SPORTS & ENTERTAINMENT LAW JOURNAL
ARIZONA STATE UNIVERSITY
VOLUME 6 SPRING 2017 ISSUE 2

SMART STADIUMS: AN ILLUSTRATION OF HOW THE "INTERNET OF THINGS" IS REVOLUTIONIZING THE WORLD

Brendan Alan Melander*

"*To invent, you need a good imagination and a pile of junk.*"
Thomas Edison

"*There are no great limits to growth because there are no limits of human intelligence, imagination, and wonder.*"
Ronald Reagan

I. INTRODUCTION

Imagine walking into your favorite sports team's stadium. You have a sense of anticipation because you heard that the stadium has recently become "Smart" and you are not quite sure what to expect. As you near the gates, you attempt to pull your ticket from your pocket, but there's no need because a camera uses facial-recognition technology to spot you and opens the gate to allow entrance. As you walk in, a screen emerges from the wall to your right, greets you by your name, and shows you the shortest route to your seat. Your watch vibrates on your arm, and you notice that the stadium has offered you a discount for your favorite beverage, an ice-cold Coors Light. You click the purchase button and your watch navigates you to a concession line that is conveniently located near your seat. The wait for the beverage is non-existent because your watch alerted

* J.D. Candidate 2018, Sandra Day O'Connor College of Law, Arizona State University.

the stand to prepare your drink before you even arrived. With an excited grin, you grab your drink, which was automatically paid for by your electronic debit card, and head to your seat just in time for the coin toss.

Throughout the game you are invited by the announcer to use your phone to view live statistics, fun facts, compete in interactive games and polls against other fans in the stadium, and receive individualized coupons and promotions based on your past game consumptions. Don't worry about leaving your seat for a refill or a hotdog because you can click a button on your smartphone app and a vendor brings what you want directly to you. And when you have to go to the restroom after consuming your pick of beverages, an app on your phone alerts you to the closest restrooms, and the one with the shortest line. This scenario is just a prelude of the many amazing opportunities that the Internet of Things will bring to Smart Stadiums.

The "Internet of Things" ("IoT") is a concept that has fueled many modern innovations, and is set to drastically change the way the modern world operates.[1] But, what exactly is the "Internet of Things"?[2] IoT is a broad array of interconnected devices that use sensors to gather data, share that data between devices, and store or evaluate that data.[3] This machine-to-

---

[1] *See* Kim Walker, *The Legal Considerations of the Internet of Things*, COMPUTERWEEKLY.COM (July 2014), http://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things.

[2] *See, e.g.*, Kevin Maney, *Meet Kevin Ashton, Father of the Internet of Things*, NEWSWEEK (Feb. 23, 2015, 12:10 PM), http://www.newsweek.com/2015/03/06/meet-kevin-ashton-father-internet-things-308763.html. Kevin Ashton, a former brand manager for Proctor & Gamble and cofounder of MIT's Auto-ID Center, used the phrase "Internet of Things" as a title of a presentation in 1999 that described an innovative process used to track inventory of product in stores using electronic microchips. *See also* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986 (providing insight into the world of IoT and the future implications of the technology).

[3] Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/

machine (M2M) communication, in combination with the sensors, allows for devices that traditionally had no use for the Internet (e.g., such as coffee makers, alarm clocks, and refrigerators) to become "smart."[4] Moreover, "the real value that the Internet of Things creates is at the intersection of gathering data and leveraging it."[5] Cloud computing allows for these devices to analyze and transmit data between the devices to maximize convenience and efficiency in our everyday lives.[6] However, on a more troubling note, the IoT allows companies and governments to gather more information about people than ever before.[7]

As a direct result of the increasing accessibility of the Internet, decreased cost of manufacturing electronics, and smartphone ownership, the market for IoT is booming.[8] In a progressively fast-paced world, both the consumer and businesses are always searching for ways to save time and money.[9] "[The] reality is that the IoT allows for virtually endless opportunities and connections to take place, many of which we can't even think of or fully understand the impact of today."[10]

---

jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#314554c66828.

[4] *See* Daniel Burrus, *The Internet of Things is Far Bigger Than Anyone Realizes*, WIRED, https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/ (last visited Apr. 9, 2016).

[5] *Id.*

[6] *Id.*; *see also* Eric Griffith, *What is Cloud Computing?*, PCMAG.COM (May 3, 2016), http://www.pcmag.com/article2/0,2817,2372163,00.asp (noting that cloud computing allows for storage and access to data from any location with Internet connectivity).

[7] *See* Morgan, *supra* note 3.

[8] *See id.*; *see also* Jacob Poushter, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, PEW RES. CTR. (Feb. 22, 2016), http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/ (finding that 72% of adults in the United States own a smartphone and 89% of adults use the internet at least occasionally).

[9] *See* Morgan, *supra* note 3 (noting that the IoT allows a business or consumer to leverage the technology to make daily lives more efficient and convenient).

[10] *See id.*

Thus, many businesses have already taken steps to implement IoT into their technology, and it is likely many more will follow.[11] While there are legal problems with the implementation of any emerging technology, IoT's enormous impact upon society warrants special consideration into the pertinent legal and policy issues.[12]

This note will underline the application of IoT to sports stadiums, effectively creating "Smart Stadiums."[13] First, it will briefly discuss the vast benefits and effects of IoT from both the business and consumer perspective, with an emphasis on Smart Stadiums. Next, it will discuss the legal issues presented by the implementation of IoT, as an emerging technology, into society. Finally, it will apply these issues directly to Smart Stadiums, and recommend the stance the government should take to create an effective and thriving IoT infrastructure.

II. THE BENEFITS AND IMPLICATIONS OF IOT

The IoT is poised to be a major contributor in the global economy.[14] One study forecasts that there will be over twenty billion devices connected to the Internet by 2020.[15] Additionally, IoT is projected to contribute as much as $11.1 trillion per year

---

[11] *See* Dean Takahashi, *IBM to Pour $200 Million into Watson Internet of Things A.I. Business in Munich*, VENTURE BEAT (Oct. 3, 2016, 6:39 PM), *http://venturebeat.com/2016/10/03/ibm-to-pour-200-million-into-watson-internet-of-things-a-i-business-in-munich/* (stating that IBM, a global leader in technological advances, is set to invest $200 million into their IoT technology).

[12] *See infra* notes 15–19 and accompanying text.

[13] *See infra* note 30 and accompanying text.

[14] James Manyika et al., *The Internet of Things: Mapping the Value Beyond the Hype*, MCKINSEY GLOBAL INST. (June 2015), http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx.

[15] *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, up 30 Percent from 2015*, GARTNER (Nov. 10, 2015), http://www.gartner.com/newsroom/id/3165317.

to the global economy by 2025.[16] If these projections become reality, the IoT will impact almost eleven percent of the global GDP.[17] Of course, this is a highly speculative measurement and is dependent upon a large number of factors such as interoperability between devices and applications, privacy, technology prices, security, organization, and public policy, all of which will be discussed in this note.[18] The IoT has the potential to dramatically change lives, and the technology and its uses are only going to continue to grow.[19] Thus, a brief look at the business outlook and consumer benefit outlines the impact that the IoT will have on society.

