Court stated, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id.*

[67] *See* Posner, *supra* note 53 (listing different cases in which the Third-Party Doctrine has been addressed). In 1984, the Supreme Court upheld the Third Party Doctrine established in *Miller*, but provided that Congress had the ability to expressly limit it. *Id. See, e.g.,* Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (concluding that the government requested installation of a pen register on the petitioner's phone was not a search in violation of the Fourth Amendment); United States v. Graham, 824 F.3d 421, 438 (4th Cir. 2016) (holding that historical cell site location

Over the years, questions of where someone has a reasonable expectation of privacy have resulted in many limitations, especially in light of advancing technology and the increased threat of terrorism.[68] The Supreme Court addressed this problem directly in *United States v. Jones*.[69] The Court was faced with the question of whether placing a GPS tracking device on the defendant's wife's car was a violation of the Fourth Amendment.[70] The Government argued and the District Court held that the evidence was admissible on the basis that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[71] However, the Supreme Court emphasized that the decision in *Katz* – that an unreasonable search and seizure could take

data may be used to determine whether the defendants were guilty of being in possession of a firearm, armed robbery, and conspiracy); United States v. Davis, 785 F.3d 498, 532-33 (11th Cir. 2015) (affirming that the use of telephone company business records in linking the defendant to the location of seven armed robberies was not a violation of the Fourth Amendment).

[68] *See* Posner, *supra* note 53 (suggesting that the rise of terrorism and the fear that new technologies may be used by terror organizations in the wake of September 11th, have altered the public's understanding of what a "reasonable" expectation of privacy is); *see also* United States v. Jones, 565 U.S. 400, 427 (2012) (Sotomayor, J., concurring) (implying that as the government implements new technologies, the temptation to restrict or infringe upon individual privacy rights will grow). Justice Sotomayor also argues that the Third Party Doctrine is ill-equipped to handle the obstacles of the digital age due to the large amount of information that individuals disclose via the internet without even realizing it (citing *Katz,* 389 U.S. 347). *Id.* at 415.

[69] *See Jones*, 565 U.S. at 404-5 (illustrating how improving technology has influenced determinations of reasonable expectations of privacy (citing *Katz,* 389 U.S. 347)). The Court addressed the fact that with GPS and other types of technology, it is important to uphold the principle that a violation of the Fourth Amendment does not require a physical intrusion. *Id.*

[70] *See id.* at 402-04 (outlining the facts of the case). The Defendant was under suspicion of drug trafficking and the Government applied for a warrant to authorize the use of a GPS tracking device on the Defendant's car. *Id.* The device was capable of determining a vehicle's location within 50 to 100 feet of the actual location. *Id.* At trial, the Government admitted evidence collected from the GPS device to show that the defendant had been at a house where they found 850,000 dollars in cash and 97 grams of cocaine, among other illicit paraphernalia. *Id.* at 403-04.

[71] *See Jones*, 565 U.S. at 402-404 (stating the District Court's determination on whether the defendant had a reasonable expectation of privacy). The Government argued that there was no reasonable expectation of privacy because where the GPS was positioned and the car's location on the public road were both accessible to the public and therefore, no reasonable expectation of privacy existed. *Id.* The District

place when no physical intrusion had taken place – does not erase the protection that the Fourth Amendment provides against physical intrusion.[72] Placing the GPS tracker on the car then served as a trespass on the defendant's property and constituted a search that was subject to the restrictions of the Fourth Amendment.[73] Further, the Court highlights issues that may arise in terms of surveillance as technology advances.[74] Particularly in terms of GPS and other surveillance methods capable of producing significant amounts of personal information, it is possible for law enforcement to evade the limits put in place to constrain abuse and strain relations with the community.[75]

As these cases illustrate, it is often difficult to determine whether certain government surveillance methods, especially in the context of advancing technologies, are subject to a Fourth Amendment analysis and therefore qualify as a breach of an individual's privacy.[76]

Court suppressed evidence collected while the Jeep was parked in the defendant's garage, but allowed evidence collected while the car was in use. *Id.* at 403.

[72] *See id.* at 409 (emphasizing that the *Katz* holding adds to the trespass standard rather than substituting it).

[73] *See id.* at 406 (explaining why the Court does not need to address whether the defendant had an expectation of privacy while driving the car).

[74] *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (suggesting that technological advances will affect the *Katz* test by influencing "societal privacy expectations").

[75] *See id.* at 416 (illustrating the potential problems created by non-invasive surveillance methods). Justice Sotomayor wrote:

> Awareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society.

Id.

[76] *See Jones,* 565 U.S. at 404-05 (determining that there is a reasonable expectation of privacy in a parked car when police attach a GPS device to track the vehicle's movements); *e.g.* United States v. Miller, 425 U.S. 435, 440 (1976) (establishing that there is no reasonable expectation of privacy in information provided to a bank in the ordinary course of business and therefore, said information is not constitu-

C. *Privacy as a Civil Cause of Action*

Finally, we must look at how privacy law is applied in the absence of a state actor relationship.[77] Introduced by Samuel Warren and Louis Brandeis, the concept of privacy as an individual cause of action was initially described as "the right to be let alone."[78] The Restatement (Second) of Torts established a more concrete definition of the common law idea of invasion of privacy.[79] The Restatement establishes a cause of action for when someone intrudes upon an individual's seclusion or his private affairs and concerns.[80] Many states have adopted statutes enacting the Restatement's defined cause of action for an invasion of privacy.[81] The most common, intrusion upon

---

tionally protected); *Katz*, 389 U.S. at 353 (holding that although no physical intrusion had occurred, the government violated the defendant's justifiable expectation of privacy).

[77] *See* Michael McFarland, *Why We Care About Privacy*, MARKKULA CTR. FOR APPLIED ETHICS (Jun. 1, 2012), *archived at* https://perma.cc/WE4X-GK7U (highlighting that our concept of privacy is vitally important to our other fundamental rights and that violating this privacy could be also detrimental for businesses).

[78] *See* Posner, *supra* note 51 (Matthew Bender & Co. 2016) (citing Samuel Warren and Justice Louis Brandeis as the developers of the concept of the right to privacy); *see also Intrusion Upon Seclusion: Invasion of Privacy,* TIBBETTS, KEATING, & BUTLER (Apr. 11, 2013), *archived at* https://perma.cc/H4WB-YSKN (elaborating on the history of the invasion of privacy and how it first gained legal footing).

[79] *See* RESTATEMENT (SECOND) OF TORTS § 652A (AM. LAW. INST. 1977) (establishing ways in which the right to privacy can infringed upon). The Restatement states in relevant part:

> The right of privacy is invaded by . . . unreasonable intrusion upon the seclusion of another . . . appropriation of the other's name or likeness . . . unreasonable publicity given to the other's private life . . . publicity that unreasonably places the other in a false light before the public . . . .

Id.

[80] *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW. INST. 1977) (outlining the intrusion upon seclusion tort).

[81] *See* STEVE C. POSNER, PRIVACY L. AND THE USA PATRIOT ACT, §2.03 (Mathew Bender & Co. 2016) (emphasizing that while most states have some form of an invasion of privacy tort, not all states define the tort in the same way). While states differ in their statutory and common law definitions and formulations of the invasion of privacy action, there are certain characteristics that are similar among them all. *Id.*

seclusion, occurs when someone intentionally intrudes in a place or into the affairs of another.[82] In order to satisfy a claim for intrusion upon seclusion the complainant must prove that (1) there has been an intentional intrusion, (2) into a place, conversation, or matter that the complainant has a reasonable expectation of privacy in, and (3) that the intrusion is one that would be highly offensive to a reasonable person.[83]

The Restatement gives some guidance on how these elements must be met.[84] First, all that is required to establish an intentional intrusion is that the defendant acted with knowledge or intent to violate the complainant's privacy.[85] Second, the Restatement establishes that conduct is only actionable when the defendant has intruded into a private place or has otherwise invaded the complainant's seclusion.[86] Finally, there will be no liability imposed on the defendant unless the intrusion would be offensive to a reasonable person, which means that the intrusion must be a substantial one.[87]

---

[82] *See* RICHARD RAYSMAN, PETER BROWN, JEFFREY D. NEUBURGER AND WILLIAM E. BRANDON III, EMERGING TECHNOLOGIES AND THE LAW: FORMS AND ANALYSIS, § 9.03 (Law Journal Press, 2017) (defining the tort of intrusion upon seclusion).

