". . .AND THE EYE IN THE SKY IS WATCHING US ALL"[1] – THE PRIVACY CONCERNS OF EMERGING TECHNOLOGICAL ADVANCES IN CASINO PLAYER TRACKING

*Stacy Norris**

INTRODUCTION

Casino patrons have come to expect the 'eye in the sky' watching their every move; heightened surveillance helps monitor the significant amount of money trading hands within the casino walls, and lately has taken a greater importance in monitoring suspicious activity.[2] Video surveillance is a part of daily life in a large majority of countries, with cameras ever-present in retail shops, parking garages, gas stations, and along public roads. What people might not be aware of, however, are the lengths that a casino will—and can—go to in order to track players' activity and become intimately involved with gamblers' identities. With more states legalizing gambling and new casinos popping up, there is an unprecedented opportunity for people to wager on their favorite games. Forty-six states currently have casino gambling, whether in privately owned or tribal casinos, and twenty-two states allow eighteen-year-olds to gamble at those casinos.[3]

Our technology-hungry society is faced with two questions: how far is too far for a company to track its customers and guests without disclosure, and how

* The author would like to say thank you to everyone involved in this article: to my family and friends for their love and support, to the UNLV William S. Boyd School of Law and past and current UNLV Gaming Law Journal staff, to the G2E Expo for inspiring this topic, and to the Electronic Privacy Information Center (EPIC) for fighting to protect our privacy. The author also acknowledges that technology moves faster than publishing and that additional sources and developments have happened since this note was written. What has not changed, however, is the need for transparency on where this information is going and how it will be used.

[1] CASINO (Universal Pictures 1995). *See* Geoff Schumacher, *You lookin' at us?*, NEV. PUB. RADIO (Oct. 22, 2015), https://knpr.org/desert-companion/2015-10/you-lookin-us.

[2] *See* Matt Pearce et al., *In Las Vegas, the casino is always watching – and yet it missed Stephen Paddock*, L.A. TIMES (Oct. 12, 2017, 3:00AM), http://www.latimes.com/nation/la-na-vegas-shooting-casino-security-20171012-story.html.

[3] *Complete Guide to USA Casino Gambling*, CASINO.ORG, https://www.casino.org/local/guide/ (last visited May 14, 2019).

much of this tracking is within the scope of the United States Constitution?

Casinos initially began tracking players to monitor levels of play and to reward those who gambled the most money ("high-rollers") at the casino.[4] This tracking has evolved into a method of creating a personalized experience for consumers while tiptoeing around the privacy line by collecting vast and varied information on unknowing guests and visitors.[5]

Part two of this Note will address the history of player tracking in casinos. Part three will address proposed technological advancements in player tracking and the emergence of futuristic methods of assessing player behavior, mood, and personal characteristics. Part four will address the constitutional issues, and whether these advancements in player tracking are or have the capacity to violate the Fourth or Fifth Amendments. Finally, part five will address how to balance the casino's interests and people's liberties and provide suggestions for how to achieve that balance. There is no easy answer in the debate of privacy versus technological advancements. This note will address the benefits and detriments of new technologies and will finish by proposing legislation to protect personal information in this new age of technology.

I. CASINOS TRACK YOUR EVERY MOVE, FOR THEIR BENEFIT AND YOURS

When one thinks of 'player tracking' as related to casinos, what comes to mind? Anyone who has been in a casino would likely think of the rewards card offered by casinos. Generally, in exchange for nothing more than a scan of one's driver license, the casino rewards center will turn a visitor into a card-carrying loyal patron.[6]

By using that card in slot machines and presenting it at table games, a player can accrue points through every dollar spent gambling, perhaps even earning a higher rewards level due to particularly robust play.[7] Behind the scenes, however, the casino is using that rewards card to track "which machines you played, how long you played them, coin-in (the amount you bet) and coin-out (the amount you won)" in addition to taking your driver's license information

---

[4] John Acres, *How Player Tracking Was Invented*, CASINO ENTERPRISE MGMT., Oct. 2006, *republished at* ACRES http://acres4.com/how-player-tracking-was-invented-by-john-acres/.

[5] *Id. See also* John G. Brokopp, *How much do casinos know about you?*, NWI.COM (Sept. 28, 2012), http://www.nwitimes.com/entertainment/columnists/john-brokopp/how-much-do-casinos-know-about-you/article_91e19c4b-f40e-58e3-8e66-1902856a3c1d.html.

[6] *See my BoardingPass Official Rules,* STATION CASINOS, https://www.sclv.com/MyBoardingPass/BoardingPassRules (last visited May 14, 2019).

[7] *See id*. *See also my BoardingPass Help & FAQ,* http://www.sclv.com/MyBoardingPass/FAQ (last visited May 16, 2019). For example, Station Casinos has five levels for their "Boarding Pass," ranging from the entry level "Preferred" to elite "Chairman" for those who have accrued 300,000 or more credits.

and "match[ing] it against third-party demographic data and tell[ing] whether a patron has kids or how much he makes per year."[8] This section will address the history of player tracking, as well as the current technology used by casinos to identify, monitor, and market to players.

A. History of Casino Player Tracking

Player tracking began in the 1960s and 1970s at the Harrah's Reno, in Reno, Nevada, where players received a paper coupon for every twenty dollars they gambled in slot machines.[9] The tickets, a tangible form of the points accrued today by casino patrons on their players cards, "could be exchanged for prizes such as toasters, transistor radios, and televisions at a redemption booth set up in the casino's basement."[10] This system evolved into slot machines adopting "automatic ticket dispensers" to remove the human ticket-giver element and automatically issue tickets to gamblers for every fifty dollars they put in the machine.[11]

John Acres, a former slot machine repairman who founded Electronic Data Technologies (EDT) in 1981, is one of the forefathers of player tracking.[12] EDT sold ticket dispensers to casinos in Las Vegas, but Acres quickly realized that the technology was insufficient for casinos' needs and too costly in comparison to their return.[13] A visit to a South African casino changed Acres' course, as it was there that he first experienced the use of plastic cards as keys to enter hotel rooms.[14] This discovery, coupled with his observation of the advanced technology in the children's toy "Speak & Spell,"[15] led Acres and EDT to develop the first method of tracking players' slot machine usage through "loyalty cards."[16]

Acres next big step was the development of progressive jackpots,[17] and before long other companies and forward-thinkers were moving into the field. In 1986, emerging powerhouse International Gaming Technology (IGT), whose focus previously had been on video lottery games and slot machine distribution,

---

[8] John G. Brokopp, *How much do casinos know about you?*, NWI.COM (Sept. 28, 2012), http://www.nwitimes.com/entertainment/columnists/john-brokopp/how-much-do-casinos-know-about-you/article_91e19c4b-f40e-58e3-8e66-1902856a3c1d.html; Kim Nash, *Casinos hit jackpot with customer data*, CNN.COM, (July 3, 2001, 8:59 AM), http://www.cnn.com/2001/TECH/industry/07/03/casinos.crm.idg/.

[9] Acres, *supra* note 4.

[10] *Id*.

[11] *Id*.

[12] *See* Adam Tanner, *House of Cards*, WORTH (Feb. 1, 2014), http://www.worth.com/house-of-cards/.

[13] *See* Acres, *supra* note 4.

[14] *Id*.

[15] *Id*.