A. BUSINESS OUTLOOK

IoT offers a unique method for businesses to maximize profit margins both internally through their operations and externally by enhancing customer experience with their products and services.[20] Although most publications and conversations point to the obvious consumer advantage, business-to-business ("B2B") applications will account for nearly seventy percent of the estimated value that IoT will contribute to the global economy.[21] Implementing IoT into B2B allows for increased

---

[16] Manyika et al., *supra* note 14, at 4. A study by the McKinsey Global Institute analyzed over 150 IoT cases throughout the world and concluded that, including the total value captured throughout the entire chain of business, the total economic impact could range between $3.9 trillion to $11.1 trillion per year by 2025. The study identified nine settings where IoT could make the largest impact: human, home, retail environments, offices, factories, worksites, vehicles, cities, and outside.

[17] Manyika et al., *supra* note 14, at 2 (contribution based on World Bank projection of $99.5 trillion per year in global GDP in 2025).

[18] Manyika et al., *supra* note 14, at 2.

[19] *See* Manyika et al., *supra* note 14, at 2.

[20] *See* Jacques Bughin et al., *An Executive's Guide to the Internet of Things*, MCKINSEY QUARTERLY (Aug. 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/an-executives-guide-to-the-internet-of-things.

[21] *Id.*; *see also* Katherine Arline, *What is B2B?*, BUS. NEWS DAILY (Jan. 2, 2015, 10:09 AM), http://www.businessnewsdaily.com/5000-what-is-

productivity in supply chain and manufacturing processes.[22] Additionally, IoT allows for businesses to optimize their operations by using the data gathered by the sensors to make informed and data-driven strategic decisions.[23] IoT technology enables businesses to expand to new markets and to offer new products to the consumer.[24] It will give businesses an effective tool to decrease operating costs, increase productivity, and allow new business opportunities; all of which increases profit margins and permit the business to sell products and services to the consumer at a lower price.[25]

B. CONSUMER BENEFIT

While businesses stand to benefit greatly from the economic impact of IoT, consumers are also poised to benefit in numerous ways.[26] As IoT allows businesses to become more efficient and produce products at a lower price, the consumer will purchase more "smart" products to use with the IoT.[27] These devices, in their abundance, will make the average consumer's life more convenient by allowing them to use the data gathered by their connected devices to maximize their efficiency and time.[28] IoT's data analysis will lead to reduced expenses, improved health, and optimal living conditions.[29] For example, the IoT can help calculate the most efficient route during a commute, customize and tailor advertisements to your personal interests, and adjust your home settings to maximize your comfort and minimize costs.

---

b2b.html (stating that B2B focuses on marketing and selling products between other companies, as opposed to the consumer).

[22] Bughin et al., *supra* note 20.

[23] *Id.*

[24] John Greenough, *How the 'Internet of Things' Will Impact Consumers, Businesses, and Governments in 2016 and Beyond*, BUS. INSIDER (July 18, 2016, 10:24 AM), http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10.

[25] *Id.*; *see also* Bughin et al., *supra* note 20.

[26] Manyika et al., *supra* note 14, at 4–6.

[27] *See id.*

[28] *Id.*

[29] *Id.*

C. SMART STADIUMS—WHAT ARE THEY, AND WHY DO WE CARE?

Smart Stadiums will take the IoT business model to the next level by utilizing sensors, WiFi capabilities, cameras, and other internet-connected devices to improve the fan experience at the game and further improve profits for sports franchises.[30] Thus, Smart Stadiums appear to be the perfect testing ground for massive-scale IoT technologies, such as "Smart Cities."[31]

Due to the prominence of the "At-Home Experience," which has resulted from the availability of instant streaming services, high-definition video and audio, increased WiFi speeds, and other technological improvements, stadium owners are left with an alarming issue—how do we get fans off of the couch and into the stands?[32] Just as sports franchises have a right to be concerned with this phenomenon, the issue is also concerning to the cities in which the stadium is located.[33] Stadiums have an enormous economic impact on their surrounding communities, which have an interest in economic sustainability and growth.[34] For many franchises and cities, perhaps Smart Stadiums can be the answer.

Smart Stadiums will increase the value of attending a sporting event by creating an enhanced fan experience.[35] To make it worthwhile for the consumer to spend the money on tickets, merchandise, and other expenses involved in attending a

---

[30] *See Smart Stadiums Take the Lead in Profitability, Fan Experience, and Security*, INTEL 1, http://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/iot-smart-stadiums-brief.pdf (last visited Apr. 4, 2017) [hereinafter INTEL].

[31] *See* O'BROLCHAIN & GORDIJN, THE ETHICS OF SMART STADIA – A WHITE PAPER 1 (2015). Smart Stadiums, while an exciting opportunity for sports franchises, opens an even greater opportunity of "Smart Cities." It is impossible to fathom the benefits and possibilities that the IoT concept will bring to an increasingly technological, urban society.

[32] INTEL, *supra* note 30, at 1.

[33] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 5.

[34] *See id.* For example, Arizona State University's stadium hosts over 180 events each year for an annual economic impact of $209.4 million.

[35] *See* INTEL, *supra* note 30, at 1.

sporting event, the fan must have fun. Smart stadiums will revolutionize the fan experience with convenience, targeted messages, and access to the Internet.[36] Through the use of smartphones, fans will be able to order merchandise and refreshments with the touch of a button, obtain access to deals, and connect to WiFi to view live statistics and interact with other fans.[37] Like other IoT applications, a Smart Stadium will maximize convenience and reduce expenses for the consumer.[38]

Sports Stadiums will lead to further profits for sports-affiliated businesses. Because the fan experience will be taken to a new level, more people will attend sporting events.[39] More merchandise will be sold in the stadium with the use of personalized marketing and convenient applications, which encourage the fan to consume at a greater rate.[40] Not only will profits from consumers increase, but also the efficiency within the infrastructure will reduce operating costs.[41] Precise data will allow for supply chain efficiency. Automated systems will shrink energy costs.[42] Maintenance costs will decline as staff is automatically alerted to address issues before they occur, and if an issue does arise, it will be resolved quickly.[43]

An additional benefit of IoT application into Smart Stadiums, which is important to both the consumer and the stadium operators, is security and safety of the guests. With tens of thousands of adrenaline-filled fans in a tightly enclosed space, security can become a real issue. Because the IoT utilizes an extensive system of cameras, they can be used to monitor large crowds or other security threats.[44] Sensors can be utilized to detect any unusual activity in the stadium.[45] Both the sensors and

---

[36] *Id.*
[37] *Id.* at 2–3.
[38] Manyika et al., *supra* note 14, at 4–6.
[39] *See* INTEL, *supra* note 30, at 2–4.
[40] *See id.*
[41] *Id.* at 2.
[42] *Id.* at 2–4.
[43] *Id.*
[44] O'BROLCHAIN & GORDIJN, *supra* note 31, at 6–7.
[45] *Id.* at 7.

cameras can facilitate anti-terrorist efforts, quickly break-up fights in the crowd, and prevent other criminal activity.[46] Face-capturing technology can limit access to restricted areas.[47] If an issue arises, law enforcement, security or medical personnel can rapidly respond to the precise location of the incident.[48] These examples, among others, demonstrate how IoT enhances stadium security.