[83] *See* RESTATEMENT (SECOND) OF TORTS §652B (AM. LAW. INST. 1977) (setting forth the elements of a prima facie case for a tort claim of intrusion upon seclusion); F. LAWRENCE, STREET LAW OF THE INTERNET, § 2.06 (Matthew Bender & Company Inc., 2016) (providing a concise explanation for proving the elements of intrusion upon seclusion).

[84] *See* RESTATEMENT (SECOND) OF TORTS, §652B (AM. LAW. INST. 1977) (elaborating in the comments about different issues that may arise when looking at an intrusion upon seclusion claim and how they should be addressed).

[85] *See id.* at cmt. (a) (asserting that all that is required is an intentional interference with the complainant's interest in his solitude). Further, the Restatement addresses that the intrusion need not be a physical one, but may also include various means to oversee or overhear a conversation or matters that an individual wishes to remain private. *Id.* at cmt. (b).

[86] *See id.* at cmt. (c) (commenting that while taking a picture of an individual while he is in public would not be considered an intrusion into a private place, there may still be things that an individual may wish to keep private, even when they are out in public); *see also* LAWRENCE, *supra* note 83 (suggesting that the determination of whether an individual has a reasonable expectation of privacy is substantially similar under the intrusion upon seclusion context as in the Fourth Amendment context).

[87] *See* RESTATEMENT (SECOND) OF TORTS §652B, cmt. (d) (AM. LAW. INST. 1977) (discussing that the interference becomes a "substantial burden" when increased persistence and frequency amount to "hounding"). *See also* Shulman v. Group W Prods., Inc., 955 P.2d 469, 490 (1998) (illustrating the requirement that an invasion of privacy be considered serious enough before imposing liability).

The intrusion upon seclusion claim has been raised more frequently due, in part, to the rise in information technology being used in more commercial settings.[88] As Sebastian Sevignani articulates, information has become a commodity in our current society.[89] As a commodity, the methods of information collection by major companies is a form of business investment.[90] The information collected allows them to target advertisements to certain consumer groups that are most likely to respond to their marketing campaigns.[91] In order to collect this information, many companies implement digital surveillance methods that lead to serious privacy issues.[92]

Specifically, location technologies, such as Global Positioning System (GPS) and Radio Frequency Identification (RFID), have presented significant issues in terms of intrusion actions.[93] These systems make it possible for companies to monitor the consumers' movements and actions and collect this information to be used for their own purposes.[94] This information can be used to identify a particular consumer's habits and personality in order to target marketing that is specifically tailored to the individual.[95] Furthermore, if companies do not inform the consumers that their information and is being collected and used in this way, the question becomes whether the

[88] *See* Roland Hung, *Intrusion Upon Seclusion Part 2: Implications for Businesses Across Canada*, SNIP/ITS (Aug. 1, 2014), *archived at* https://perma.cc/N876-DTAU (instructing Canadian businesses on why it is important to prepare for a rising number of intrusion upon seclusion claims).

[89] *See* SEBASTIAN SEVIGNANI, PRIVACY AND CAPITALISM IN THE AGE OF SOCIAL MEDIA 58 (Taylor & Francis Group, 2016) (asserting that corporations collect information in order to exchange and profit from this information).

[90] *See id.* (implying that companies only care about this information because it helps them to advance their business goals).

[91] *See id.* (illustrating how a company might decide to direct an ad campaign at a particular demographic).

[92] *See id.* at 62-63 (explaining how social media companies in particular walk a fine line between surveillance and privacy).

[93] *See* RICHARD RAYSMAN, PETER BROWN, JEFFREY D. NEUBURGER AND WILLIAM E. BRANDON III, EMERGING TECHNOLOGIES AND THE LAW: FORMS AND ANALYSIS § 9.04 (Law Journal Press, 2017) (presenting some of the potential issues raised by locational technologies).

[94] *See id.* (explaining how data is collected, compiled and used by companies through the use of technology).

[95] *See id.* (detailing how personal information is collected and can be used in order to enhance marketing tactics).

consumers had the opportunity to consent the use of their personal information.[96]

Recently, many courts have been faced with this issue when companies—and specifically, their websites—place Internet cookies on to an individual's private computer.[97] Two of these cases, against Google and Facebook, have highlighted the importance of establishing how the right to privacy operates in certain industries as technology continues to advance.[98]

In 2015, the Third Circuit addressed the issue of Google's circumvention of the consumers' cookie-blocking software in order to place third-party cookies on their computers.[99] The plaintiffs alleged that the use of third-party cookies allowed Google to create detailed profiles of each individual user based on their web browsing history and that doing so by circumventing the cookie-blocking technology installed on their computer was an invasion of their privacy.[100] In analyzing the invasion of privacy claims, the court stated that the plain-

[96] *See id.* (highlighting issues such as lack of consent, inability to negotiate, and impose restrictions on the use of their personal information); *see also* Joel R. Reidenberg, et. al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 J. L. & POL'Y FOR INFO. SOC'Y 485-86 (highlighting that the choice and notice frameworks have been the favored method for preventing against privacy violations for the last fifteen years).

[97] *See* Crystal N. Skelton, *Cookies, Promises and California: Why the 3rd Circuit Revived Privacy Claims Against Google*, AD LAW ACCESS (Nov. 19, 2015), *archived at* https://perma.cc/8L4F-ZPCD (explaining a recent lawsuit against Google and why other companies that use cookies should pay attention to the 3rd Circuit's decision).

[98] *See id.* (suggesting that companies pay close attention to privacy practices and how data is being collected, used and shared in order to protect themselves).

[99] *See* In re Google Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 132 (3rd Cir. 2015) [hereinafter *In re Google*] (illustrating how Google was able to work around Safari's cookie blocking software). Defendants asserted several claims, under both federal and state law, against Google that were all related to the cookie blocking. *Id.* The defendants, including Google, were internet advertising companies that used third-party servers to place ads on various websites that the *plaintiffs* visited in order to target advertisements based on the users' browsing history. *Id.* at 130-31. The plaintiffs were Internet users that had made use of their web browsers cookie-blocking technology to prevent the use of third-party cookies on their computers. *Id.* at 131-32. Google and the other defendants were able to exploit loopholes in the cookie-blockers that allowed them to circumvent the protections and continue to place third party cookies on the plaintiffs' computers. *Id.* at 132.

[100] *See id.* at 131 (articulating the argument that was outlined in the complaint).

tiff must have both a legally protected privacy interest and a reasonable expectation of privacy; in addition, the intrusion must be so severe in "nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms."[101] The court highlighted that while a reasonable person may know that some of their browsing information will be sent to Google, the fact that these plaintiffs were under the assumption that the cookie-blockers were preventing this *information* from being collected gave them a subjective expectation of privacy that was reasonable under the circumstances.[102]

The court further established that due to the nature in which Google obtained the information – i.e. misleading consumers to believe that their cookie-blockers were preventing the placement of cookies on their web browsers—the actions could be considered an egregious breach of social norms and therefore, a reasonable jury could find an invasion of privacy had occurred.[103] In light of the fact that Google led users to believe that their cookie blockers were working to prevent the use of third-party cookies, the court determined that the plaintiffs were entitled to pursue their intrusion claim.[104]

The courts have continued to recognize that due to the prevalence of the Internet in our daily lives, protecting online privacy is an important justification for upholding the intrusion upon seclusion cause of action.[105] *In re Nickelodeon Consumer Privacy Litigation*,[106] the court revisited, and affirmed, whether Internet users could sustain an intrusion upon seclusion action against Internet advertising