[16] *See* Tanner, *supra* note 12.

[17] Acres, *supra* note 4.

established Megabucks, "a progressive slot machine linking Nevada casinos via phone line with a giant computer at IGT headquarters."[18] Soon after, other major players entered the scene, with Konami Gaming developing the "Konami Casino Management System, or KCMS" to apply contemporaneous player tracking and analysis.[19]

B. Emergence of Heightened Surveillance

Video surveillance has become a way of life around the globe, as countries and businesses alike have found benefit to monitoring activities to curb illegal activity, track individuals, and provide day-to-day operations oversight.

In London, England, 500,000 cameras surround the city to keep citizens safe and address security threats.[20] In the United States, cities have benefitted from surveillance systems on streets to identify criminals (e.g., the suspects in the Boston Marathon bombing) and in assisting police forces with "put[ting] more eyes on the streets."[21]

The casino industry was one of the first industries to adopt video surveillance technology in the 1960s and 1970s.[22] They began to employ surveillance for many purposes, including: (1) to catch cheaters; (2) to catch thieves; and, (3) to a lesser degree, to maintain safety of guests and employees.[23] Closed circuit television, or CCTV, surveillance in casinos was a huge breakthrough in allowing security a bigger picture of the casino floor than they would have walking the floor.[24] Cameras enabled casino security to monitor patterns of suspicious behavior "among thieves, cheats and dishonest employees" to prevent and detect "pick pocketing, employee theft, and card cheats."[25] However, this technology was not without its flaws: early casino surveillance in the late 1970s involved "cameras housed 'in bubbles the size of large black beach balls. They

---

[18] *See* Bill O'Driscoll, *Timeline: The IGT Story*, RENO GAZETTE J. (July 17, 2014, 3:05 PM), http://www.rgj.com/story/money/business/2014/07/16/timeline-igt-years/12728037/.

[19] Carolan Pepin, *Player Tracking: You've Come a Long Way, Baby*, GLOBAL GAMING BUS. MAG. (May 25, 2011), https://ggbmagazine.com/article/player-tracking-youve-come-a-long-way-baby/.

[20] *See* Jackie Valley, *You're Being Watched: Inside Las Vegas' Surveillance Culture*, LAS VEGAS SUN (Oct. 5, 2014), https://lasvegassun.com/youre-being-watched/.

[21] *Id.*

[22] Jennifer, *Security Cameras in Gaming*, VIDEOSURVEILLANCE.COM (Dec. 19, 2006, 7:28 AM), https://www.videosurveillance.com/blog/industry/hospitality/security_cameras_in_gaming.asp.

[23] *See* Jesse Davis West, *Is Biometric Surveillance Set To Replace Traditional Surveillance In Casinos?*, FACEFIRST (June 13, 2017), https://www.facefirst.com/blog/biometric-surveillance-set-replace-traditional-surveillance-casinos/.

[24] *Id.*

[25] Jennifer, *supra* note 22.

moved about two degrees a second. A little old lady with a walker could outrun the cameras.'"[26]

Since the 1970s, the technology of cameras and recording has evolved—from VHS to digital, HD, and wireless—and has allowed for better quality footage, ease of video storage, and a closer zoom.[27] Casino surveillance cameras can even detect infrared beams that could not normally be seen.[28] Today's camera systems involve "360-degree, high definition cameras that record with so much clarity that surveillance operators can zoom in after the fact," and "tracking software to follow certain people through the casino."[29]

C. Casino Player Tracking Today and Proposed New Technology—the Future is Now

Technological advancements in video surveillance, biometrics, and other varying means to identify and track people have reached an almost Orwellian level of intrusiveness. Indeed, "[w]ith the advent of smartphones and widespread surveillance cameras, no conversation or movement in the public sphere can be considered private."[30] Once the stuff of science fiction, facial recognition is now prevalent in an increasing number of products—from the new generation of iPhones which implement facial recognition to allow users to unlock their phone by holding it to their face,[31] to Facebook's "largest biometric database in the world" of photos submitted by users, which it uses to prompt users to tag their friends in uploaded photos.[32] Developers in China have even begun working on systems where people can purchase tickets, provide access to apartments, and

---

[26] J. Freedom du Lac, *At Maryland Live Casino, relentless surveillance operation targets cheats, thieves*, WASH. POST (Feb. 22, 2014), https://www.washington post.com/local/at-maryland-live-casino-relentless-surveillance-operation-targets-cheats-thieves/2014/02/22/e772bbd8-900a-11e3-b46a-5a3d0d2130da_story.html. .

[27] *See* Jennifer, *supra* note 22.

[28] *See* Daintry Duffy, *Casino Surveillance at Mohegan Sun: Two of a Kind*, CSOONLINE.COM (Oct. 1, 2003, 8:00 AM), https://www.csoonline.com/article/2116673/loss-prevention/casino-surveillance-at-mohegan-sun—two-of-a-kind.html.

[29] Freedom du Lac, *supra* note 26.

[30] Alan Greenblatt, *Our Surveillance Society: What Orwell and Kafka Might Say*, NPR (June 8, 2013, 3:31 PM), https://www.npr.org/2013/06/08/189792140/our-surveillance-society-what-orwell-and-kafka-might-say.

[31] *See* Kif Leswing, *Apple just released new information about how facial recognition on the iPhone X works,* BUS. INSIDER (Sept. 27, 2017, 12:00 PM), http://www.businessinsider.com/apple-new-details-iphone-x-facial-recognition-works-2017-9.

[32] Martin Kaste, *A Look Into Facebook's Potential To Recognize Anybody's Face*, NPR (Oct. 28, 2013, 3:38 AM), https://www.npr.org/sections/alltechconsidered/2013/10/28/228181778/a-look-into-facebooks-potential-to-recognize-anybodys-face.

pay at restaurants by just showing their face.[33]

Casinos began using facial recognition technology around the turn of the century.[34] It was introduced as far back as 1994 at the Bally's Las Vegas casino in Las Vegas, but the technology at that time was not advanced enough to follow a person nor to identify faces unless the person looked straight at the camera.[35] By the early 2000s, facial recognition had become a staple at casinos, and today the technology has advanced enough that some developers boast they can identify someone through facial recognition with fifty-five percent accuracy, despite the person's face being obscured with "a hat, scarf, and glasses," and sixty-nine percent accuracy "when just glasses were removed."[36]

By 2006, the Surveillance Information Network (SIN) contained 2,500 photographic records of "known cheats and hustlers" shared with casinos around the world.[37] By 2016, Biometrica—the company responsible for compiling the SIN—reported that they could "give subscribers the ability to run operational real-time facial recognition scans of any individual on their property against a law enforcement-verified database of criminals numbering in the millions."[38] Biometrica operates a global "security and surveillance operations center" out of Las Vegas and allows near-real-time mobile search access to their database of known criminal profiles, so casinos can quickly assess any criminal threats.[39]

"Biometrics" refers to the method of identifying persons through scanning a part of the human body possessing unique characteristics: "For identification, an image is run against a database of images. For authentication, an image has to be accessed from the device to confirm a match. The latter is typically used for unlocking computers, phones, and applications."[40] This can include fingerprint, facial, and iris scans; speech patterns; "heartbeat data"; "how you walk and type"; and "the uniqueness of vascular patterns in the eyes or even a person's specific gait. . .."[41]

---

[33] *See* Will Knight, *Paying with Your Face: 10 Breakthrough Technologies*, MIT TECH. REV. (Feb. 22, 2017), https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/.