Smart Stadiums are becoming a reality. To stay competitive, fun, and safe in the modern technological era, all stadiums should embrace the IoT model.[49]

III. INTEGRATING IOT INTO SPORTS STADIUMS — THE LEGAL CONSIDERATIONS

While Smart Stadiums have the ability to create numerous benefits to consumers and businesses, there are multiple issues of law that should be considered. The chief issues include: security, privacy, data management, and the need for standards and protocols.

A. SECURITY

The widespread use of IoT technology and massive data collection by the affiliated devices requires an acute emphasis on security.[50] In 2013, the Federal Trade Commission ("FTC") first recognized the need for companies to secure their IoT devices.[51] However, because there were not any standards specifically regulating the use of IoT technologies, the FTC settled the

---

[46] *Id.*

[47] INTEL, *supra* note 30, at 3.

[48] O'BROLCHAIN & GORDIJN, *supra* note 31, at 7.

[49] *See id.* at 1. An increase in competition will likely drive new innovations and applications of IoT to the arenas, and would further benefit society.

[50] *See supra* notes 14–16; *see also supra* text accompanying note 16.

[51] *See* Julie Brill, Fed. Trade Comm'r, Fed. Trade Comm., Keynote Address Before the Center for Strategic and International Studies, "Stepping into the Fray: The Role of Independent Agencies in Cybersecurity" (Sep. 17, 2014). TRENDnet, Inc., a company that sells baby monitors, failed to provide secure software to protect the baby monitor's live feed from being accessed from outside sources.

claims against TRENDnet under Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[52] After settling the charges against TRENDnet, the FTC declared that a need to "establish a comprehensive information security program designed to address security risks that could result in unauthorized access to or use of the company's devices, and to protect the security, confidentiality, and integrity of information that is stored, captured, accessed, or transmitted by its devices."[53]

In a 2015 staff report, the FTC echoed its comments made against TRENDnet by repeatedly stressing the growing importance of securing IoT technologies, but it declined to recommend to Congress to enact IoT-specific legislation.[54] In that same report, the FTC declared that although the privacy and security risks are real, IoT-specific legislation would be "premature" because IoT is an emerging technology in which all of the potential uses are currently unknown.[55] Instead, the FTC recommended to Congress that they should enact "general data security legislation" which would apply to the application of IoT technologies.[56] Additionally, the FTC concluded that they would encourage self-regulation, educate businesses and consumers, and enforce through their existing powers.[57]

In 2016, the FTC used their existing powers to sanction ASUSTeK for failing to secure a router, which is a very common

---

[52] 15 U.S.C. § 45 (2012). Section 5 was enacted in 1914 to give the FCC the power to regulate and secure data in the business context.

[53] *FTC Approves Final Order Settling Charges Against TRENDnet, Inc.*, FED. TRADE COMMISSION (Feb. 7, 2014), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

[54] *Internet of Things: Privacy & Security in a Connected World*, FTC STAFF REP. 48–49 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[55] *Id.* at 49.

[56] *Id.* at 49–50.

[57] *Id.* at 53 (using the FTC Act, among others, the FTC encourages businesses to implement appropriate security measures into their devices and software).

IoT device, and for failing to inform consumers of the security flaws inherent in the routers.[58] Hackers were able to access over 12,900 consumers' routers remotely and gain access to all of the data on the network.[59] While TRENDnet and ASUSTeK involve relatively small breaches of security, they portray the very real risk of massive security breaches within IoT systems if appropriate security measures are not taken.

In October 2016 hackers were able to exploit numerous unsecure IoT devices to facilitate a massive distributed denial of service ("DDoS")[60] attack on popular Internet sites, such as Twitter, Netflix, and Spotify.[61] This DDoS attack was coordinated by what is called a "Mirai botnet" which uses IoT devices to flood a server, and because the IoT connects traditionally unrelated devices together, the DDoS attack was able to reach strengths never achieved before.[62] In November 2016 the same Mirai botnet was used to take down the internet infrastructure of the entire country of Liberia, a population of around 4.5 million people.[63] While anonymous hackers launched these attacks, "[i]magine what a well-resourced state actor could

---

[58] ASUSTeK Computer, Inc., No. C-4587, 2016 WL 4128217, at *1–5 (F.T.C. July, 2016).

[59] *Id.* at *7–8.

[60] Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of Kind in History, Experts Say*, THE GUARDIAN (Oct. 26, 2016 4:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet (stating a DDoS attack occurs when a "network of computers infected with special malware, known as a 'botnet', are coordinated into bombarding a server with traffic until it collapses under the strain").

[61] Sam Thielman & Chris Johnston, *Major Cyber Attack Disrupts Internet Service Across Europe and US*, THE GUARDIAN (Oct. 21, 2016, 12:06 PM), https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service.

[62] Woolf, *supra* note 60.

[63] Lee Matthews, *Someone Just Used the Mirai Botnet to Knock an Entire Country Offline*, FORBES (Nov. 3, 2016, 4:00 PM), http://www.forbes.com/sites/leemathews/2016/11/03/someone-just-used-the-mirai-botnet-to-knock-an-entire-country-offline/#3233144d51f0.

do with insecure [IoT] devices."[64] The potential for this Mirai botnet to be used as a weapon should alert lawmakers of the security implications associated with IoT technology and speed up Legislative action.

1. Physical Security Within Stadiums

Smart Stadiums must protect the physical safety of the guests entering the stadium. In light of the recent security breaches that were facilitated by IoT technology, it's not difficult to imagine the various scenarios that could emerge.[65] If even one device connected to the IoT is susceptible to a breach, the entire system could be vulnerable to hackers.[66] Additionally, there is a possibility that terrorists could use IoT to plan, survey, and carry out an attack upon a venue filled with thousands of people.[67] Cameras could be hacked to give terrorists access to real-time video feed of the stadium, exits could be locked remotely leaving guests trapped inside, and the stadium's own security systems could be used against it.[68] While a deliberate attack may sound like fiction, one can imagine the situations that could arise if adequate security measures are not implemented.

On the other side of the spectrum, there is always the risk of an accident. While the IoT is intended to prevent and alleviate loss in an accident,[69] there is always the risk the technology could malfunction and cause greater devastation.[70] If security and medical personnel become reliant upon these systems that are designed to prevent and reduce human harm in the event of an accident, and they fail, a catastrophic event could

---

[64] Woolf, *supra* note 60.
[65] *See id.*
[66] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 14; Bernard Marr, *5 Simple Steps to Protect Yourself from IoT Security Threats*, FORBES (May 3, 2016, 3:19 AM), https://www.forbes.com/sites/bernardmarr/2016/05/03/5-simple-steps-to-protect-yourself-from-iot-security-threats/#2ec241532b22.
[67] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 14.
[68] *See id.* at 14.
[69] *See id.* at 7, 14 ("Sensors will also be able to detect structural problems in the stadium before any damage can be done.").
[70] *Id.* at 14.

occur.[71] For example, if a sensor fails to notify the IoT there is a fire and no backup security measures are in place, it could engulf an entire area in flames before first responders are able to detect and then extinguish it. Smart Stadium owners and the cities in which they are located have a significant interest in preventing the loss of life, harm to its' guests, and property damage. Consequently, a Smart Stadium owner should be concerned with creating best practices and internal policies to address the issue of physical security within the stadium.