[101] *See In re Google,* 806 F.3d at 149-50 (listing the elements for an invasion of privacy under the California formulation of the tort).
[102] *See id.* at 150 (theorizing that the explicit lying to consumers about whether the cookie blockers were actually working could support a finding of violation of the consumers' privacy).
[103] *See id.* at 150 (asserting that it is not simply whether the action itself would be an intrusion but how the action occurs). Google argued that the plaintiffs voluntarily sent the information to Google by using the web browser and cannot establish an invasion of privacy claim. *Id.*
[104] *See In re Google,* 806 F.3d at 151 (vacating the dismissal of the plaintiff's claims under the California Constitution and California tort law). The District Court dismissed the plaintiffs' claims on the basis that Google's actions were not egregious enough to meet the standard for an invasion of privacy. *Id.* at 150.
[105] *See* Justin Lee, *The Reasonable Expectation of Privacy*, AMERICAN BAR ASSOCIATION: PRACTICE EDGE, *archived at* https://perma.cc/HS9R-337R (illustrating how privacy issues in regards to technology have affected the way society thinks about the reasonable expectation of privacy).
[106] 827 F.3d 262 (3rd Cir. 2016) [hereinafter, *In re Nickelodeon*].

companies for placing cookies on their computers.[107] The plaintiffs claimed that Viacom and Google collected information about video watchers against an explicit statement that they would not collect any personal information.[108] Considering Viacom and Google failed to get permission to place the cookies and collect information from the users—and actually promised that they would not do just that—the Court determined that there had been an intentional intrusion on the seclusion of the users, which would be highly offensive to a reasonable person.[109] While the common law tort action for invasion of privacy has many similarities with the Fourth Amendment analysis, courts have placed much more emphasis on the ideas of notice and consent and what would be offensive to a reasonable person, especially when it comes to digital data collection.[110]

III. Facts

Following the success of Disneyland in California, Walt Disney set a new goal of changing the way that communities were structured and how members of that community interacted.[111] Disney believed that by integrating technology more seamlessly into

[107] *See id.* at 267 (stating that many of the claims made in the current case overlap with those alleged by the plaintiffs in *In re Google*).
[108] *See id.* (explaining the plaintiffs' intrusion upon seclusion claim). The plaintiffs, who were children under the age of thirteen, alleged that while completing the registration process in order to use the website "Nick.com," they were required to provide information such as their birthdate and gender. *Id.* at 268. Further, during the registration process, a notice to parents stated, "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!" *Id.* at 269. The plaintiffs also asserted a claim under the Video Privacy Protection Act. *Id.* at 278.
[109] *See* In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 293-94 (3rd Cir. 2016) (outlining the elements required for the intrusion claim and how they have been satisfied in the present case). A statement on the registration form for the website stated, "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!" *Id.* at 268-69.
[110] *See id.* at 294 (stating that the "presence or absence of consent" is a key factor in determining the validity of an intrusion upon seclusion claim).
[111] *See* SAM GENNAWEY, WALT DISNEY AND THE PROMISE OF PROGRESS CITY 128 (Bob McLain ed., 2014) (illustrating that Walt Disney did not like urban cities and wanted to change the way they were structured). Following World War II, an expansion of many urban cities resulted in lifeless cities with no personality. *Id.*

communities around the country, Americans would be able to fix many of the problems with transportation, housing, and urban management.[112] With this idea in mind, Walt Disney set out to create a new immersive experience: an Experimental Prototype Community of Tomorrow- EPCOT for short.[113] This community, which was intended to be a model for urban planners across the country, presented significant problems when faced with zoning laws.[114] In order to avoid red tape at every turn while designing this futuristic city, Walt Disney would have to find a way to prevent the government from getting in his way.[115]

Disney and his team initially looked to receive help from a government program implemented by President Lyndon B. Johnson, the Demonstration Cities and Metropolitan Development Act of 1966.[116] This Act was the result of the unrest in many metropolitan cities in the mid 1960s where one of the goals of the program was to "provide financial and technical assistance to develop 'new and imaginative proposals'" as well as "to promote the… application of new

Walt Disney wanted to fix this by creating communities where people would be able to experience life and create together. *Id.* at 130.

[112] *See id.* at 130 (highlighting Walt's desire to show everyone that by engaging with technology we could solve many of the problems faced by urban communities).

[113] *See id.*(detailing Walt Disney's vision for a community that would highlight American ingenuity and serve as a model for modern communities). Walt Disney stated, "[I}t's not another Disneyland. I have learned things. I have a better plan and an idea of what to do. This will not be a sequel. This will be a city where people will live, work and enjoy a better way of life." *Id.* at 139. *See also,* Shenk, *supra* note 7 (outlining the evolution of the concept for EPCOT).

[114] *See* GENNAWEY, *supra* note 111, at 143 (stating that another Disney executive convinced Walt and Roy Disney that creating their own municipality would allow them to maintain control over the land).

[115] *See* GENNAWEY, *supra* note 111, at 143 (discussing that by creating a new municipality, they would be able to limit interference from other government agencies); *see also* Dakota Gardner, *4 Powers You Didn't Know Walt Disney World Could Use*, THEME PARK TOURIST (Sept. 19, 2014), *archived at* https://perma.cc/JB4B-H9YD (articulating that Walt Disney knew that in order to succeed in his plan of creating such an experimental community, it would be necessary to avoid as much government back up as possible).

[116] *See* GENNAWEY, *supra* note 111 at 139 (highlighting that due to the sheer size of the Florida Project, the Disney team was fully aware that they would need some assistance in financing the project in order to make Walt's dream a reality).

and improved technologies."[117] However, maintaining control over the project was of paramount importance to Walt Disney, and he was unwilling to give up some of his control in order to gain assistance from the Federal Government.[118] A Florida attorney soon convinced Walt Disney that in order to obtain the level of control he was looking for, he would need to create his own municipality.[119]

After obtaining approval from the Florida legislature in 1967, the Disney Company was able to create a government structure that allowed them to maintain control over the land, residents and businesses within the almost 30,000 acres of land in central Florida.[120] The structure that was created was a "twin-tiered" government.[121] The Disney Company created two different cities: Lake Buena Vista and Bay Lake.[122] The residents of each city vote to elect city officials.[123] These city officials then turn over the management of publicly run services such as utilities, waste management, and emergency

[117] *See* GENNAWEY, *supra* note 111 at 139 (delineating the purposes and goals of the Demonstration Cities and Metropolitan Development Act of 1966, later known as the Model Cities Act).

[118] *See* GENNAWEY, *supra* note 111 at 139 (asserting that Disney was more interested in unrestrained control in order to fully realize his vision than he was in receiving financial assistance). *See also* Adrienne Vincent-Phoenix, *Starbucks and Disney: Behind the Beans,* MOUSEPLANET (Apr. 25, 2012), *archived at* https://perma.cc/FF8M-26U5 (illustrating that while the Disney company is willing to work with other entities, such as Starbucks, there is always a need to retain control).

[119] *See* GENNAWEY, *supra* note 111 at 143 (presenting a municipality as the best way to ensure limited review and oversight from other agencies).

[120] *See* Shenk, *supra* note 7 (detailing the reasons why Walt Disney sought to create his own government structure). Walt Disney initiated a vast lobbying campaign seeking exemption from local regulations and zoning laws. *Id.* This campaign included the blue print for his idea for EPCOT. *Id.* After Walt Disney's death in 1966, the Disney Company continued to pursue legislative approval of the plan, highlighting the advantages that unrestricted authority would bring to their ability to fulfill Walt Disney's plan. *Id.*

[121] *See* GENNAWEY, *supra* note 111, at 144 (explaining that the purpose of the two cities was to create an environment where the land was part of one municipality). In the twin-tiered system, there would be two general purpose governments that were fully controlled by a special purpose district on top. *Id.* The special-purpose district is controlled by the Disney Company. *Id.*

[122] *See* Shenk, *supra* note 7 (outlining what happened once the Disney Company got approval for their Florida Project).