[34] *See* Dan Koeppel, *Casino hackers*, CNN.COM (Oct. 23, 2006, 1:30 PM), http://www.cnn.com/2006/TECH/07/13/popsci.gambling/.

[35] *See* Valley, *supra* note 20.

[36] Jamie Condliffe, *Facial recognition is getting incredibly powerful, and even more controversial*, BUS. INSIDER (Sept. 8, 2017, 8:07 PM), http://www.business insider.com/facial-recognition-controversy-improvement-2017-9.

[37] *See* Koeppel*, supra* note 34.

[38] *Law Enforcement,* BIOMETRICA SYSTEMS INC, https://biometrica.com/law enforcement/ (last visited May 14, 2019).

[39] *SSIN (Security & Surveillance Information Network),* BIOMETRICA, https://bio metrica.com/products/ssin/ (last visited May 14, 2019).

[40] April Glaser, *Biometrics Are Coming, Along With Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM) https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.

[41] *Id.*

Through technological advancements in biometrics, casinos and developers have been working to incorporate this heightened identification into slot machine technology. In 2009, U.S. patent number 7,506,172 was issued for IGT for a "[g]aming device with biometric system."[42] This "gaming device" would incorporate a biometric fingerprint scan on the machine that could either compare information with an inserted card to verify the user's identity or "[t]he biometric data may be sensed through the button, meaning that the actuation of the button for a particular game function also actuates the biometric device, even if it is physically separated from the button. For example, a separate facial scan device could be actuated as the player initiates the game. . .."[43]

Further, in 2017 the U.S. Patent and Trademark Office (USPTO) issued patent number 9,754,445 to Tennessee-based Video Gaming Technologies, Inc. for a "[s]tress detecting input device for a gaming machine[.]"[44] This patent is for a slot machine with an "input device comprising a sensor configured to measure the interaction of the player with the input device" through biofeedback—"the processor is further programmed to execute a mental state calibration phase. . .collecting measured data from the sensor for a defined period of time; associating gaming events that correspond to the interaction of the player;. . .[and] determining a median mental state threshold for the player for each of the associated gaming events."[45] In another science-fiction-like twist, this patent is for technology that will detect "a level of stress; a level of positive excitement; a level of negative excitement; a level of depression; a level of boredom; and a level of intoxication" through collection of "biofeedback data" via "infrared cameras, pupil scanners, body movement scanners, body temperature sensors, blood pressure sensors, pulse sensors," and more.[46] Monitoring this data, according to the patent, will allow the machine to determine if "the player is stressed and/or his/her stress level is rising," and respond accordingly: "[A] message may appear that says 'Congratulations!! Take a few deep breaths and enjoy this moment!'" or the machine may provide a message with an option to take a break if it senses a player may be depressed.[47]

1. Proposed New Technology for Facial Recognition

With great technological advancements come great setbacks and controversies. Facial recognition technology might not be ready for widespread implementation, as facial recognition cameras around Los Angeles have

---

42 U.S. Patent No. 7,506,172 (filed Jan. 7, 2002).
43 *Id*.
44 U.S. Patent No. 9,754,445 (filed Dec. 31, 2013).
45 *Id*.
46 *Id*.
47 *Id*.

performed poorly on correctly identifying African Americans.[48] This flaw could result in "innocent citizens being marked as suspects in crimes,"[49] and misidentifying persons based on facial scans seems to negate the whole purpose of these systems. In a casino setting, this could lead to an innocent person being misidentified as a problem gambler or thief, which could lead to greater liability for casinos using this software if that information is then used against the customer. Arrests, public dissemination of private information, and the use of undisclosed personal information of a guest or their associates could severely and permanently impact the lives of innocent people simply out to have a good time.

In September 2017, news hit that a Stanford University study determined that artificial intelligence and "deep neural networks" can correctly identify a person's sexual orientation from photos with an eighty-one to ninety-one percent accuracy.[50] Studies have also been run on identifying criminals versus non-criminals through facial identification, and it's been suggested that eventually AI could be used to identify "other qualities, such as IQ or political leaning."[51] While this technology is still in development, casinos could conceivably use this additional identifying information to better classify, market to, and provide customized experiences for their players.[52]

Artificial intelligence that can detect your emotions and engagement level is also being perfected in the realm of video games.[53] Developer Affectiva has been working on technology dubbed "Emotion AI" to "humanize technology," allowing it to "respond to users' emotions in real time."[54] Affectiva's "Emotion Software Development Kit" works through use of a webcam or other recording device that can "identify key landmarks on the face. . .then analyze pixels in those regions to classify facial expressions. . .. Combinations of these facial expressions are then mapped to emotions."[55] In video games, this technology can

---

[48] *See* Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, THE ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[49] *Id*.

[50] Condliffe, *supra* note 36. *See also* Heather Murphy, *Why Stanford Researchers Tried to Create a 'Gaydar' Machine,* N.Y. TIMES (Oct. 9, 2017), https://www.nytimes.com/2017/10/09/science/stanford-sexual-orientation-study.html.

[51] Condliffe, *supra* note 36.

[52] *See* Natasha Dow Schüll, *The Touch-Point Collective: Crowd Contouring On The Casino Floor*, LIMN (Mar. 2012), https://limn.it/articles/the-touch-point-collective-crowd-contouring-on-the-casino-floor/.

[53] *See* Kevin Murnane, *Gaming: 'Nevermind' Reads Your Mind And Adapts To Your Emotions*, FORBES (Mar. 3, 2016 10:00 AM), https://www.forbes.com/sites/kevinmurnane/2016/03/03/gaming-nevermind-reads-your-mind-and-adapts-to-your-emotions/#53c17ef87c10.

[54] *SDK*, AFFECTIVA, https://www.affectiva.com/product/emotion-sdk/ (last visited May 14, 2019).

[55] *Id.*

create a different playing experience for each player playing the same game, with those who appear scared or hesitant getting a more intense experience than those who are not engaging as much.[56]

Affectiva's software combined with a slot machine could lead to the casino monitoring engagement with the machine, and providing bonuses or tweaking the odds of a payout in order to keep the player interested.[57] Additionally, this software can "identify 7 emotions, 20 expressions and 13 emojis" and "detects emotion on individual faces as well as for groups of 20+."[58] A casino could potentially use this software to monitor passing customers' interest or disinterest for the machine to better track machine preference in individuals.

II. AT WHAT POINT DO THESE TECHNOLOGICAL ADVANCEMENTS VIOLATE CONSTITUTIONAL RIGHTS OR CONSTITUTE AN INVASION OF PRIVACY?

The Fifth Amendment of the United States Constitution guarantees that no person shall be "deprived of life, liberty, or property, without due process of law[.]"[59] These due process rights have been applied to the individual states as well through the Fourteenth Amendment.[60] Additionally, the Fourth Amendment guarantees citizens the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]"[61] The United States Constitution guarantees these rights to citizens against federal or state government action, but what about the actions of private industries such as casinos?