2. Security and Protection of Data

Smart Stadiums have a significant interest in the security and protection of the private data of their guests and businesses operating within the location. While this may not be as important as the physical safety within the stadium, it is certainly a more pertinent and realistic concern to protect against. If fans embrace the Smart Stadium model, and given that occupant capacities in the largest stadiums can reach an excess of seventy thousand people with millions of annual visitors, the data from vast amounts of people will be exposed to the stadium's network.[72]

Many of the functionalities of the Smart Stadium require a guest to connect their smartphone to the IoT network.[73] When a fan connects their device to an unsecure network an extraordinary amount of their personal data is at risk.[74] An average smart phone contains a wide variety of sensitive information, including bank accounts, emails, social media

---

[71] *See id.*

[72] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 2; *see also Sustainable Stadiums & Arenas*, WASTE MGMT. 1, https://www.wm.com/sustainability-services/documents/insights/Stadiums%20and%20Arenas%20Insight.pdf (last visited Apr. 6, 2017) ("Each year the top 200 stadiums in the U.S. draw nearly 181 million visitors, placing the industry in a unique position to integrate sustainability into U.S. culture.").

[73] *Supra* note 30 and accompanying text.

[74] *See* Donna Tapellini, *Smart Phone Theft Rose to 3.1 Million in 2013*, CONSUMER REPORTS (May 28, 2014, 4:00 PM), http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

accounts, photos, contacts, and other private information.[75] If a hacker infiltrated the Smart Stadium network all of this data would be susceptible to a breach. When one's phone holds the key to the intricacies of their life, including financial and other private information, a security breach could lead to frightening effects. If the guests do not feel that a Smart Stadium IoT network is secure, they would likely refrain from connecting and utilizing the benefits that a Smart Stadium has to offer, which would undermine the core purpose of creating a Smart Stadium in the first place.[76]

Overall, the guests, stadium businesses, and municipalities stand to benefit from the security benefits of IoT technology in Smart Stadiums.[77] There have always been inherent risks of security in stadiums that IoT is poised to help combat; however, there are new issues, as discussed above, created by IoT.[78] Additionally, with new security technology and surveillance methods, other rights and benefits we value as a society could be infringed upon.[79]

B. PRIVACY

With the sheer amounts of data collected by IoT and shared through the network, there are serious privacy concerns. Privacy is a fundamental right held by an individual, and is the chief legal implication of the IoT.[80] While security has other purposes, the measures taken, as discussed above, also protect privacy rights. Thus, the two considerations are closely related and an understanding of security is insightful when discussing privacy. The first and most obvious privacy concern, which is addressed in the Security section, is that the consumers' private

---

[75] *Id.*
[76] *See* INTEL, *supra* note 30, at 1, 4.
[77] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 6–7.
[78] *See supra* notes 65–71 and accompanying text.
[79] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 9–18 (explaining users of IoT are likely to notice a loss of privacy, infringement of autonomy, and increased surveillance activities).
[80] *See* Washington v. Glucksberg, 521 U.S. 702, 770–71 (1997).

information can be hacked by an outside party.[81] Second is the threat that a business would collect data and use it for unauthorized purposes such as selling it or using it beyond the scope of the consumer's expectation.[82] Finally, there is a threat that, because of the vast multitude of cameras and sensors, one's personal data, pictures, or other information will be readily available or accidentally disclosed to the public just by way of being present in the stadium.[83]

1. Privacy Principles: The Foundation

Because IoT is such a disruptive and innovative technology, and society continues to see rapid advancement in the computing space, United States law will likely resort to fundamental privacy principles that have been developed over time.[84] These "Fair Information Practice Principles" originated in the 1970s, but since have been adopted by the FTC.[85] The Fair Information Practice Principles originally focused on five core needs: notice, consent, access, security, and enforcement.[86] Subsequently, in 2012, the FTC consolidated and incorporated

---

[81] GARY MARCHANT, SMART STADIUMS AND PRIVACY 2 (2015) (on file with author).
[82] *Id.*
[83] *See id.* at 3.
[84] *See id.* at 7; *see also After Moore's Law*, THE ECONOMIST: TECHNOLOGY QUARTERLY, http://www.economist.com/technology-quarterly/2016-03-12/after-moores-law (last visited Apr. 1, 2017) (computing power has roughly doubled every two years since Gordon Moore's famous 1965 paper). While there are generally no privacy laws that apply, there may be an exception in the case of a government-operated stadium, such as a public university. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 333–337 (1985). In the case of public institution, Fourth Amendment issues may be triggered. *Id.*
[85] ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2.17 ed. 2016), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.
[86] *Id.* There are an additional two principles, data minimization and accuracy, which may not apply to the IoT setting.

the original five into three modern principles: "Privacy by Design," "Simplified Consumer Choice," and "Transparency."[87]

Privacy by Design comprises data security, reasonable collection limits, sound retention practices, and data accuracy.[88] Accordingly, Privacy by Design incorporates the original security and access principles into its formula. Furthermore, the FTC recommends that businesses should create their own internal standards and protocols.[89]

Simplified Consumer Choice requires that businesses, at the time of data collection, provide the consumer with the opportunity to make an educated decision of whether or not they want their data to be collected.[90] However, if the data is collected and used in the context of their continuing relationship, a commonly accepted process, and in the manner in which the consumer would expect it to, the business does not need to provide choice in the form of notice and consent.[91]

Transparency requires that clear, concise, and comprehendible privacy notices be given to the consumer.[92] Additionally, consumers should be given reasonable access to the data that the business has collected, and at a minimum these businesses should offer consumer access to "the types of information the companies maintain about them" and "the sources of such information."[93]

These three privacy principles offer a consolidated approach to the original five. Privacy by Design incorporates security and access into its formula, while Simplified Consumer Choice contains notice and consent. Transparency uses access, notice, and consent. When enforcing IoT under Section 5, the FTC will likely take these principles into account.[94] Moreover,

---

[87] FEDERAL TRADE COMMISSION, FTC REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012).
[88] *Id.* at 23–30.
[89] *Id.* at 30–32.
[90] *Id.* at 48.
[91] *Id.* at 36–48.
[92] *Id.* at 61–4.
[93] *Id.* at 67.
[94] *See* 15 U.S.C.A. § 45 (2012).

with these privacy principles in mind, privacy issues in Smart Stadiums should be addressed by the topics of informed consent, surveillance, autonomy, and data ownership.[95]

2. Informed Consent

Informed consent is a legal concept that comes into play at the onset of data collection.[96] Traditionally, if a business gains informed consent to collect one's personal data, the business is free to do so as long as it is reasonable in light of that consent.[97] Accordingly, informed consent embodies the principles of notice, consent, and Simplified Consumer Choice.[98] However, in the context of IoT and Smart Stadiums, informed consent becomes attenuated.[99] A Smart Stadium, which has thousands of sensors and cameras utilizing IoT technology, creates problems of obtaining informed consent.[100] For example, "many people attending will be unaware that they are producing data—that they themselves are data nodes."[101]

Framed narrowly, the issue is how a fan can give informed consent to all the different data they ceaselessly transmit through the vast multitude of sensors and cameras. One answer is that informed consent, along with the privacy principles that embody it, is simply not applicable in the Smart Stadium setting. However, this note advocates that there is an effective way to apply the FTC privacy principles. A Smart

---

[95] *But see* FEDERAL TRADE COMMISSION, *supra* note 54, at 19 ("While some participants continued to support the application of all of the [Fair Information Practice Principles], others argued that data minimization, notice, and choice are less suitable for protecting consumer privacy in the IoT.").