[123] *See Reedy Creek Improvement District*, DISNEY PARK HISTORY (Oct. 27, 2017), *archived at* https://perma.cc/5EVR-NFQF (detailing the government structure of Bay Lake and Lake Buena Vista); *see also* GENNAWEY, *supra* note 111,111 at 144

services to the Reedy Creek Improvement District (RCID).[124] RCID, an independent government agency, is in charge of the basic day-to-day responsibilities of a normal municipality, such as fire protection, environmental protection, building codes, land use and planning, utilities and roads.[125] A Board of Supervisors that are elected by the landowners of the district run RCID.[126] This structure allows the Disney Company to do or construct almost anything they want without of fear of government intervention or regulation, including implementing new and experimental forms of technology.[127] While the

(illustrating that voting rights were a major issue that needed to be dealt with in determining what the government structure would look like). Walt Disney was well aware of the fact that in order to preserve the experimental nature of the community, it would be imperative for the company to maintain full control. *Id.* The solution was to restrict voting rights to property owners and the Disney Company was the sole owner of the property. *Id.* Anyone else that lived on the property would merely be leasing the property from the company. *Id.*

[124] *See* Shenk, *supra* note 7 (stating that the only task performed by the city councils of Lake Buena Vista and Bay Lake was to assign everything to RCID); *see also Reedy Creek Improvement District*, *supra* note 123 (listing all of the public services run by RCID).

[125] *See* Shenk, *supra* note 7 (outlining the structure and responsibilities of the Reedy Creek Improvement District); *see* GENNAWEY, *supra* note 111, at 144-45 (discussing the intertwined private and public nature of the RCID). It should be noted that while RCID is technically an independent agency, it is controlled by the Disney Company. *Id.* The RCID now has more power than many elected governments in the United States. *Id.*

[126] *See Reedy Creek Improvement District*, *supra* note 123 (describing the governance of RCID, specifically distinguishing the Board of Supervisors and officials of the cities). The landowners of Bay Lake and Lake Buena Vista are senior employees of the Disney Company and their families. *Id.* Each owns a five-acre lot of land, which is the only land within the district that is privately owned and not controlled by the Disney Company. *Id.* While there are approximately forty residents that live in communities within Bay Lake and Lake Buena Vista, these residents are not landowners and, therefore, cannot vote for the Board of Supervisors. *Id. See also* GENNAWEY, *supra* note 111, at 145 (stating that the governor of Florida once told Roy Disney, "I've studied the Reedy Creek Improvement District. It's very comprehensive. I notice only one omission. You made no provision for the crown"). Allowing the Disney Company to maintain control over the RCID ensures that they, and they alone, have the ability to control anything that happens on the property. *Id.*

[127] *See Reedy Creek Improvement District*, *supra* note 123 (suggesting that the "far-reaching powers" awarded to RCID allows the Disney Company to have a large amount of control over the land). At one point, the Disney Company considered building a nuclear power plant but eventually settled on a traditional power source. *Id.*

world would never see Walt Disney's dream of a community where residents live, work and play while engaging with technology in order to solve today's urban problems, the structure of Disney's government and the creation of the RCID have allowed the Disney Company to continue to experiment with and develop new technologies to enhance the consumer experience.[128]

One of these new technologies, the MagicBand system, illustrates how technology can be used to streamline many daily activities.[129] The MagicBand is an "all-in-one" wearable device that allows guests to control almost every aspect of their vacation.[130] The process begins when guests make a reservation for a Disney hotel online.[131] After making a hotel reservation, guests are allowed to either customize a plastic wristband with their name and a particular color, or opt out of the system all together by accessing their account on the website.[132] The wristband corresponds to an online system

[128] *See* Shenk, *supra* note 7 (highlighting that Walt Disney's desire for his theme parks was to create an "alternate reality").

[129] *See* Kuang, *supra* note 4 (discussing how the idea for the MagicBand system came to be and what the goals of the project were). The idea for a frictionless system was first suggested in 2008 by then Disney World President, Meg Crofton. *Id.* Over the next five years, Disney executives, engineers and other employees worked on every aspect of the system until the MagicBand System was first introduced in limited public tests in 2013. *Id.* The Walt Disney Company has continued to improve and add new features to the MagicBand system. *Id.*; *see also* Thomas Smith, *MagicBand 2 Coming to Walt Disney World Resort*, DISNEY PARKS BLOG (Nov. 19, 2016), *archived at* https://perma.cc/WDD4-66LD (illustrating the new wristband design that the company came out with in late 2016).

[130] *See FAQs: What is a MagicBand?*, DISNEY HELP CENTER (Nov. 27, 2016), *archived at* https://perma.cc/W5E7-M2DD (outlining what the MagicBand system can do). The MagicBand serves as a guest's hotel room key, provides access to Disney World's ride reservation system, and can be used to purchase food and merchandise. *Id.*

[131] *See FAQs: How can I get a MagicBand?*, DISNEY HELP CENTER, *archived at* https://perma.cc/R83E-7QZ3 (stating that MagicBands are available for Annual Pass holders and Walt Disney World Resort guests).

[132] *See* Anthony Murphy, *The Good, the Bad, and the Ugly of Disney's Magic Bands*, THEME PARK INSIDER (Nov. 4, 2013), *archived at* https://perma.cc/M5VH-84KG (explaining the details of the system and how guests are introduced to it); *see also FAQs: What happens if I don't customize my MagicBand?*, DISNEY HELP CENTER (Mar. 5, 2017), *archived at* https://perma.cc/A4LN-7YP5 (articulating what happens if a guest fails to customize his or her MagicBand). As the site makes clear, failure to customize a MagicBand does not automatically opt one out of the system. *Id.* Instead, one must affirmatively opt out of the system, otherwise she

known as My Disney Experience, where guests are able to create dining reservations, make FastPass+ reservations for certain attractions, and plan other details of their vacation ahead of time.[133] The connection between the MagicBand and My Disney Experience systems illustrate the way that the system as a whole integrates technology into the in-park activities.[134]

Each wristband uses a radio frequency identification device (RFID) that communicates reservations and guest information from My Disney Experience to long and short range "readers" within the park.[135] The RFID chip in the wristband stores the data from the online system and communicates this data when activated by an electromagnetic wave, created by the reader.[136] In Disney World, these readers are located at the entrance to the park, on rides and attractions, at the cash register in restaurants and stores, and within the resort hotels.[137]

---

will still receive an un-customized MagicBand that is attached to her personal account. *Id.*

[133] *See FAQs: What is a MagicBand?*, *supra* note 130 (detailing how the MagicBand system is connected to the choices made by guests while planning their vacation online); *see also* Beth Gorden, *Everything You Need to Know about Disney MagicBands*, 123 HOMESCHOOL 4 ME (Oct. 31, 2013), *archived at* https://perma.cc/2GE9-T5H2 (providing information on the services provided by the MagicBand and MyMagic+ systems).

[134] *See* Kuang, *supra* note 4 (emphasizing the seamless integration of the MagicBand system into the Disney experience); *see also FAQs: What is a MagicBand?*, *supra* note 130 (highlighting the connection between the MagicBand and My Disney Experience Systems); Murphy, *supra* note 132 (differentiating between the positive and negative effects of the MagicBand system on the in-park experience).

[135] *See FAQs: How do I use my MagicBand?*, *supra* note 3 (outlining how the MagicBand system works); *see also* Adam Clark Estes, *How I Let Disney Track My Every Move*, GIZMODO (Mar. 28, 2017), *archived at* https://perma.cc/BYM8-UE68 (illustrating the convenience that the MagicBand system adds by allowing users to book rides ahead of time and make cashless purchases in stores).

[136] *See* Kevin Bonsor & Wesley Fenlon, *How RFID Works: RFID Tags Past and Present*, HOW STUFF WORKS (Nov. 5, 2007), *archived at* https://perma.cc/JH7K-J4L4 (explaining how RFID technology communicates data). The antenna located in the RFID reader creates electromagnetic energy that can be detected by the antennae located in the RFID chip. *Id.* The chip then uses power from an internal power source to send data back the reader through radio waves. *Id.* The reader translates these radio waves into readable data. *Id.*

[137] *See FAQs: How do I use my MagicBand?*, *supra* note 3 (highlighting a few of the ways in which the RFID readers are integrated into the theme park experience).