Some states have enacted laws classifying casino operations as state action by developing casino control commissions to set requirements for casinos and oversee their operations.[62] Prior to the opening of the first casinos in their state, Ohio amended its state constitution by adding Article XV, Section (6)(C)(4), creating the "Ohio casino control commission" to "ensure the integrity of casino gaming" and empowering the Commission to approve minimum surveillance standards, and set requirements for development of a surveillance system plan.[63]

The United States Supreme Court vacillates in its position of declaring privacy as a constitutional right. While the Supreme Court still applies *Griswold v. Connecticut*[64] to state impositions on personal privacy and habits, recent cases

---

[56] *See* Murnane, *supra* note 53.

[57] *See* Matt Richtel, *From the Back Office, a Casino Can Change the Slot Machine in Seconds*, N.Y. TIMES (Apr. 12, 2006), https://www.nytimes.com/2006/04/12/technology/from-the-back-office-a-casino-can-change-the-slot-machine-in.html.

[58] AFFECTIVA, *supra* note 55.

[59] U.S. CONST. amend. V.

[60] *See id.* amend. XIV.

[61] *Id.* amend. IV.

[62] *See, e.g.*, OHIO CONST. art. XV, § 6(C)(1).

[63] *See id.* art. XV, § 6(C)(4). *See also* OHIO REV. CODE ANN. § 3772.03 (West 2018).

[64] 381 U.S. 479 (1965).

involving a person's privacy from their employer have found that any state or industry interest in the alleged privacy violation is sufficient to justify its existence.[65] In *Minnesota v. Carter*, the Supreme Court held that an expectation of privacy must be reasonable in order for a defendant's conduct to invoke Fourth Amendment protections.[66] Further, in *United States DOJ v. Reporters Comm. for Freedom of the Press*, the Court held that an individuals' privacy interest in their criminal history "rap sheet" (compiled by the DOJ on the Medico family of "organized crime figures") took precedence over the Freedom of Information Act.[67] In that case, a third-party request by CBS News for government-compiled criminal information was an unwarranted privacy intrusion.[68]

A. Constitutional Concerns of Collecting Personal Information?

However, is withholding personal information a violation of the Fourth Amendment right to be free from searches and seizures, or even Fifth Amendment due process rights? In 1965, the U.S. Supreme Court determined that there is only a "zone of privacy" created between the Third, Fourth, Fifth, and Ninth Amendments regarding intrusion on *fundamental* rights (in that case, to protect the relations of married couples).[69]

The concept of privacy in unauthorized dissemination of photos or personal information is not a new one. Justice Louis Brandeis, at the time a student at Harvard Law School, wrote "The Right to Privacy" in 1890, touching on what he believed to be just as important as any other right guaranteed by the Constitution: "the right 'to be let alone.'"[70] As far back as 1890 there existed "unauthorized circulation of portraits of private persons[,]" "invasion of privacy by the newspapers," and idle gossip that invaded people's lives and privacy.[71] Justice Brandeis's proposal of a right to privacy came as a result of the technological advancements in photography, after Brandeis saw that "the latest advancements in photographic art [had] rendered it possible to take pictures surreptitiously," allowing photos to be taken without consent and published.[72] He further broke down this right as extending to the protection of "the unwarranted invasion of individual privacy[,]" and exempting persons who

---

[65] *See, e.g.*, Nat'l Aeronautics and Space Admin. v. Nelson, 562 U.S. 134, 157–59 (2011) (remanding for proceedings consistent with opinion that the collection of background information from government employees was a lawful government interest and not a violation of the Privacy Act).

[66] 525 U.S. 83, 88 (1998) (citing Rakas v. Illinois, 439 U.S. 128, 143–44 (1978)).

[67] *See* Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762–65 (1989).

[68] *Id.* at 757, 771.

[69] *Griswold*, 381 U.S. at 485–86 (emphasis added).

[70] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[71] *Id.* at 195–96.

[72] *Id.* at 211.

choose to live their life in public, communications that would be "slander and libel[,]" oral publication, and information published with the individual's consent.[73] One has to wonder what Justice Brandeis would say of today's gossip magazines, surreptitious monitoring,[74] and video surveillance.

In 1967, the U.S. Supreme Court held that a person had a right to be free from unreasonable search and seizure under the Fourth Amendment while making calls in a glass-enclosed telephone booth.[75] In *Katz v. U.S.*, a criminal defendant was caught through the Federal Bureau of Investigation's tapping of his conversations while he used a telephone booth to unlawfully transmit wagering information.[76] In his majority opinion, Justice Stewart emphasized that this does not make telephone booths a "constitutionally protected area" with a "right to privacy."[77] He reworded the Fourth Amendment issue to broaden the scope of the right, stating that Katz had not "shed his right" to protection of his conversations "simply because he made his calls from a place where he might be seen[,]" noting that he "sought to exclude when he entered the booth. . .the uninvited ear."[78]

Advancements in biometrics within other fields have led to similar questions of constitutionality regarding the use of gained information for searches. The Supreme Court has interpreted the Fifth Amendment as "appl[ying] to compelled information that is of a testimonial or communicative nature[,]" and that "compelled production or displays of purely physical characteristics do not violate the Fifth Amendment's privilege."[79] Recently, courts have found it is not a violation of the Fifth Amendment for police to force suspects to unlock their phone through the fingerprint scanner or face scanner mechanisms.[80] Courts will likely continue to wrestle with this concept, seeing the biometric data as less testimonial than asking a suspect for their passcode, and balancing how the law treats something you know (a passcode) as being quite different than something you are (a biometric).[81]

---

[73] *Id.* at 214–18.

[74] *See* Ronald Holden, *Okay, Alexa, Promise You Won't Spy On Me, Okay?*, FORBES (Mar. 29, 2017, 1:53 PM), https://www.forbes.com/sites/ronaldholden/2017/03/29/okay-alexa-promise-you-wont-spy-on-me-okay/#445e10f05905.

[75] *See* Katz v. United States, 389 U.S. 347, 361–362 (1967).

[76] *Id.* at 348.

[77] *Id.* at 349–50.

[78] *Id.* at 352.

[79] Erin M. Sales, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, 69 U. MIAMI L. REV. 193, 195 (2014).

[80] *See* Cyrus Farivar, *Court rules against man who was forced to fingerprint-unlock his phone*, ARS TECHNICA (Jan. 18, 2017, 11:06 AM), https://arstechnica.com/tech-policy/2017/01/court-rules-against-man-who-was-forced-to-fingerprint-unlock-his-phone/.