[96] O'BROLCHAIN & GORDIJN, *supra* note 31, at 13 ("Consent is considered fully informed when a competent person, who fully understands the nature of the data being gathered about and fully understands what they are disclosing voluntarily consents to treatment or participation on this basis.").

[97] O'BROLCHAIN & GORDIJN, *supra* note 31, at 13.

[98] *See* GELLMAN, *supra* note 85, at 14.

[99] *Id.* at 13–14.

[100] *Id.*

[101] *Id.* at 13.

Stadium should strive to provide notice that is transparent, clear, and concise so that a reasonable person will understand what information will be collected and how it will be used.[102] This notice can come in many forms: a waiver on the ticket, push notifications to a guest's phone throughout the event, terms and conditions before connecting to WiFi, or signs physically posted at the stadium.[103] Whatever the method that is used to gain informed consent, it must articulate to an ordinary person the extent that their real-time data will be collected, their consumption habits analyzed, and used by the Smart Stadium to further their business objectives.

3. Surveillance

With additional safeguards, security measures, and technological advances comes the potential for the infringement of privacy.[104] Improved surveillance methods, with the IoT, can result in a loss of privacy.[105] All of the devices, sensors, and cameras could be used to accumulate massive amounts of data about an individual without the use of traditional surveillance methods.[106] In the context of Smart Stadiums, where thousands of IoT devices are available to collect data on thousands of individuals throughout the stadium, the infringement of autonomy and privacy becomes a concern. There are two main surveillance concerns in a Smart Stadium: 1) the government will acquire and routinely use IoT data in mass surveillance programs; and 2) data will be unknowingly collected or used for

---

[102] MARCHANT, *supra* note 81. For example, if the data will be sold or given to a third party, this information should be highlighted or there should be additional safeguards to prevent unauthorized use of personal information.

[103] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 13.

[104] *See supra* notes 80–83 and accompanying text.

[105] *See* Spencer Ackerman & Sam Thielman, *US Intelligence Chief: We Might Use the Internet of Things to Spy on You*, THEGUARDIAN (Feb. 9, 2016, 4:51 PM), *https*://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

[106] *Id.*

unauthorized purposes by the business. Thus, sound policy must be created to address these concerns.

Surveillance is broadly defined as the "[o]bservation and collection of data to provide evidence for a purpose."[107] However, modern surveillance techniques have made it increasingly easy to collect massive amounts of data, and with powerful tools, comes the high potential for abuse.[108] For example, surveillance was brought to the national spotlight in June 2013 when Edward Snowden, a Central Intelligence Agency (CIA) contractor, leaked details of the National Security Agency's (NSA) information gathering techniques.[109] If left unchecked the government could utilize the IoT, along with its current surveillance methods, to collect unprecedented amounts of data on the public.[110]

IoT surveillance allows a business access to significantly more information than traditional data-collection methods. This access to information could be used detrimentally against an individual's privacy rights.[111] For example, Samsung is already using its "SmartTVs" voice recognition function to capture private conversations in your home.[112] The data is then

---

[107]Surveillance, THE LAW DICTIONARY, http://thelawdictionary.org/surveillance/ (last visited Apr. 9, 2017).

[108] *NSA Surveillance*, AM. C.L.UNION (last visited Apr. 9, 2017), https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance.

[109] *Edward Snowden: Leaks That Exposed US Spy Programme*, BBC NEWS (Jan.17, 2014), http://www.bbc.com/news/world-us-canada-23123964 (stating that the NSA, with a secret court order, was accessing and collecting millions of American's phone records)..

[110] Ackerman & Thielman, *supra* note 105 (stating that according to James Clapper, the United States Intelligence Chief, that the government plans to use IoT devices as part of their surveillance techniques).

[111] *See* MARCHANT, *supra* note 81, at 14–15.

[112] David Goldman, *Your Samsung TV is Eavesdropping on Your Private Conversations*, CNN (Feb. 10, 2015, 6:38 AM), http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy.

transmitted to third parties with the IoT.[113] Although Samsung has a disclaimer in their privacy policy, this is clearly concerning.[114]

A Smart Stadium creates a haven for mass surveillance methods. With a camera seemingly pointed in every nook and cranny of the stadium and sensors recording your every step, there is no escaping the reach of the IoT. Of course, the legitimate need of security of the guest is furthered by surveillance, but the privacy interest will need to be weighed against that need.[115] Thus, the issue is not how to limit the *collection* of data, which is seemingly impossible due to the nature of the IoT. Instead, the solution is to limit the *use* of the data collected. If the government is able to use IoT in their surveillance methods there is an important need for transparency of what data will be collected, how it will be used, and the extent that the government can compel a private entity to hand over the data.[116] Additionally, the Smart Stadium will need to inform the guest that the IoT will be used to collect data, clearly state what the guest's data will be used for, and create an understanding of the implications of the technology.[117] The survival of informed consent in a world filled with IoT technology is dependent upon proper regulation and notice given to the consumer.

4. Autonomy

Autonomy is a value that the Founders of our Constitution treasured, and one that citizens of our free nation

---

[113] *Id.*
[114] *Id.*
[115] *Compare* O'BROLCHAIN & GORDIJN, *supra* at 7 *with* O'BROLCHAIN & GORDIJN, *supra* at 14, in footnotes 69–70.
[116] *See Super Bowl Snooping*, N.Y. TIMES (Feb. 4, 2001), http://www.nytimes.com/2001/02/04/opinion/super-bowl-snooping.html. Indeed, surveillance methods such as these have already occurred without the help of the IoT. *Id.* In 2002, Tampa Bay police used facial recognition technology to scan all guests attending Super Bowl XXXV. *Id.* These facial scans were then compared with images of criminals and potential suspects to help ensure the safety of those attending the event. *Id.*
[117] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 13.

still cherish today.[118] Autonomy is an individual's ability to make their own decisions and to pursue the life they want.[119] Personal autonomy is at risk when a person is controlled by an outside source.[120] Thus, the IoT may infringe on autonomy because a business could use the data collected, in combination with targeted advertising and nudging, to influence and potentially control the consumer.[121] The IoT enables advertisers to use the massive amounts of data collected to use marketing methods that are extremely targeted and sophisticated, which may not allow a person to make their own decisions.[122]

There is a relatively low risk of these advertising strategies having a detrimental effect upon autonomy when a fan attends a game in a Smart Stadium because the fan is only in the stadium for a short period of time.[123] However, the long-term effects are more concerning, as the data could be used to influence the guests once they leave the stadium.[124] For example, if personal data is sold or given to a third party, and that third party uses that information in combination with other data collected, it could lead to pervasive nudging and an overall negative effect upon autonomy.[125] While a relatively small concern when compared to the other issues discussed above, Smart Stadiums and the legislature should take autonomy into account as each attempts to regulate the IoT.