While this system helps streamline and enhance the vacation experience for the guests, the Disney Company is also able to track MagicBand users as they move around the park.[138] The privacy policy for the MagicBand system states that "certain information" will be tracked through means "other than the My Disney Experience website and mobile app" while a guest is located within the park.[139] This data collection technique is used to collect any and all information about guests that the Disney Company can use to not only enhance the guest experience, but also ensure that these guests will continue to return to and spend their money in the parks.[140]

RFID technology is used in a variety of different industries to track products, animals and people.[141] But with the increased popularity of RFID technology, many are concerned that invasion of privacy will become a much larger issue.[142] These concerns are particularly important to the use of RFID chips in the MagicBand

---

[138] *See Making the Band — MagicBand Teardown and More*, ATDISNEYAGAIN (Jan. 27, 2014), *archived at* https://perma.cc/4H39-WUPM (stating that due to the particular design of Disney's MagicBands, the bands are able to communicate data over a longer distance, allowing Disney to collect data from all over the park); *see also* Foreman, *supra* note 10 (highlighting the fact that Disney markets the MagicBand system as a way to improve guest experiences).

[139] *See FAQS: My Disney Experience*, DISNEY HELP CENTER (Nov. 27, 2016), *archived at* https://perma.cc/Q6LU-DMCD (laying out how different types of data are collected through the My Disney Experience and MagicBand systems). While the privacy policy discusses how data is collected, how it may be shared and how guests can opt out of the system, there are not details given on what information is used and why. *Id.*

[140] *See* Foreman, *supra* note 10 (listing just a few of the questions that guest information and data can help answer). Foreman suggests that much more can be learned from human interactions in the "meat space," or real life, than can be learned from online profiles and transactions. *Id.*

[141] *See* Bonsor & Fenlon*, supra* note 136 (illustrating different uses for RFID technology).

[142] *See* Bonsor & Fenlon*, supra* note 136 (criticizing the potential expansion of the use of RFID technology to one day be used for mandatory human chipping); Robert Malone, *Can RFID Invade Your Privacy?*, FORBES (Dec. 7, 2006), *archived at* https://perma.cc/6GS5-NLS9 (detailing potential privacy concerns and how some states are addressing these problems); *see also* Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C. R. C. L. REV. 133, 140-43 (2006) (establishing that the unique nature of RFID's ability to automate aspects of the data collection process poses significant privacy implications); Darren Handler, *The Wild, Wild West: A Privacy Showdown on the Radio Frequency Identification (RFID) Technology Systems Technological Frontier*, 32 W ST. L. REV. 199, 201-02 (2005) (providing

system.[143] There is a significant amount of personal information that is attached to the online accounts of guests using the MagicBand system, making the ability to remotely read the data on these cards a serious personal security threat.[144] The Disney Company's ability to track individual movement within the park is also concerning for many people as it feels like a severe invasion of privacy.[145] While Walt Disney's vision for integrating technology with daily life was meant to solve many problems, it seems that this idea has opened the door for more issues.[146]

IV. Analysis

As stated above, Disney World walks a very narrow line between public and private.[147] In order to better understand the privacy implications of the MagicBand system, Disney World's public or private status must first be established.[148] First, it must be determined whether or not Disney World would qualify as a State Actor.[149] As-

some of the concerns that arise with the ability to collect massive amounts of personal data)

[143] *See* Quinn R. Shamblin, *The Magic of Disney MagicBands,* CSO ONLINE (Jan. 12, 2015), *archived at* https://perma.cc/3G9T-K78J (detailing some of the privacy and security risks presented by the MagicBand system).

[144] *See id.* (suggesting that recent security breaches of major corporations such as Target and Home Depot could mean that Disney World could soon be a target for hackers and other "bad guys"). Personal information attached to the online profile include your name, address, credit card number and personal PIN number. *Id.* Shamblin also emphasizes that no company can ensure that their information is 100% safe from a security breach. *Id.*

[145] *See id.* (citing NSA-style surveillance as another privacy concern for many people). People are very wary of government agencies that are able to track every move that they make both on or offline. *Id.*

[146] *See* GENNAWEY, *supra* note 111, at 129-30 (restating that Walt Disney wished to use technology to solve many modern urban problems faced after World War II).

[147] *See* Shenk, *supra* note 7 (establishing the way that Walt Disney World walks the line between public and private). As stated above, due to the unique structure of Disney World's form of government, the public and private aspects of Disney World are substantially intertwined. *Id.* The intertwined nature complicates the state actor analysis by making it difficult to decide which actor and what conduct is at issue. *Id.*

[148] *See* Niles, et. al., *supra* note 19, at 886-87 (stating that the Constitution only applies to state actors).

[149] *See infra* Part IV(A) (walking through the state actor analysis established by Niles, Tribble, and Wimsatt).

suming that Disney World can be classified as a state actor, it is important to analyze how the Fourth Amendment may be applied to the MagicBand system.[150] Finally, in the alternative, this Note will suggest that Disney World may still be considered liable under the tort theory of intrusion upon seclusion.[151]

A. Is Walt Disney World a State Actor?

Disney World's unique government structure makes it somewhat difficult to discern which category the community fits.[152] Niles, Tribble, and Wimsatt created an analysis, which suggests an answer as to whether Disney World is a state actor.[153]

First, one must identify the conduct at issue and to whom said conduct is attributable to.[154] For this particular analysis, this normally easy question becomes more complicated due to the number of actors that are interconnected.[155] For example, the corporation owns the land, which is regulated by the local governments of Bay Lake and Lake Buena Vista and maintained by the RDIC, which is controlled by the Disney Company.[156] Additionally, the corporation runs

[150] *See infra* Part IV(B) (determining that the MagicBand system poses serious privacy questions under the Fourth Amendment).
[151] *See infra* Part IV(C) (outlining the ways in which Disney World could be held liable if it is not found to be a state actor).
[152] *See* Shenk, *supra* note 7 (highlighting the unique government structure of Walt Disney World). *See also,* Gennawey, *supra* note 111, at 144 (providing a description of why the government structure of Disney World is so unique and allows for the most control). The twin-tiered system consists of two general-purpose city governments, both of which are controlled by the special-purpose district government, the RCID. *Id.* The RCID itself is controlled by the Disney Company. *Id.*
[153] *See* Niles, et. al. *supra* note 19, at 887-88 (articulating how to apply the state action doctrine). The authors explain that the different approaches which courts have taken in analyzing the state actor question, have resulted in a myriad of scholars attempting to give meaning to these different theories. *Id.* at 898. The authors suggest that all of these approaches can be consolidated into a single theory which they proceed to explain in detail. *Id.* at 898-99.
[154] *See* Niles, et. al., *supra* note 19, at 898 (outlining the first step in a state action analysis).
[155] *See* Shenk, *supra* note 7 (discussing the blueprint of the massive infrastructure supporting Walt Disney World's operation).
[156] *See* Shenk, *supra* note 7 (introducing the way that Lake Buena Vista and Bay Lake give control of certain jobs to the RCID). The RCID is in charge of waste

the theme parks, hotels, shops and restaurants.[157] However, when taking into consideration the fact that the MagicBands are issued by the Disney Company itself, rather than the cities of Bay Lake and Lake Buena Vista or the RDIC, it becomes evident that the actor and conduct at issue in this case is the Disney Company's use of RFID technology in conjunction with the MagicBand system to collect large amounts of data from their visitors.[158]

After identifying the Walt Disney Company as the actor at issue, the next step is to identify whether the company is public or private in nature.[159] The Walt Disney Company is a publicly traded corporation, and therefore does not qualify as a governmental entity itself.[160] However, a non-governmental entity may still be classified as public in nature if they are controlled by a governmental entity.[161] While there is still a question about how much government control is required in order to justify a determination that a non-governmental entity is public in nature, the argument is that there are cases where the private entity and the state are too inextricably linked to shield the

management, fire and environmental protection, emergency services, roads, transportation, building codes, and land use. *Id. See also Reedy Creek Improvement District*, *supra* note 123 (noting the responsibilities and services the RCID).

[157] *See* Shenk, *supra* note 7 (showing how the Walt Disney Corporation still has control over all aspects of the park themselves). *See also* Vincent-Phoenix, *Starbucks and Disney: Behind the Beans,* MOUSEPLANET (Apr. 25, 2012), *archived at* https://perma.cc/FF8M-26U5 (providing an example of how the Disney Company has contracted with Starbucks so that they can do business in the parks). While Starbucks is allowed to conduct business on the property, they have mutually agreed upon terms. *Id.*

[158] *See FAQs: How can I get a MagicBand?*, *supra* note 131 (detailing that the MagicBands are distributed in conjunction with a hotel reservation through the Disney Company's website).