[81] *Id. See* Cyrus Farivar, *Woman ordered to provide her fingerprint to unlock seized iPhone*, ARS TECHNICA (May 2, 2016, 2:49 PM), https://arstechnica.com/tech-policy/2016/05/should-the-govt-be-able-to-force-you-to-open-your-phone-with-

B. Are Casinos "State Actors" for Purposes of Constitutional Violations?

There is also the issue of whether casinos can be considered state actors for violations of player's constitutional rights. Courts have found that "[a] private actor may be considered a person acting under color of state law pursuant to [42 U.S.C. § 1983] when his conduct is 'fairly attributable to the state[,]'" and to this the Supreme Court applies three main tests: "1) the nexus test; 2) the public function test; and 3) the state compulsion test."[82] Under the "public function test" of Section 1983, "a private entity will be considered a state actor only if it is exercising powers that are traditionally and exclusively exercised by the state."[83]

The Iowa Supreme Court in 2006 held in *Green v. Racing Association of Central Iowa* that a gaming racetrack was not a state actor for purposes of a Fourteenth Amendment claim by jockeys, stating the necessity of "a sufficiently close nexus between the State and the challenged conduct to establish state action exists. . .."[84] In *Green*, the Iowa Supreme Court determined that despite a close relationship with the state in a mutually beneficial lease agreement, the County did not participate in any operations of the racetrack, nor use "coercive power" over the track's operations and management, and plaintiff jockeys failed to "show that Polk County benefited *from the constitutional violation alleged*[,]" not just from the operation of the track.[85]

Conversely, in 2008 the First District Court of Appeals in Michigan held in *Moore v. Detroit Entertainment, L.L.C.* that a casino that employed security guards who were state-licensed, state-trained, and worked closely with Michigan State Police made the casino itself a state actor regarding detention of patrons due to suspected theft.[86] In its fact-specific holding in *Moore*, the Michigan Court of Appeals cited *Romanski v. Detroit Entertainment, L.L.C.*, which held that since the casino's security officer was a licensed "private security police officer" under state law, thus having the "authority to arrest a person without a warrant[,]" that security officer was a state actor.[87]

This is where the clarity ends on this issue, however, as there are no Supreme Court decisions yet regarding tracking, investigation, and use of biometrics, biofeedback and facial recognition to monitor all aspects of a player's life.

---

just-your-fingerprint/.

[82] Christopher Pastore & Crystal Tatco, *Under the Color of State Law*, CASINO ENTERPRISE MGMT., June 2009, at 8.

[83] *Id.*

[84] Green v. Racing Ass'n of Cent. Iowa, 713 N.W.2d 234, 239 (Iowa 2006) (citing Burton v. Wilmington Parking Auth., 365 U.S. 715 (1961)).

[85] *Id.* at 242–43.

[86] Moore v. Detroit Entm't, L.L.C., 755 N.W.2d 686, 697–98 (Mich. Ct. App. 2008).

[87] *Id.* at 694 (citing Romanski v. Detroit Entm't, L.L.C., 428 F.3d 629, 633 (2005) (cert denied)).

C. If a Casino Is Not a State Actor, Could a Plaintiff Have a Cause of Action for Invasion of Privacy?

If it is determined that there is no constitutional violation in the covert monitoring and tracking of casino players through this new technology, it's worth considering whether a player could bring an invasion of privacy suit. There are four invasion of privacy torts: intrusion on seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a person in false light.[88] This section will focus on the possibility that covert, undisclosed monitoring via surveillance and biometrics could constitute intrusion on seclusion.

There are two elements to a claim for intrusion on seclusion: (1) intrusion on the "solitude or seclusion of another or his private affairs or concerns," "physically or otherwise", and (2) whether "the intrusion would be highly offensive to a reasonable person."[89] Therefore, tortious behavior occurs when a defendant has "intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy."[90] In *Hernandez v. Hillsides, Inc.,* the defendant employer's use of video surveillance equipment to catch unauthorized computer use was found not to be an invasion of privacy because it was narrowly tailored to a specific focus, and prompted by legitimate business concerns.[91]

Potential plaintiffs would have a difficult time proving they have a reasonable expectation of privacy in a casino, due to the widespread knowledge that casinos employ camera surveillance to monitor guests and money and prevent problems with either. Additionally, it is true that it is harder to question the reasonableness of an expectation of privacy outside of one's home.[92] However, while the conscious presence of cameras to ensure personal and financial safety may be known and accepted, the inquiry shifts to whether it is reasonable to expect the gathering of personal information through biometrics, facial recognition, and the extent of other personal information collected by casinos.[93]

Furthermore, the tort is difficult to show as it is unreasonable for a patron to expect "seclusion" within a casino or on casino property. Restatement (Second) of Torts §652B Comment (a) explains that the intrusion must be to one's "person

---

88 RESTATEMENT (SECOND) OF TORTS, § 652A (AM. LAW INST. 1977).

89 *Id.* § 652B

90 Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1072 (Cal. 2009).

91 *Id.* at 1082.

92 *See* Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. Crim. L. & Criminology 477, 483 (2007).

93 *See* ERIC Z. WYNN, PRIVACY IN THE FACE OF SURVEILLANCE: FOURTH AMENDMENT CONSIDERATIONS FOR FACIAL RECOGNITION TECHNOLOGY 46–47 (March 2015).

or as to his private affairs or concerns," and the drafters use the word "private" multiple times.[94] Indeed, the comment references that there was no liability for intrusion on seclusion where a defendant monitored a "special line not to be used for private calls[.]"[95] It is unlikely that a court would find that there was a reasonable expectation of privacy from video surveillance and facial recognition while at a slot machine within a casino.

The "seclusion" alleged, however, could be argued regarding the collection and/or monitoring of a player's biometric data. In 1998, the Colorado Court of Appeals in *Doe v. High-Tech Institute* found that an uncontested HIV test on a student's blood sample constituted an intrusion on seclusion as it was an "intrusion[] into a person's private concerns based upon a reasonable expectation of privacy in that area."[96] Here, the court recognized that "there is a generally recognized privacy interest in a person's body[,]" adding that "[b]ecause personal information concerning a person's health may be obtained through one's blood, urine, and other bodily products, such products cannot be extracted from a person or initially tested without either consent or proper authorization."[97] Additionally, the court went on to recognize a "privacy interest in information concerning one's health[,]" stating that consent was necessary before collecting a person's health records.[98] Finally, they addressed that the level of intrusiveness is not determined by the "minimal" size of the act, but rather by the level of offensiveness of the action.[99] "Indeed, 'the most basic violation [of one's right to privacy] possible involves the performance of unauthorized tests—that is, the non-consensual retrieval of previously unrevealed medical information that may be unknown even to [plaintiff][.]'"[100]

Using *Doe* as a framework, an argument could be made that there is an intrusion on seclusion in collection of biometric data such as that proposed in the aforementioned "stress detecting input device for a gaming machine" patent by Video Gaming Technologies.[101] It remains to be seen how courts will approach the concept of stress level, depression, heart rate, and emotional state, and whether they will view this more as medical data (private) or public information.

D. Will Casinos Be Required to Disclose New Monitoring Technology?

With the patents developed to use the new technology, a large question looms: Will casinos inform players of heightened tracking? After all, a slot

---

94 RESTATEMENT (SECOND) OF TORTS, § 652B cmt. a (AM. LAW INST. 1977).
95 *Id*. (REPORTER'S NOTES).
96 Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1061, 1068 (Colo. App. 1998)
97 *Id*. at 1068.
98 *Id*.
99 *Id*. at 1069.
100 *Id.* at 1070, (citing Norman-Bloodsaw v. Lawrence Berkeley Lab.,135 F.3d 1260, 1269 (9th Cir. 1998)).
101 *See* U.S. Patent No. 9,754,445 (filed Dec. 31, 2013).

machine that reads your fingerprint when you press a button could appear to be a tortious invasion of privacy, or an unreasonable search and seizure in violation of the Fourth Amendment.