---

[118] *See generally* U.S. CONST. amend. I, IV, XIV (illustrating through specific and targeted provisions, the Constitution does not explicitly state the term autonomy but it is implicit in many areas such as the First, Fourth, and Fourteenth Amendments).
[119] O'BROLCHAIN & GORDIJN, *supra* note 31, at 16.
[120] *Id.*
[121] *Id.* at 17. Nudging is a subtle advertising technique that is "pervasive, invisible, and constant" which may encourage or influence people to act in a certain way. *Id.*
[122] *Id.* at 18.
[123] *Id.*
[124] *Id.*
[125] MARCHANT, *supra* note 81, at 2.

5. Data Ownership

The theme of this note is clear—the IoT will permit businesses to accumulate massive amounts of data that can be utilized for many different purposes. But, who owns the data is another issue. Data ownership can establish different rights, such as the right to access, use, transfer, and control.[126] Likewise, defining data ownership and the affiliated rights may help resolve some of the other privacy issues, such as surveillance and informed consent.[127]

For the IoT to be effective, the data collected must be analyzed and leveraged effectively.[128] Many businesses often rely on third party services to store, analyze, and maintain this data.[129] In addition to the consumer or guest from which the data is collected, the "data has value, not only to the company generating it, but to the technology companies that provide data-crunching services."[130] An issue arises when a third party uses the data for purposes outside the initial reason it was collected.[131] Therefore, it is important to determine who owns the data and what rights are attached to that ownership.

Data ownership collected from the guests in a Smart Stadium can become particularly tricky. The guest plays an integral part in producing the data, yet they do not own the data obtained from the different sensors and cameras.[132] However, the guest may still expect a certain level of privacy. Once the data is analyzed it could reveal highly personalized and accurate information ranging from consumption habits to economic

---

[126] *See* O'BROLCHAIN & GORDIJN, *supra* note 31, at 12.
[127] *Id.* For example, if an individual does not own any data recorded by sensors in a Smart Stadium, then there is no reason to obtain consent. *Id.*
[128] Burrus, *supra* note 4.
[129] Barb Darrow, *The Question of Who Owns the Data is About to Get a Lot Trickier*, FORTUNE (Apr. 6, 2016, 10:00 PM), http://fortune.com/2016/04/06/who-owns-the-data/.
[130] *Id.*
[131] O'BROLCHAIN & GORDIJN, *supra* note 31, at 12.
[132] *Id.*

status.[133] If a third-party data management company is able to transfer or sell the personalized information to an advertising company, a guest may feel their privacy has been infringed upon.[134]

Applying the principles of privacy and informed consent could help mitigate the data ownership dilemma. If a Smart Stadium incorporates Privacy by Design, Simplified Consumer Choice, and Transparency into their data collection policies, it could help reduce a guest's private information from being used in undesirable ways. [135] A guest would be safeguarded with reasonable collection limits, a knowledge of how their information is to be used, and have reasonable access to the information that has been collected.[136]

Further measures could be taken to ensure data ownership stays in the hands of Smart Stadiums. The Smart Stadium could use licensing agreements or other contracts that explicitly retain ownership of the data, and prohibit the use of data by the third party for any other purposes. Data could be collected anonymously, which would not allow third parties to have knowledge about an individual.[137] Lastly, legislation could be put into place controlling how businesses use the IoT data they collect and transfer to third parties.

C. DATA MANAGEMENT

Once consumer data is lawfully collected, businesses are faced with the challenge of data storage and management. The IoT collects unprecedented amounts of data. At this point, data management directly intersects with both the security and privacy considerations. Data management must be efficient, cost effective, secure, and maintain the integrity of private information.

---

[133] *Id.*
[134] MARCHANT, *supra* note 81, at 2.
[135] FEDERAL TRADE COMMISSION, *supra* note 87.
[136] *Id.*
[137] O'BROLCHAIN & GORDIJN, *supra* note 31, at 12.

Today, cloud computing has taken the lead in data management.[138] Cloud computing offers many competitive advantages.[139] The cloud permits a business to access data over the Internet from any location, does not require the purchase and maintenance of physical hardware, and is remarkably efficient.[140]Most pertinent to the IoT, the cloud enables the data collected by individual devices to be synced and analyzed with other independent devices.[141] Additionally, cloud computing is highly cost effective.[142]

While it is clear that the IoT could not survive without cloud computing, there are two drawbacks. First, most of a businesses' data is in the hands of a third party company.[143] The business collecting data and utilizing a third party to manage that data must ensure that it is not used for any unauthorized purposes and appropriate security measures are taken to prevent unauthorized access.[144] The business collecting the data must retain a cloud computing service provider that is "capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so."[145] Luckily, it is relatively easy to find a reliable cloud computing service due to the competition in the market.[146]

Second, because IoT data accumulates exponentially over time, it could eventually become burdensome to manage the data. However, this concern is marginalized by the decreasing

---

[138] Griffith, *supra* note 6. The cloud computing industry is estimated to be valued at over $500 billion by 2020. *Id.*
[139] *Id.*
[140] *Id.*
[141] *See id.*
[142] Julie Bort, *Something Called 'The Race to Zero' Is Scaring A Lot Of Tech Companies*, BUS. INSIDER (Nov. 9, 2014, 9:03 AM), http://www.businessinsider.com/cloud-storage-race-to-zero-2014-11. In what's being called "the race to zero", competition in the market for cloud computing has dropped prices incredibly low while increasing storage limits.
[143] Darrow, *supra* note 129.
[144] *Supra* notes 80–83 and accompanying text.
[145] FEDERAL TRADE COMMISSION, *supra* note 54, at 30.
[146] Bort, *supra* note 142.

costs and availability of cloud computing services.[147] Additionally, a business may choose to set limits or delete certain types of data after a specified period of time.

A Smart Stadium presents unique challenges for data management. With thousands of people attending events and flooding the IoT with information, it will be important to have a reliable data management system that can handle the incoming traffic demands. Moreover, the internal procedures of collecting the data must have adequate safeguards to prevent unauthorized access to the network. Once the data is collected, it must be transmitted to a reliable cloud computing service that is used solely for storage and analytics. While it is fairly simple to create an effective data management system, internal business procedures and official legislation would help ensure the privacy of the fan's information, while helping create a best practice in the IoT industry.

D. THE NEED FOR STANDARDS AND PROTOCOLS

After the discussion of the legal considerations involving security, privacy, and data management, it is clear that there is a need for uniform standards and protocols for IoT. The legislature, administrative agencies, and the IoT industry have all recognized the need, and are taking steps to address the considerations.[148] Thus, the challenge is balancing innovation with regulation, while allowing those innovations to flourish.