[159] *See* Niles, et. al., *supra* note 19, at 901-02 (illustrating the application of the second step of the state action analysis to a real case). This step is important because, as stated above, the Constitution can only be applied to actors that can be classified as state actors. *Id.*

[160] *See Walt Disney Company,* BLOOMBERG MARKETS (Oct. 31, 2017), *archived at* https://perma.cc/W8AZ-3ZGL (detailing Disney's presence on the stock market). *See also* Niles, et. al., *supra* note 19, at 902 (defining a government entity as either a body that makes up some level of local, state, or federal government or an entity that is controlled by a governmental entity). There is no need for further analysis, when a company is owned privately or by stockholders, because they cannot be considered a government entity. *Id.*

[161] *See* Niles, et al., *supra* note 19, at 901-02 (illustrating that in cases where there is a high degree of state ownership and control, a private entity may be found to be a state actor).

private actor from being held liable for constitutional violations.[162] A situation like this has yet to be decided in court, however, it is arguably a case where the private actor, such as the Disney Company, and the state, (in this case, the city governments of Bay Lake and Lake Buena Vista), are so entwined that a determination classifying the Walt Disney Company as public in nature is necessary.[163]

Even if it is determined that the Walt Disney Company is not a government entity, they may still be considered a state actor if they have acted in a capacity that is typically reserved for the state.[164] If we follow the analysis of *Marsh v. Alabama*, then it is clear that RCID could be considered a state actor due to their control over the basic functions typically reserved for the city.[165] However, since the specific conduct at issue in this analysis is the sale and use of the MagicBands in the collection of guest information, the reasoning of

[162] *See* Jackson v. Metropolitan Edison Co., 419 U.S. 345, 351 (1974) (establishing that a "sufficiently close nexus" must be found to exist between the state and the state-regulated entity). In *Jackson*, the Court found that State regulation was not enough to say that there was sufficiently close nexus between the private utility company and the State in order to hold the private entity liable for a Constitutional violation. *Id.*

[163] *See id.* (highlighting the necessity for the nexus in order to find a private actor and a state actor sufficiently connected). *See also* GENNAWEY, *supra* note 111, at 144-45 (suggesting that because the Disney Company maintains control over the RCID and the RCID maintains control over the Disney World property, the Disney Company has unprecedented control over the park).

[164] *See* Niles, et al., *supra* note 19, at 901 (expressing that the next step in the state actor analysis for the courts is to determine whether the private actor's conduct is sufficiently public in nature to say that the private entity acted in a public capacity during the conduct at issue).

[165] *See* Marsh v. Alabama, 326 U.S. 501, 506 (1946) (stating that the more a particular function is performed in order to benefit the public, the more likely it is to be considered one that is typically reserved for the state). The *Marsh* Court highlighted that a private shipping company could be held liable for a violation of the Constitution because they were acting in place of the local government that exists in normal municipalities. *Id.* Here, the conduct at issue is that of the Disney Company, which is not acting in the place of the local government. *See FAQs: What is a MagicBand?*, *supra* note 130 (helping to establish that the actor in question is really the Disney Company).

the *Marsh* Court does not fit as easily.[166] In *Marsh* the conduct at issue was the company exercising their power as a municipality.[167] This is different than the sale of a product by a company, such as the Disney Company's sale and use of the MagicBands, to collect data on its customers, which is the conduct at issue here.[168]

Following this reasoning, it is unlikely that the Walt Disney Company would be found to be a public actor in terms of the state actor analysis.[169] However, it is possible that the Walt Disney Company may still be found to be a state actor if the state's interaction in the conduct is "sufficient for the deprivation to be fairly attributable to the state."[170] In order to make this determination courts will look to whether the state intended to take action that would cause the constitutional violation to be more likely to occur.[171]

The reasoning in *Jackson v. Metropolitan Edison Company* might shed more light on how a court would analyze the public nature of a corporation that holds a monopoly in a certain geographic

---

[166] *See Marsh*, 326 U.S. at 507 (highlighting that it is not the corporation's property interest in the town that creates the issue, but rather the control over the municipality and its citizens). Likewise, the Walt Disney Company's ownership of the land is not enough to justify a finding of state action. *Id.* Furthermore, since the Walt Disney Company does not directly control the municipality, there is not a basis to find state action in the same way as in the *Marsh* case. *Id.*

[167] *See id.* at 503 (detailing the conduct that allegedly violated the Constitution was the company-municipality's attempt to restrict the plaintiff from distributing religious pamphlets on the side walk).

[168] *See FAQs: What is a MagicBand?*, *supra* note 130 (illustrating that the MagicBand system is established and used by the Walt Disney Company).

[169] *See* Niles, et al., *supra* note 19, at 910 (establishing that only government entities and non-governmental entities acting in a public capacity are automatically subject to constitutional scrutiny under a state actor analysis).

[170] *See* Niles, et al. *supra* note 19, at 910-11 (detailing the third and final step in the state actor analysis). The last question in determining whether a private entity can be held liable as a state actor is whether the State interacted with the private entity in such a way that the conduct may be attributed to the State. *Id.* In order to be held liable, the State's interaction has to fall somewhere in between permission and encouragement to the private actor in performing the conduct at issue. *Id.*

[171] *See* Niles, et al., *supra* note 19, at 912-13 (articulating how the conduct of a state actor can be attributed to the state). The authors articulate that there are varying levels of state interaction with the private entity. *Id.* While prohibition of the conduct, discouragement of the conduct and passive permission of the conduct are not enough to determine that the state was sufficiently involved in the conduct, active encouragement and mandating the conduct at issue are enough. *Id.* The difficulty lies in when a certain case, the conduct, such as in the case of Disney World, falls somewhere in between permission and encouragement. *Id.*

area.[172] Applied to this case, the Jackson Court's reasoning would establish that while mere regulation and certification of the private actor is not enough to warrant a state actor determination, there is a higher level of support given to Walt Disney World through the local government.[173] In fact, the local government has been structured in a way that would make it easier for the Walt Disney Company to operate without fear of interference from outside government influences.[174] This makes it clear, that the state, (the city governments), is sufficiently encouraging to the private actor, (the Walt Disney Company), in their use of the MagicBand system.[175]

B. MagicBand Privacy Implications under a State Actor Analysis

Due to the finding that Disney World is a state actor, it is likely that the Court would analyze the MagicBand system's potential privacy issues as a violation under the Fourth Amendment of the

[172] *See* Jackson v. Metropolitan Edison Co., 419 U.S. 345, 351 (1974) (explaining that the actions of a state regulated monopoly may more readily be found to be a state actor). In *Jackson* the Court looked at whether a private utility company violated the Due Process Clause by shutting off a customer's utilities for a failure to make payments. *Id.* at 348. The customer asserted that because the State issued a certificate to conduct business to the utility company, they had inherently authorized the conduct at issue. *Id.* at 350-51. The court held that issuing a license to a utility company is not sufficient to allow the conduct of the private actor to be attributed to the state. *Id.* at 358-59.

[173] *See* Shenk, *supra* note 7 (illustrating the structure and interdependence of the Walt Disney Company and the local governments of Bay Lake and Lake Buena Vista); *see also* GENNAWEY, *supra* note 111, at 144 (highlighting the amount of control that the Disney Company has over the RCID and the Disney World property). Unlike in *Jackson*, the state entity, RCID, did not mere grant the Walt Disney Company a license to conduct business. *Id.* at 145. The Disney Company controls RCID who then grants them the ability to conduct business and essentially do whatever they want. *Id.* This is arguably enough to attribute the conduct of the Disney Company to the RCID. *Id.*

[174] *See* Shenk, *supra* note 7 (implying that Walt Disney World has a unique government structure in order to avoid government red tape).

[175] *See* Niles, et. al., *supra* note 19, at 910-13 (asserting how a non-state actor may become liable for a Fourth Amendment violation if they have sufficient support from the state).