Withholding this information from players and guests can be considered an additional security measure. The director of security at a casino in Maryland, while being interviewed for an article on casino security, flatly refused to confirm details about the surveillance system out of concern that too much information "might somehow give crooks and cheats an edge."[102] With a seemingly never-ending stream of guests intending to defraud casinos, this makes sense: Don't give the public an edge to develop ways around your security system.[103]

The American Civil Liberties Union will likely take a different stance on this matter. Back in 2010, the City of Tampa admitted that its use of facial recognition software, deployed on public streets and later at Super Bowl XXXV to identify threats among attendees, had failed to result in any arrests or tangible positive outcomes, despite the city's receipt of hefty federal grants.[104] The ACLU reached out to Tampa officials after learning of their use of surveillance and facial recognition, and called for public hearings to inform the public of the technology's use and address any concerns.[105] The ACLU expressed concern with the fact that the technology can be "used in a passive way that doesn't require the knowledge, consent, or participation of the subject"[106] as demonstrated by the fact that thousands of fans who attended Super Bowl XXXV had no idea they were being "silently digitized and matched up against the mug shots of criminals and terrorists[.]"[107]

States do have laws in place to mandate security of personal information collected by casinos, and as of 2010, forty-six states had enacted these laws.[108] For example, Nevada enacted NRS 603A to address the security of personal information required by state law and mandated notification when there is

---

102 Freedom du Lac, *supra* note 26.

103 *See id*.

104 *See* Ryan Singel, *Jan. 28, 2001: Hey, Don't Tampa With My Privacy*, WIRED (Jan. 28, 2010, 12:00 AM), https://www.wired.com/2010/01/0128tampa-super-bowl-facial-recognition/.

105 *See id.*; PRESS RELEASE, AMERICAN CIVIL LIBERTIES UNION, ACLU CALLS FOR PUBLIC HEARINGS ON TAMPA'S "SNOOPER BOWL" VIDEO SURVEILLANCE (Feb. 1, 2001), *available at* https://www.aclu.org/news/aclu-calls-public-hearings-tampas-snooper-bowl-video-surveillance.

106 *Facial Recognition Technology*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology (last visited May 14, 2019).

107 Press Release, *supra* note 105.

108 Letter from Randall E. Sayre, Member, Nev. Gaming Control Bd., to All Nonrestricted Licensees Who Maintain Personal and/or Financial Information of Patrons in a Computerized Database and Interested Persons (Dec. 15, 2010), *available at* https://gaming.nv.gov/modules/showdocument.aspx?documentid=5571.

unauthorized access.[109] However, Nevada "does not require a business to destroy [personal information] after a certain period of time[,]" meaning that casinos can hold on to player information indefinitely.[110] In response to technological developments, several states, such as Illinois, Texas, and Washington, have passed "Biometric Information Privacy" acts.[111] In 2014, Congress even entertained a Biometric Information Privacy Act, to prevent and set penalties for unauthorized disclosure of biometric information.[112] This bill was sponsored by Congressman Steve Stockman from Texas, but it died in the 113th Congress in 2014, and has not been introduced since.[113]

The unknown future uses of tracking facial movements and player biometrics has yet to be addressed by the ACLU, but will likely lead to the same result: casinos have a substantial amount of information on players as it is—to add physical characteristics, fingerprints, and facial scanning could mean the casino has a more thorough database on citizens than the government.

E. What Illinois' Biometrics Privacy Information Act Could Indicate for States and Private Companies Moving Forward

Illinois passed the Biometric Privacy Information Act in 2008 as a reaction to proposed testing of "biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias" in Chicago.[114] The Biometric Information Privacy Act (BIPA) "forbids the unauthorized collection and storing of some types of biometric data."[115] This means that biometric information (defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"[116]) taken surreptitiously and then shared or used to map facial features for recognition is prohibited by law: A person needs to be informed of the photograph and give their consent for it to be

---

109 *Id.*

110 Karl Rutledge, et al., *Casino Player Clubs & Nevada's Data Protection Requirements*, CASINO ENTERPRISE MGMT. (Dec. 2013), *available at* https://www.lrrc.com/files/Uploads/Documents/Rutledge_1213.pdf.

111 Karla Grossenbacher & Christopher W. Kelleher, *Hazards Ahead: Uptick in Biometric Privacy Laws Can Put Employers in Hot Seat*, SEYFARTH SHAW (Oct. 3, 2017), https://www.laborandemploymentlawcounsel.com/2017/10/hazards-ahead-uptick-in-biometric-privacy-laws-can-put-employers-in-hot-seat/#.

112 *See* Biometric Information Privacy Act, H.R. 4381, 113th Cong. § 4 (2014) (as introduced by H.R.).

113 *See H.R. 4381 - Biometric Information Privacy Act*, CONGRESS.GOV, https://www.congress.gov/bill/113th-congress/house-bill/4381/all-actions?q=%7B%22search%22%3A%5B%22H.+R.+4381+113th+Congress%22%5D%7D&r=3 (last visited May 14, 2019).

114 740 ILL. COMP. STAT. 14/1, 14/5 (2008).

115 Rivera v. Google, Inc., 238 F. Supp. 3d 1088, 1090 (N.D. Ill. 2017).

116 *Id.* at 1094-95.

used.[117] In a 2017 case out of Illinois, Google's use of photographs to create facial scans of plaintiffs was found to constitute a "biometric identifier," despite the Illinois Privacy Act's exclusion of "photographs" from its definition.[118]

Most concerning for casinos is the provision within BIPA that allows "[a]ny person aggrieved by a violation of this Act. . .a right of action in a State circuit court[.]"[119] Defendants found to have acted intentionally, recklessly, or negligently are liable for damages: "liquidated damages of $1,000 or actual damages, whichever is greater" for those acting negligently, and "liquidated damages of $5,000 or actual damages, whichever is greater" for those acting intentionally or recklessly.[120] Remedies also can include attorney fees and injunctive relief.[121]

As the use of technology has increased, so have the number of lawsuits. Illinois residents have sued local businesses and world-wide companies alike for their use of facial recognition software and fingerprint scans, and have engaged in class action suits to take on major corporations on behalf of all persons affected through the use of biometrics.[122] In *Norberg v. Shutterfly, Inc.*, a plaintiff brought a class action lawsuit against Shutterfly, an online photo-sharing company, alleging that the company's "facial recognition capabilities to identify and categorize photos based on the people in the photos" and "collecting, storing, and using the biometrics (face geometry)" of users was in violation of BIPA.[123] *Norberg* is particularly troublesome for companies: Although the plaintiff was not a user of Shutterfly's services, in denying the defendant's motion to dismiss, the Court found that the plaintiff had "plausibly stated a claim for relief under the BIPA" merely due to the fact that he could potentially be affected by their facial recognition technology.[124] Additionally, the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corporation* overturned a lower court and held that a plaintiff alleging a violation of BIPA "need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[125]

Notice seems to be the underlying theme of the recent Illinois cases. A recent class action complaint filed against Wow Bao restaurant in Illinois alleges that

---

117 *Id.* at 1093. *See also* 740 ILL. COMP. STAT. 14/15 (2008).

118 *Rivera*, 238 F. Supp. 3d at 1096–97.

119 740 ILL COMP. STAT. 14/20 (2008).

120 *Id.*

121 *Id*.

122 Amy Korte, *Illinois Employers Flooded with Class-Action Lawsuits Stemming from Biometric Privacy Law*, ILL. POLICY (Oct. 17, 2017), https://www.illinois policy.org/illinois-employers-flooded-with-class-action-lawsuits-stemming-from-biometric-privacy-law/.