1. A Step in the Right Direction—The Developing Innovation and Growing the Internet of Things Act

Despite the FTC's hands-off approach, use of alternative methods to regulate IoT, and recommendations that Congress enact "general security legislation," the Senate passed a Resolution in March 2015 expressing the need for a "national

---

[147] *Id.*

[148] *See generally, supra* notes 51–59 and accompanying text; *infra* notes 149–155 and accompanying text; *infra* notes 171–184 and accompanying text.

strategy" on the development of the IoT.[149] Acting quickly, in April 2016, the Senate's Commerce, Science, and Transportation Committee pushed a bill.[150] The Developing Innovation and Growing the Internet of Things (DIGIT) Act, if passed by Congress, requires a working group led by the Commerce Department to study IoT and make recommendations to "appropriately plan for and encourage the proliferation of the Internet of Things in the United States."[151] The crux of the DIGIT Act requires:

> The working group must: (1) identify federal laws and regulations, grant practices, budgetary or jurisdictional challenges, and other sector-specific policies that inhibit IoT development; (2) consider policies or programs that encourage and improve coordination among federal agencies with IoT jurisdiction; (3) implement recommendations from the steering committee; (4) examine how federal agencies can benefit from, use, and prepare for the IoT; and (5) consult with nongovernmental stakeholders.[152]

The DIGIT Act would require the working group to report these findings and recommendations to the appropriate federal agencies within eighteen months "to implement recommendations."[153] Additionally, the act requires the FTC to seek public comment on "IoT's spectrum needs, regulatory

---

[149] *Senate Passes "The Internet of Things" Resolution*, DEB FISCHER, U.S. SENATOR FOR NEB. (Mar. 24, 2015), http://www.fischer.senate.gov/public/index.cfm/2015/3/senate-passes-the-internet-of-things-resolution; FEDERAL TRADE COMMISSION, *supra* note 54.

[150] Paul Merrion, *Senate Bill Lays Groundwork for Federal Oversight of Internet of Things*, CQ ROLL CALL (Apr. 28, 2016), 2016 WL 1694637. This bill is sponsored by Senator Deb Fisher, and has bipartisan support. *Id.*

[151] *Id.*

[152] DIGIT Act, S. 2607, 114th Cong. (2016) (as amended by S. Comm. on Commerce, Science, and Transportation Sep. 27, 2016).

[153] *Id.*

barriers, and growth" and submit these comments to Congress.[154] However, the FTC has already undertaken the task of researching and reporting on IoT to the Legislature.[155] Furthermore, because the 114th Congress did not ultimately adopt the DIGIT Act, it will have to be introduced at the next session. While admittedly a step in the right direction of regulating IoT, the DIGIT Act appears to be burdened by the snail-like speed of the bureaucratic process.

2. Administrative Agencies and Their Role

As the DIGIT Act entails, Congress generally delegates individual enforcement powers to an administrative agency.[156] Since the introduction of IoT, the FTC is the administrative agency that has been the most concerned with the technology.[157] The FTC has already laid the groundwork by researching and reporting the effects of IoT.[158] Additionally, the FTC has used their broad powers under section 5 of the Federal Trade Commission Act to enforce misrepresentation claims against companies utilizing IoT technologies.[159] However, because the IoT is so dynamic, another administrative agency may also have a claim to regulate the technology.

After the October 2016 Mirai Botnet attacks,[160] which used the IoT to shut down popular websites throughout the United States, Senator Mark Warner sent a letter to the Federal Communications Commission (FCC) Chairman, Tom Wheeler, asking how the FCC could assist the Legislature in combating the IoT security issue.[161] Generally stated, the FCC "regulates

---

[154] *Id.*
[155] FEDERAL TRADE COMMISSION, *supra* note 54.
[156] DIGIT Act, S. 2607, 114th Cong. (2016) (as amended by S. Comm. on Commerce, Sci., and Transp., Sep. 27, 2016).
[157] *See* 15 U.S.C. §45 (2012).
[158] *Id.*
[159] *Id.*
[160] Woolf, *supra* note 60.
[161] Brendan Bordelon, *FCC Holds Off on Security Mandates for Internet of Things*, MORNING CONSULT (Oct. 31, 2016), https://morningconsult.com/2016/10/31/fcc-will-hold-off-security-mandates-internet-things.

interstate and international communications by radio, television, wire, satellite, and cable."[162] The FCC has not been directly vested with the power to deal with Internet security issues; however, "the FCC retains broad flexibility in determining whether security actions undertaken by telecommunication providers are reasonable."[163]

In November 2016, just over a week later, the FCC released a final report and order of the FCC's broadband privacy rule.[164] In that report, the FCC included the words "functional equivalents" to expand the definition of technologies that are subject to regulation by the FCC.[165] Additionally, the FCC made sure to specify that their reach included devices and sensors connected to the web, which are core requirements of IoT technologies.[166]

Given the present void in existing law, any mention of regulation of the IoT industry would be a step in the right direction, but the FCC's recent moves are somewhat concerning. Recognizing that the FTC may be the more appropriate agency to regulate the technology, FCC Commissioner Michael O'Reilly stated in his dissenting opinion that this order "makes this sweeping power grab without explaining how it has authority to do so."[167] Due to the FTC's activity within the IoT arena, Commissioner O'Reilly acknowledged that the FCC is behind the curve by stating, "[t]he Commission is intentionally setting itself on a collision course with the FTC[]."[168] More concerning, this privacy rule only requires the advance consent for "web browsing history, application usage history, and the *functional equivalents* of web browsing history or application usage

---

[162] *What We Do*, FED. COMMUNICATIONS COMM., https://www.fcc.gov/about-fcc/what-we-do (last visited Apr. 3, 2017).
[163] Bordelon, *supra* note 161.
[164] Paul Merrion, *FCC Privacy Rule Stakes Out Jurisdiction Over Internet of Things*, CQ ROLL CALL (Nov. 7, 2016), 2016 WL 6572693. This rule requires advanced consent for Internet providers to sell or share private consumer information.
[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] *Id.*

history."[169] Therefore, the FCC's language does not call for the regulation of websites or social media sites themselves and leaves a gap in the FCC's enforcement power.[170]

The IoT and its implications have caught the attention of the FCC, FTC, and the Congress. However, there appears to be a lack of consensus on what agency should take the lead in regulation of the IoT. In the meantime, IoT technology continues to evolve and become more prevalent in our society. Congress should explicitly decide which agency is in control of IoT regulation, consolidate both studies and research, and timely pursue IoT-specific regulation.

3. Creation of an Industry Standard

As an emerging technology integrates with society, multiple standards and platforms for the technology will be created.[171] As time progresses, the market will adopt the most efficient standard to facilitate growth of the technology.[172] Thus, the creation of an industry standard in emerging technologies within a capitalistic free market is a complex and dynamic process.[173] In the United States, standards are generally market-led and driven by competition in the private sector.[174] However, "the Federal Government may play an important role . . . where there are significant regulatory challenges."[175] Thus, the United States takes the position that the market should develop a standard on its own, but the government may actively participate in helping adopt and form the standards if necessary.[176]

The National Telecommunications & Information Administration ("NTIA"), acting under the authority of the

---

[169] *Id.* (emphasis added).
[170] *Id.*
[171] *See* Eoin O'Sullivan & Laure Brévignon-Dodin, *Role of Standardisation in Support of Emerging Technologies* (June 2012), http://www.ifm.eng.cam.ac.uk/uploads/Resources/Reports/OSullivan_Dodin_Role_of_Standardisation_June_2012__2_.pdf.
[172] *Id.*
[173] *Id.* at 3.
[174] *Id.* at 15.
[175] *Id.*
[176] *Id.* at 18.