Constitution.[176] To do this, the first step is to establish whether visitors to Walt Disney World would have a reasonable expectation of privacy while in the parks.[177] While the visitors to Walt Disney World have placed themselves in the public light and therefore should have little to no expectation of privacy, according to the reasoning in *Katz*, the mere presence in a public space, such as a phone booth or an amusement park, is not enough to establish that individuals have given up all expectation of privacy.[178] Visitors to the parks would arguably not be comfortable with someone knowing what they ate for lunch, when and how often they go to the bathroom in the parks, and where they are within the facility at any given point of the day.[179] This would imply that there is at least some information that is collected by the MagicBand system that visitors would prefer to keep private.[180] Additionally, the information that is being collected and used by the company is the type of information that could allow a person to create a detailed and descriptive profile of the individual guest that amounts to more information than what the individual is able to express by simply being in public.[181] Following this line of reasoning, it is likely that an individual would have the same expectation of privacy in an amusement park such as Walt Disney World that he or she would have in the phone booth at issue in *Katz*.[182]

---

[176] *See* POSNER, *supra* note 53 (suggesting the starting point for Fourth Amendment analysis after a state actor has been established).

[177] *See* Burten, *supra* note 55, at 361 (articulating the "reasonable expectation of privacy" standard for Fourth Amendment analysis); *see also* LAWRENCE *supra* note 83 (defining a reasonable expectation of privacy as one where both the individual and society as a whole would recognize as reasonable to want to keep private or secluded).

[178] *See* Katz v. United States, 389 U.S. 347, 351 (1967) (stating that what a person seeks to preserve as private, even when in a public space, is still subject to the Fourth Amendment).

[179] *See* Foreman, *supra* note 10 (illustrating a few of the ways that Walt Disney World is able to peek into a visitor's life while they are visiting the park).

[180] *See* Foreman, *supra* note 1010 (suggesting that many visitors would not be comfortable with this information being collected).

[181] *See* Burten, *supra* note 55, at 369 (highlighting that the aggregation of certain information through the use of technology has the ability to be more invasive than what can be collected about an individual by simply observing them in public). *But see* Estes, *supra* note 135 (stating that Disney executives have insisted that the MagicBand system de-identifies personal information and expresses doubt as to how this might work).

[182] *See Katz*, 389 U.S. at 359 (establishing that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures").

Proving that society recognizes the expectation of privacy as reasonable is a more difficult analysis.[183] In this determination, the most important factor is whether or not there was a knowing exposure to the public.[184] This is a particular issue for any claim that is made against Walt Disney World, because participating in the MagicBand system is voluntary.[185] If people are voluntarily taking part in the system, then this would imply that they are knowingly exposing themselves to the surveillance and privacy implications that are associated with the system.[186] While it is true that visitors consent to the MagicBand system, it is unclear how much information they are given about what and how the company uses their information.[187] Without this active consent, the visitors have arguably not made a *knowing* exposure of their private information to the public.[188] Without a knowing exposure, it is likely for a court to find that

In *Katz*, the Court stated that even though a person may be out in public there is still personal information that he may wish to keep secret. *Id.* at 352. Likewise, while a visitor to Disney World may be technically in public, there may be certain aspects of their day that they do not wish to broadcast to everyone. *Id. See also* Foreman*, supra* note 10 (establishing some of the intimate details that may be collected by the Disney Company through the use of the MagicBand system). Examples of this information includes what you ate for breakfast, how often you use the restroom while in the parks, and how much you are spending in the gift shops. *Id.*

[183] *See* Burten, *supra* note 55, at 366 (stating that the second prong of reasonable expectation determination is difficult because one has to decide how to frame "society").

[184] *See* Burten, *supra* note 55, at 366 (describing the weight that is given to the knowing disclosure factor).

[185] *See* Kuang, *supra* note 4 (suggesting that while surveillance makes people nervous, they are also very excited to participate in the MagicBand and similar systems); *see also See FAQs: How can I get a MagicBand?, supra* note 131 (articulating that if you do not qualify for a MagicBand or chose to not participate you will receive a plastic card as your park ticket).

[186] *See* Kuang, *supra* note 4 (implying that by participating in the system, "your consent has simply been assumed.").

[187] *See FAQs: What is a MagicBand?*, *supra* note 130 (highlighting the small amount of information collected through the MagicBand system). The information provided on what is collected through the MagicBand system is very limited and general. *Id.*

[188] *See* Burten, *supra* note 55, at 367 (pointing to the importance of a knowing exposure in the reasonable expectation analysis).

society would recognize a reasonable expectation of privacy for visitors to Walt Disney World.[189] Since it is likely that a court would recognize that there is a reasonable expectation of privacy for a visitor at Walt Disney World, and Walt Disney World collects large amounts of private information about these visitors through the MagicBand system, it is likely that the court would also find that this system violates the Fourth Amendment.[190]

C. MagicBand Privacy Implications under a Non-State Actor Analysis

In the event that Walt Disney World is determined to not be a state actor, they may still be liable to an individual under the tort theory of intrusion upon seclusion.[191] As noted above, due to the scope of the information that the Walt Disney Company is able to collect through the MagicBand system and the average visitor's lack of knowledge about how this information is used, it is likely that the intrusion will be considered enough to make it past the initial threshold question.[192] Furthermore, by following the analysis of the Court in *In re Google*, the Walt Disney Company could be liable for a seclusion action.[193] If the court were to find that by advertising the MagicBand

[189] *See* Burten, *supra* note 55, at 366-67 (arguing that without a knowing disclosure, it is more difficult to find that there was not a violation of a reasonable expectation of privacy).

[190] *See* Posner, *supra* note 53 (asserting that once a determination that a reasonable expectation of privacy has been made, the violation of the Fourth Amendment becomes evident.).

[191] *See* RAYSMAN, *supra* note 93 (establishing that GPS and RFID technologies have been the subject of many intrusion upon seclusion actions after becoming more commonly used technologies); *see also* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW. INST. 1977) (defining the elements for an intrusion upon seclusion action). As stated above, in order to assert an intrusion upon seclusion claim, the complainant must be able to prove that (1) there was an intentional intrusion (2) into an area of privacy, (3) and that the interference is one that would be highly offensive to a reasonable person. *Id.*

[192] *See infra* Part II (B); *see also* Shulman v. Group W Prods., Inc., 955 P.2d 469, 490 (1998) (pointing to the need for the violation to be sufficiently invasive in order to sustain an action for intrusion upon seclusion).

[193] *See e.g., In re Google,* 806 F.3d 125, 151 (2015) (finding Google liable for failing to properly inform consumers of their use of third-party cookies); *see also In re Nickelodeon*, 827 F.3d 262, 294 (2016) (imposing liability on Viacom for promising to no collect any information from children and then proceeding to collect information about their browsing habits).

system purely as a way to enhance the guest experience without fully informing them about how their information is collected and used, they are misleading customers in the same way that the Google users were misled about their cookie use.[194]

The issue of consent could also affect a court's determination in an intrusion upon seclusion action, like in *In re Nickelodeon*.[195] As mentioned above, while Walt Disney World does require the guest to consent to participation in the MagicBand system, they also do not include all of the information about how data is collected and used through the system.[196] While the users in *In re Nickelodeon* did not give consent to the collection of information at all, many guests that participate in the MagicBand system are not fully aware of what exactly they have consented to.[197] This lack of consent could implicate Walt Disney World in intrusion actions in a similar way that it has for the companies involved in both *Google* and *Nickelodeon*.[198]

However, there is an argument to be made that consumers consent to this level of surveillance because of the benefits that it provides.[199] For Disney World guests, these benefits could be as simple

---

[194] *See In re Google,* 806 F.3d at 151 (implying that the way that Google collected user information through misleading them to believe that cookies were disabled lead to the Court's ultimate decision). In *In re Google*, Google was using the information collected through the cookies to create a detailed profile of individual users in order to tailor advertisements. *Id.* at 131. Disney uses the information collected about you in a similar vein: "to enhance your experience at the Walt Disney World Resort." *See also My Disney Experience- Frequently Asked Questions*, HELP CENTER (Mar. 5, 2017), *archived at* https://perma.cc/463F-ACUS (providing very little information about how the information will be used).

[195] *See In re Nickelodeon,* 827 F.3d at 293-94 (establishing that the lack of consent from the users was important in the court's decision). The Court asserted that the presence or absence of consent is a key factor in an intrusion upon seclusion claim and one that is weighed heavily in many courts' analysis. *Id.*

[196] *See infra* Part II (B); *see also FAQs: What is a MagicBand?: What is a MagicBand*, *supra* note 130 (showing the lack of information that is provided about how the MagicBand system operates).