123 Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

124 *See id.*

125 Rosenbach v. Six Flags Entm't Corp., No. 123186, 2019 WL 323902, at *8 (Ill. Jan. 25, 2019).

the plaintiff's main concerns regarding the restaurant's acquiring facial biometric data to provide "authentication for food and beverage purchases" are the failure to notify consumers of the "specific purpose and length of time" relating to collection of their biometric data, the need to "[p]rovide a publicly available retention schedule and guidelines for permanently destroying" biometric data, and the need to obtain "a written release. . .to collect, capture, or otherwise obtain their facial biometrics, as required by BIPA."[126]

The impact of these cases on casinos who choose to incorporate biometric data collection could be huge. Obtaining consent from casino players would not be enough; casinos would have to obtain consent from everyone walking through the doors, as a facial-recognition camera system in the sky or in slot machines could collect and store data on all persons inside or near the casino.

III. THE MORALITY DECISION: USE THIS INFORMATION FOR GOOD OR EVIL?

The sheer amount of player and guest information that casinos compile and hold perpetually is of a size beyond comprehension. Back in 2001, CNN reported that MGM Resorts International's Mirage Las Vegas Hotel & Casino had a six-terabyte database of its customers, and the casino boasted that it could "tell you which of its 9 million customers are poker players who also like onions on their hamburgers."[127] Additionally, Harrah's Las Vegas Hotel & Casino has reported that it does not delete any customer data; unable to anticipate future uses for the information, it has retained all customer data since 1995.[128] The amount and diversity of information retained by casinos leads to questions regarding how it is being used. This information can be used to benefit consumers, such as by providing a customized and personal experience for players, and combating problem gambling by identifying risk factors before a player loses it all.[129] For the casino, this data can help establish trends such as "[i]dentification of peak hours and low occupancy hours" as well as "[i]ncreased retention of players[.]"[130] However, it could foreseeably be used to manipulate customers and

---

[126] Class Action Complaint at 3, 7, Regina Morris v. Wow Bao Franchising, L.L.C., No. 2017-CH-12029 (Ill. Cir. Ct. Sept. 5, 2017). *See also* Class Action Complaint, Howe v. Speedway LLC, No. 2017-CH-11992, 2017 WL 4019942, ¶ 5 (Ill. Cir. Ct. Sept. 1, 2017) (alleging violations of BIPA because of a lack of requisite notice and consent, and failure to post a data retention schedule); Jeffrey D. Neuburger, *Wow! Illinois Biometric Privacy Suits Proliferate*, NAT'L L. REV. (Sept. 27, 2017) https://www.natlawreview.com/article/wow-illinois-biometric-privacy-suits-proliferate (discussing the *Wow Bao* and *Speedway* complaints).

[127] Nash, *supra* note 8.

[128] *Id.*

[129] *See* Tony Bradley, *AI is Transforming the World of Online Casino Gambling*, TECHSPECTIVE (Feb. 19, 2018), https://techspective.net/2018/02/19/ai-transforming-world-online-casino-gambling/.

[130] *Player Tracking & Rewards,* DELTA CASINO SYSTEMS, https://lydiancms.com/

encourage problem gambling, and this data further runs the ever-present risk of a security breach.[131]

A. How this Advanced Player Tracking Technology Can Benefit Consumers/Players

With online gambling becoming more prevalent, and the average consumer spending more time on their phone than out socially, casinos are evolving to provide a more personalized experience through "personal attention" that shows that you are important to them.[132] Through tracking player information and equipping facial recognition and fingerprint-scanning software, casinos can identify their preferred customers and high rollers as soon as they step onto the property, enabling staff to give them the "red-carpet treatment": "[w]e make sure they have flowers in the room, a drink in the hand and reservations at the restaurant[.]"[133]

This new technology can give players an immersive experience: Indian Gaming Magazine, reporting on Novomatic Biometric Systems (NBS), states that the technology will allow "the entire offering within a resort [to] be accessed via [players'] fingertips[,]" allowing a "single wallet across land-based, online, mobile and social casinos, which encourages play, as well as ensuring prompt and accurate payments."[134] The magazine continues that the biometric experience will be a natural transition to players, many of whom are accustomed to fingerprint scanners to unlock their phones and pay for items.[135] Novomatic sees their fingerprint scanner technology, which creates a "template of the fingerprint" and uploads it to a local and central server with a one-million template capacity, as providing "[c]ontrolled access to gaming premises/gaming floors" (preventing access by minors), "[a]ccess to the gaming machine" (to promote "responsible gaming"), "[t]ransfer of credits between gaming machines and ATM/cash desks[,]" and use for food and betting purchases.[136]

Additionally, tracking players at machines—through facial recognition or player loyalty cards—enables the casino to customize players' experiences. The

---

features/player-tracking-rewards/ (last visited May 14, 2019).

131 *See* Michael Kaplan, *How Vegas Security Drives Surveillance Tech Everywhere*, POPULAR MECHANICS (Jan. 1, 2010), https://www.popularmechanics.com/technology/security/how-to/a5226/4341499/ (explaining advanced technology in the casino industry and its resulting susceptibility to breach).

132 *See id.*

133 Nash, *supra* note 8.

134 *Technology Frontrunner: Novomatic Biometric Systems*, INDIAN GAMING, Mar. 2016, at 58.

135 *See id*.

136 *Novomatic Biometric Systems*, NOVOMATIC, http://www.novomatic.com/en/products/gaming/games/novomatic-biometric-systems (last visited May 14, 2019) [hereinafter NBS].

Aria casino's slot machines are on a server, "allowing supervisors to alter machines simply by pushing backroom buttons that can change games, odds and limits to suit the player or the situation. If a player is in town for the National Finals Rodeo, the slot machine could load up a game with a rodeo theme. . .[i]t'll even wish him happy birthday."[137]

Finally, this technology can also be used to help prevent problem gambling. If casinos were to adapt biometric recognition combined with machines on a server, "it would give players the ability to opt out. So you could go to casinos. . .and say, 'Hey I don't want to gamble anymore. It's not for me, I have a problem.' And the way bio metric recognition would work, is if you were to sit down at the machine, it would literally not let you bet."[138] Additionally, following the Novomatic model, a casino could recognize a problem gambler (or the gambler could self-identify to the casino), and that gambler could be shut off from playing machines through rejection of their fingerprint scan.[139] Problem gamblers are a big issue for casinos, and attempting self-exclusion programs and counseling have had low success rates.[140]

B. How This Technology Can Negatively Impact Players/Guests

With the growing technology of player tracking and biometrics in casinos, it stands to reason that eventually the casino will know you better than you know yourself. From player's club cards to track what you play and how much you bet,[141] to facial recognition software with the ability to detect one's sexual orientation[142] and compare facial images with a national database to obtain additional information, there is an almost unlimited amount of information that casinos can obtain about their players in a matter of seconds. There is cause for concern, as casinos are gathering extensive information about your identity, personal life, and associations and storing it within an online database that can be susceptible to hackers; growing technology could lead to manipulation of games to maximize casino profits at the expense of guests, and could increase the risk that problem gambling will be assessed and exploited.