Department of Commerce, published a green paper that addresses the role the government will take and the "possibility of a national IoT strategy."[177] The NTIA maintains the position that "[e]ncouraging private sector leadership in technology and standards development, and using a multistakeholder approach to policy making" is the best route to develop a uniform standard.[178] Consistent with that position, the NTIA will "advocate for and defend a globally connected, open, and interoperable IoT environment built upon *industry-driven*, *consensus-based standards*."[179] Moreover, because the NTIA's sole focus is advocating Internet policy issues and has a goal of "ensuring that the Internet remains an engine for continued innovation and economic growth," this is an appropriate agency to address the IoT.[180]

The National Institute of Standards and Technology ("NIST"), another agency under Department of Commerce control, has also issued a publication on IoT security.[181] The NIST is the government agency responsible for information security standards and guidelines.[182] In a July 2016 guidance, the NIST defined the IoT, presented universal terminology that can be used by all, and provided examples of how the different components (e.g., sensors, cameras, and phones) could be used together to create an effective business platform.[183] NIST's guideline facilitates growth by setting a clear foundation for businesses in the industry and those looking to enter to base their strategic decisions upon.[184]

---

[177] *Fostering the Advancement of the Internet of Things*, NTIA.DOC.GOV (Jan. 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.
[178] *Id*. at 2.
[179] *Id*. at 2. (emphasis added).
[180] NAT'L TELECOMM. & INFO. ADMIN., https://www.ntia.doc.gov/home (last visited Apr. 3, 2017).
[181] Jeffrey Voas, *Network of 'Things'*, NAT'L INST. OF STANDARDS AND TECH. (July 2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf.
[182] *Id*.
[183] *Id*. at 22.
[184] *Id*.

Consequently, the Department of Commerce, supported by the NTIA and NIST, demonstrates that the government is ready to take an active role in fostering the creation of uniform IoT standards.[185] However, there is still not a uniform business standard for IoT communication or security protocols.[186] Communication between devices is central to the IoT concept.[187] Therefore, in order to create a massive and efficient IoT, a uniform standard must be adopted so that all devices can communicate effectively, regardless of the manufacturer or type of device.[188] This problem is exacerbated by the choice between open-source or proprietary platforms.[189] For example, the very nature of a proprietary platform, such as Apple Homekit, discourages uniformity because of confidentiality and copyright laws.[190] However, the most recent protocol, Open Connectivity Foundation (OCF), has pulled together some of the earlier protocols and is pushing for an open-source platform that allows interoperability between devices.[191] OCF protocol could be an indication that the industry is moving towards a uniform standard.

Uniform security protocols for all devices would be a huge measure taken to protect the security of IoT networks.[192] If effective security protocols are implemented into all devices, it

---

[185] *See generally id*.; *Fostering the Advancement of the Internet of Things*, *supra* note 177.
[186] Susan D. Rector, *'Internet of Things' Protocols: Past and Future Trends*, LAW360 (Oct. 12, 2016), https://www.law360.com/articles/850593/internet-of-things-protocols-past-and-future-trends.
[187] *Id*.
[188] *Id.*
[189] *Id.* at 1–2. There are currently seven major protocols, some that incorporate open-source and others rely on proprietary standards: (1) Alljoyn & AllSeen Alliance; (2) Thread Group; (3) Open Interconnect Consortium (OIC); (4) Institute of Electrical and Electronics Engineers (IEEE); (5) ITU-T SG20; (6) Apple Homekit; and (7) Open Connectivity Foundation (OCF).
[190] *Id.* at 2.
[191] *Id.* OCF would incorporate major software platforms such as Android, IoS, and Windows.
[192] *Id.*

will vastly reduce the chance that an individual device can be used to gain unauthorized access to the entire IoT network.[193] Security protocols should include controls such as "role-based access control, secure data storage, cryptography, key management, authentication, integrity, and confidentiality of all data received and transmitted."[194]

Smart Stadiums stand to benefit greatly from industry standards of IoT communication and security protocols. Uniform communication protocols would ensure that every device, regardless of the manufacturer, would be able to exchange and transmit data effectively. When a sensor or IoT device breaks, it can be easily replaced without worry that it will disrupt the interoperability of the IoT. Additionally, if uniform security protocols were built into every device it would enhance both the security and privacy of the stadium by ensuring that single devices are not subject to unauthorized access.

All of the essential pieces are in place to create a uniform standard for the IoT industry. The government has stated their desire to facilitate the creation of a uniform standard, and should continue doing so.[195] In due course, our nation's capitalistic market will inevitably adopt an industry standard. However, in order to accomplish this in a rapid manner, it is important that all parties work together. The appropriate administrative agencies, such as NIST and NTIA, should continue to work with these groups to research, educate, and develop the best possible standard for the market. Additionally, the government should eliminate barriers to entry into the marketplace. Once the industry has reached consensus on a standard, Congress should hastily act to require these communication and security protocols as a minimum standard protection.

IV. RECOMMENDATIONS

After years of waiting to see the how IoT technologies would evolve, it is time for action. IoT specific legislation, such

---

[193] *Id.*
[194] *Id.* at 3.
[195] O'Sullivan & Brévignon-Dodin, *supra* note 171, at 18.

as the DIGIT Act, should be pushed through Congress. However, unlike the DIGIT Act, the legislation should unambiguously charge the appropriate administrative agencies with the power to enforce and take the lead in IoT regulation.[196] In doing so, Congress would consolidate agency control and accelerate IoT research.[197]

The IoT must protect the security and privacy of individuals, and standardization will help tackle both considerations. While the IoT industry may not have conceded to a standard protocol, the government should continue to take an active role in the standardization of the industry. Once there is an apparent standard, the government should recommend and educate the industry on the standard.

In the meantime, Smart Stadiums need to create their own standards in which they can minimize consumer risk. Aligned with the privacy principles and FTC recommendations, a Smart Stadium should implement built-in security features to protect the security and privacy of consumer data.[198] In doing so, the Smart Stadium ensures their customers are educated and understand the risks of IoT. Finally, a Smart Stadium should continue to compete with other businesses and innovate new uses for IoT technology while working together to benefit society through advancement.

V. CONCLUSION

The emergence of IoT technology is shaping our world into one previously thought unimaginable. The IoT will benefit our society by increasing efficiency, safety, and convenience for both businesses and consumers alike. However, with any emerging technology, the IoT implicates key legal issues such as security, privacy, data management, and the need for standards

---

[196] The FTC, due to their experience in IoT and regulatory powers, appears to be the appropriate agency to assign this role to.

[197] DIGIT Act, S. 88, 115th Cong. (2017). For example, the DIGIT Act, gives the research committee 1.5 years to complete its research and report its findings.

[198] These protections should include effective warnings, disclaimers, and terms of service.

and protocols. If left unchecked, the IoT could have negative effects. However, if dealt with effectively, the IoT will thrive while protecting the fundamental rights of individuals.

While this note focuses on IoT application to Smart Stadiums, these insights can be applied to any IoT application. Additionally, the Smart Stadium context is an example of the large-scale use of IoT technologies and could be an excellent case study for Congress or any administrative agency looking to expedite the research process.

Ultimately, Smart Stadiums are illustrative of what could be the next big thing for the IoT, "Smart Cities," and could demonstrate how to balance living with the freedoms the Constitution has granted to the citizens of the United States, such as privacy, autonomy, and freedom, against a world increasingly reliant upon these invasive technologies.

This is our nation's chance to become a leader in a technology that will shape the future. If the IoTs legal considerations are dealt with appropriately, it could foster the creativity and innovative spirit that sets the United States apart from the rest of the world, while creating a platform for IoT technologies to prosper.

***