[197] *See In re Nickelodeon,* 827 F.3d at 294 (asserting that consent was absent due to the notice provided to parents); Foreman, *supra* note 10 (highlighting the fact that many users of the MagicBands are not aware of how the system operates).

[198] *See e.g. In re Google,* 806 F.3d at 151 (illustrating the need for accurate information about how information is being used after being collected from consumers); *see also In re Nickelodeon,* 827 F.3d at 293-94 (detailing the importance of getting consent from consumers before their information is collected and used).

[199] *See* Estes, *supra* note 135 (suggesting that consumers will consent to participate in the system in order to enjoy the benefits that are provided); Foreman, *supra* note

as streamlined dining reservations, making advanced Fast Pass+ plans, and being able to make purchases with a tap of the wrist.[200] But these benefits may extend to helping a family reunite with a lost child and reducing security risks.[201] These benefits arguably overshadow any potential privacy issues, and weigh in favor of the system as whole – if consumers are going to be under surveillance, as in the case of many aspects of life today, it might as well be one that provides some incentive for them as well.[202]

It now becomes clear that while the status of Walt Disney World as a state actor has important implications on the ability of the individuals to bring a successful action for an invasion of privacy, there are still ways to protect individuals regardless of the ultimate determination.[203]

D. How to Protect Against Privacy Violations

One of the major concerns about RFID technology's use in a consumer context is that because RFID chips are readable over a further distance than other technology such as barcodes or microchips, anyone with the ability to create an RFID reader will be able to access and read the data stored on the RFID chip – including the personal information stored on it.[204] Another concern is that the RFID tags that are attached to individuals will allow those with the proper technology to track where a person has been at any given point in

10 (highlighting that there are many places where we implicitly consent to surveillance and data collection in order to reap the benefits that such systems supply).

[200] *See* Foreman, *supra* note 10 (outlining many of the ways that the MagicBand system can improve guests' vacations).

[201] *See* Gorden, *supra* note 133 (providing information on how lost children may be reunited with his or her parents after wandering off). Because a child's MagicBand must be linked to an adult account, the adult's personal information, including contact information like a phone number, is also linked to that child's MagicBand. *Id.* A cast member that comes across a lost child will be able to scan the wristband and contact the adults. *Id.*

[202] *See* Estes, *supra* note 135 (arguing that we are always under some form of surveillance and Disney's form of surveillance provides more benefits than some of the others that we often agree to as consumers anyway).

[203] *See* Burten, *supra* note 55, at 383 (implying that there are many theories on the best way to approach privacy law and individual privacy protection).

[204] *See* Malone, *supra* note 142 (articulating that the powerful nature of the RFID chips opens up more room for an invasion of privacy if the technology is abused).

time without the individual's knowledge.[205] In order to mitigate these concerns, some states have attempted to pass legislation that addresses individual problems with the technology.[206] Even though there have been attempts to achieve broad protection against violations of privacy using RFID technology, these attempts have been mostly unsuccessful.[207] This is thought to be due largely to the concern that it is hard to pass legislation that addresses all of the privacy concerns without too severely impacting the permissible uses of RFID technology that do not pose a threat to privacy.[208] Some scholars have also suggested that in the state actor context, it would be more beneficial to protect consumer privacy under other constitutional provisions, such as the First and Fifth Amendments.[209]

Still, under the current state of legislation, the best way to protect against privacy violations is for the company to self-regulate itself and implement their own policies to prevent potential litigation.[210] Utilizing mechanisms of notice and consent in the company policy is considered to be the best practice for companies that are looking to utilize RFID technology to collect information about their

[205] *See* Malone, *supra* note 142 (expanding upon the idea that when RFID tags are attached to products used by consumers, they can be used to track the individual consumer); *see also* Darren Handler, *supra* note 142, at 211 (2005) (suggesting that RFID's capability to monitor consumers in everyday life and create a full profile of the individual is the root of the danger with privacy implications).

[206] *See Radio Frequency Identification (RFID) Privacy Laws*, *supra* note 13 (listing states that have passed legislation restricting mandatory RFID chip implantation, prohibiting "skimming" in RFID identification cards, addressing the ability to use RFID in driver's licenses and prohibiting the use of RFID to track students).

[207] *See* Hildner, *supra* note 142, at 144 (stating that while there have been many attempts at passing legislation none of them have been comprehensive and the mismatched coverage leaves gaps open in the protection of consumers).

[208] *See* Hildner, *supra* note 142, at 149 (indicating that the industry's reluctance to support legislation is due to the fact that the progress of technology is unpredictable and they do not want the legislature to over step and prevent the ability to innovate).

[209] *See* Burten, *supra* note 55, at 383 (suggesting that as technology continues to advance, courts should move away from upholding a right to privacy under a Fourth Amendment analysis, and move towards recognizing a cause of action under either substantive due process or First Amendment rights).

[210] *See* Reidenberg, et. al., *supra* note 96, at 486 (asserting that the industry still views self-regulation as the best way to protect themselves from potential privacy violations).

consumers.[211] However, companies must be wary of implementing notices to consumers that are too vague and non-descriptive to support a finding that the consumer was fully informed about the use of the technology.[212] In order to effectively implement proper notice to consumers, GS1 suggests that companies wishing to use RFID technology: (1) give clear notice to consumers when RFID technology is being used, (2) inform consumers of their choice to remove or opt out of the use of RFID, (3) provide access to accurate information to consumers about the use of RFID technology, and (4) ensure that information collected through the use of RFID technology is appropriately collected and secured.[213] While the notice and choice framework has its flaws, providing detailed information to consumers is still currently the best advice to give to companies and other entities wishing to implement RFID technology.[214]

V. Conclusion

As the proceeding discussion has illustrated, there are many reasons that companies and other private actors should be aware of how privacy law may apply to them. With rapidly developing technology, there are many temptations to use these advances to improve and streamline business models. However, as the case of Disney World's MagicBand system has shown, when this technology possibly infringes on the privacy of consumers, companies could find themselves liable under a variety of different privacy theories.

In order to protect themselves, companies must first understand whether they would qualify as a state actor, private entity, or both. In the case of Walt Disney World, the theory of privacy law under which a potential plaintiff asserts their claim could be the deciding factor in the court's determination of liability. Under a state

---

[211] *See* Reidenberg, et. al., *supra* note 96, at 486 (establishing that the notice and choice framework is often the one that is promoted by both government and the White House as the best way to mitigate the risk of privacy violations).

[212] *See*, Reidenberg, et. al., *supra* note 96, at 486 (stating that the reason why these methods receive criticism is due to the fact that companies have a tendency to under or misinform consumers on what the technology is actually doing).

[213] *See GS1 guidelines, supra* note 14 (listing the standards proposed by GS1 to ensure proper and efficient use of RFID technology).

[214] *See* Reidenberg, et. al., *supra* note 96, at 491-96 (acknowledging the potential flaws in requiring notice and choice mechanisms as the only way to protect consumer privacy).

actor analysis the Walt Disney Company could be found liable for a violation of the Fourth Amendment if they are found to be a state actor and if the MagicBand system is found to violate consumers' reasonable expectation of privacy. Due to the complicated private and public nature of Walt Disney World, it is likely that they would be found to be a state actor, and would be held liable for a violation of the Fourth Amendment. Furthermore, in the event that Walt Disney World is found not to be a state actor, it is entirely possible that they could still be held responsible for a violation of individuals' privacy under a tort theory in an intrusion upon seclusion action.

Finally, although there have been attempts to create legislation to protect against the potential privacy implications of RFID and similar technology, the legislation that does exist is piecemeal and non-comprehensive. Companies are currently still encouraged to self-regulate to prevent the possibility of unwanted litigation. Ultimately the best thing that companies, such as the Walt Disney Company, wishing to implement new technology can do is to provide specific information to their customers and obtain their consent to collect their information. As technology continues to advance, we will face even more problems in terms of consumer privacy and companies' desire to use this new technology to their advantage. It is in everyone's best interest to study the current privacy laws and identify ways in which we can improve them to better protect individuals' privacy rights.