The most obvious concern with a cache of information this large would be cybersecurity breaches. Casinos store an unprecedented amount of player data (MGM Mirage reported six terabytes of data in 2001 alone, and Harrah's

---

137 Kaplan, *supra* note 131.

138 Brian Bull, *Casinos Track Action With All-Seeing Electronic Eye*, IDEASTREAM (May 22, 2012), http://www.ideastream.org/news/casinos-track-action-with-all-seeing-electronic-eye.

139 *See generally* NOVOMATIC BIOMETRIC SYSTEMS, *supra* note 136.

140 Jon Woodward & Mi-Jung Lee, *CTV hidden camera probe sparks casino review*, CTV NEWS VANCOUVER (last updated Nov. 27, 2015, 10:02 AM), https://bc.ctvnews.ca/ctv-hidden-camera-probe-sparks-casino-review-1.519256.

141 Brokopp, *supra* note 8.

142 Condliffe, *supra* note 36.

reported their database includes information on 23 million people the same year[143]), and with a global count of roughly 8,918 casinos and betting establishments worldwide[144] and more casino chains merging and opening properties around the world, the number of persons affected by a security breach of an information network would likely be larger than that of the 2017 Equifax breach, which is said to have affected 143 million people in the United States.[145] Further, like the Equifax breach, a breach of a casino's information cache would reveal personal information with devastating results—everything from vital statistics (driver's license information) to the routine (shows attended, restaurants visited, slot machines played), and, so far as the facial recognition results are concerned, criminal records unearthed, and persons associated with the casino.[146] Further, the value of these information caches can be astronomical: Caesars Entertainment's vast store of customer data has been valued at about $1 billion.[147]

Additionally, through player monitoring, casinos can—and likely will—move into the area of personalizing the gambling experience.[148] Through personalization, the machines could be adjusted to provide big wins, withhold wins entirely, and ensure that busier nights are more lucrative for the casinos.[149] The technology and capability to adjust slot machines from a back office already exists, as the New York Times reported in 2006.[150] The New York Times reported that a casino executive could, "[w]ith a few clicks of his computer mouse," adjust all machines on the floor to have new denominations required and new payout schedules.[151] The potential for abuse is staggering: combining the technology to adjust machines with the technology to obtain personal information about players immediately, the casino could theoretically woo high

---

143 *See* Nash, *supra* note 8. *See also* Tim Fisher, *Terabytes, Gigabytes, & Petabytes: How Big are They?*, LIFEWIRE (last updated Jan. 7, 2019), https://www.lifewire.com/terabytes-gigabytes-amp-petabytes-how-big-are-they-4125169 (noting that one terabyte is about 1,000 gigabytes. Therefore, to put MGM's six-terabytes of data in 2001 into perspective, consider that one terabyte would be roughly 130,000 digital photos, and that the Hubble Telescope generates ten terabytes of information every year).

144 *Worldwide Casinos, Horse Tracks and Other Gaming*, CASINO CITY, http://www.casinocity.com/casinos/ (last visited May 15, 2019).

145 Gillian B. White, *A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable*, THE ATLANTIC (Sept. 7, 2017), https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/.

146 *See* Rutledge, *supra* note 110, at 16.

147 Andrew Thompson, *Engineers of Addiction: Slot Machines Perfected Addictive Gaming. Now, Tech Want Their Tricks,* THE VERGE, https://www.theverge.com/2015/5/6/8544303/casino-slot-machine-gambling-addiction-psychology-mobile-games (last visited May 14, 2019).

148 *See* Tanner, *supra* note 12.

149 *See id.*

150 Richtel, *supra* note 57.

151 *Id.*

rollers by manipulating machines to pay them large sums, while discouraging low-level gamblers by preventing payouts entirely. And monitoring how long someone stays at a machine can allow the casino to manipulate the patron's behavior by providing rewards to encourage longer play.[152]

Finally, there is a growing concern with problem gambling, and the technology addressed in this note creates a dilemma for casinos. By collecting information on machines played, amount of time played, amount bet per hand, and a persons' accrued losses over time and coupling that information with biometrics from their play, such as increased heart rate and the amount they drink, casinos can determine if a player is a problem gambler.[153] Slot machines are profitable because they create an addiction: people are addicted to the rhythm of the game and some claim that machines are designed to "lull [players] into a trancelike state. . .."[154] Slot machines and their varying, seemingly randomized payouts work in much the same way that food worked in psychologist B.F. Skinner's research on operant conditioning, which showed that a pigeon will press a lever more often if food comes out at random intervals.[155]

Compulsive gamblers are a huge source of casino profits, with some reports claiming that they account for up to sixty percent of total gambling revenues.[156] Using player tracking to identify problem gamblers could encourage casinos to focus their marketing efforts on these players, attracting them with free play offers, "complimentary drinks and meals, limo service, freebies from the casino gift shop," and more to encourage them to visit, stay longer, and spend more money.[157]

IV. CONCLUSION

The world is changing, and technology that was once the subject of science-fiction novels has crept into our daily lives. From smartphones that are perpetually tracking our GPS location, to facial recognition software that enhances photographs, we are growing increasingly more comfortable with computers, phones, and the internet knowing a bundle of our personal information. For the facial recognition and biometric technology that casinos are entertaining for player tracking, security, and enhancement of customer experience, the comfort level of technology among existing consumers would seem to suggest an easy transition. After all, if one's phone can be unlocked through facial recognition, how far-fetched is a slot machine that can recognize

---

152 *See* Thompson, *supra* note 147.

153 *See generally* John Rosengren, *How Casinos Enable Gambling Addicts*, THE ATLANTIC (Dec. 2016), https://www.theatlantic.com/magazine/archive/2016/12/losing-it-all/505814/.

154 *Id.*

155 *See* Thompson, *supra* note 147.

156 Rosengren, *supra* note 153.

157 *Id.*

a player when they sit down?

In truth, there is not much one can do in the way of recommending that casinos should or should not incorporate this new technology, as it is inevitable that the benefits to casinos of enhanced player tracking and the collection of biometric data to create a personalized experience will outweigh the concern that some will feel invaded. The patents have been filed for years, and the technology is waiting to be implemented.[158] Some may already be in place without the author's knowledge, as casinos' security outfits keep a tight lid on their operations.

Illinois' Biometric Information Privacy Act is a great example of legislation that allows for the use of biometric technology if people are given notice that their information is being collected, notice of what that information will be used for and how long, and the ability to consent or refuse consent to the collection and use of their data. The growing number of class-action lawsuits in Illinois should indicate to other states that this is an area that requires attention moving forward, as it is a growing concern that information is being collected without consent or notice. The best recommendation would be for states to model their own acts based on the Illinois BIPA Act – recognizing a personal interest in the privacy of their biometric data, and encouraging transparency from businesses regarding their projected use and storage of that data. The definition of 'data' should also include any information gleamed from enhanced facial recognition software, as the technological advancements in determining sexuality and emotions from facial patterns and expressions will likely be superseded by newer, more invasive software in the coming years.

Technology is not inherently bad or good, and it's important to keep in mind that although a personalized experience or a full report of a person's life and associates from a photo of their face can be convenient from a business perspective, individuals still have a reasonable expectation that information they have chosen not to share publicly will remain private. The casino industry is based on customer loyalty and winning consumers' trust and money through service; one wrong step in the collection of personal information could destroy that trust forever.

---

158 *See* U.S. Patent No. 7,506,172 (filed Jan. 7, 2002); U.S. Patent No. 9,754,445 (filed Dec. 31, 2013).