CSI LAS VEGAS: PRIVACY, POLICING, AND PROFITEERING IN CASINO STRUCTURED INTELLIGENCE

Jessica D. Gabel*

I. INTRODUCTION

"I saw you before you even got up this morning."[1] That line from the 2001 casino heist movie *Ocean's Eleven* epitomizes the day-to-day business of casino surveillance. You can gamble, eat, drink, sleep, and shop, but you cannot hide in a casino.[2] The notion that casino bosses—and their security teams—watch every nook, cranny, and person within the casino is now accepted and even expected. After all, one notorious ring of card counters might attempt to bring down the house.[3]

In their heyday, casinos conjured up a myriad of images: high rollers, Elvis, the Rat Pack,[4] mob money, craps tables packed tight with a fabulous crowd, and the overall "loose" vibe that promised "what happens in Vegas, stays in Vegas."[5] The casinos of today have attempted to—at least in some

* Assistant Professor of Law, Georgia State University College of Law. I would like to thank my talented and dedicated research assistant, Kimberly Reeves, for her research prowess, copious editing, and generally keeping me sane while writing this.

[1] OCEAN'S ELEVEN (Warner Bros. Pictures 2001).

[2] *See, e.g.*, Mark Gruetze, *Casino Surveillance Theme: "I'll be Watching You"*, PITTSBURGH TRIB.-REV., Apr. 29, 2011, http://www.pittsburghlive.com/x/pittsburghtrib/ae/gambling/s_734644.html.

[3] The card counting expertise of six M.I.T. students attained nationwide fame after their antics were memorialized in print and on film. *See generally* BEN MEZRICH, BRINGING DOWN THE HOUSE (2002); 21 (Sony Pictures 2008). The students, referred to as the "M.I.T. Blackjack Team," supposedly "took Vegas for millions," until advances in security technology thwarted the team's efforts. *Id.* Although the book originally sold as non-fiction, subsequent media sources question the credibility. *See also* Drake Bennett, *House of Cards*, BOSTON GLOBE, Apr. 6, 2008, http://www.boston.com/bostonglobe/ideas/articles/2008/04/06/house_of_cards/.

[4] Popular crooners Frank Sinatra, Dean Martin, Sammy Davis, Jr., Peter Lawford, and Joey Bishop made up the Rat Pack. Wil Haygood, *The Rat Pack: 5 Hepcats who Made Vegas their Living Room*, SEATTLE TIMES, Oct. 28, 2007, http://seattletimes.nwsource.com/html/musicnightlife/2003973045_ratpack28.html. The group epitomized Vegas cool during the 1950s. *Id.* Frequent headliners at the Sands Hotel in Las Vegas, the men were widely popular all over the Vegas Strip. *Id.* "Wit and savoir-faire were their stock in trade;" consequently, the Rat Pack men were loved not only because of their talent, but also their charm. *See id.* Despite their success, the entertainers were also known to be generous towards workers and other patrons alike. *See id.*

[5] Michael McCarthy, *Vegas Goes Back to Naughty Roots*, USA TODAY, Apr. 11, 2005, http://www.usatoday.com/money/advertising/adtrack/2005-04-11-track-vegas_x.htm ("Lost all your cash at the casino? Wake up with a hottie you don't recognize? Don't sweat it in Las Vegas. As its new ad slogan goes: 'What happens here, stays here.'").

instances—sanitize their reputations and reinvent their images. Casinos have become children-friendly destinations for family vacations.[6] Classic Vegas enterprises, like the Dunes[7] and the Stardust,[8] have been supplanted by elaborate and increasingly large resort-style casinos such as Aria[9] and the Palazzo.[10] Moreover, casinos are no longer limited to Las Vegas, Atlantic City, and international destinations such as Monte Carlo. With increasing frequency, gaming facilities have now popped up on Native American Indian reservations and along the shores of the Gulf Coast.[11] With increased competition comes the technocratic race to modernize facilities, generate revenue, and minimize losses. Thus, it was only a matter of time before casinos employed some of the most elaborate surveillance and security systems in the world.[12]

Today, most casinos boldly acknowledge the extent to which they monitor the goings on. In a large casino, thousands of cameras may be on the visual prowl[13] looking for dealers on the take, hand mucking, and, of course, card

[6] Station Casinos, for example, advertises its "Kids Quest – Kid Friendly Hotel Entertainment, where your kids can have fun, so you can too!" STATION CASINOS, http://www.stationcasinos.com/entertainment/kids-quest/ (last visited Mar. 1, 2012).

[7] The Dunes Hotel debuted in the 1950s and survived as a fixture on the strip for forty years. *Dunes Hotel*, ONLINE NEVADA ENCYCLOPEDIA, http://onlinenevada.org/dunes_hotel (Mar. 1, 2012) ("One of the venerated original properties associated with the Las Vegas Strip, the Dunes Hotel opened during a mid-1950s casino building boom, and soon became one of its casualties. Over the next four decades, the controversial Dunes would survive a succession of owners, allegations of hidden mob ownership, and marginal profits before it was destroyed to make way for several Las Vegas resorts including the $2 billion Bellagio Hotel.").

[8] The Stardust Hotel and Casino survived nearly fifty years until it too had to give way to a new crop of resort properties in 2007. Steve Friess, *Stardust Hotel-Casino in Las Vegas is Demolished*, N.Y. TIMES, Mar. 13, 2007, http://www.nytimes.com/2007/03/13/us/13cndcasino.html.

[9] Opened in late 2009, the Aria Resort and Casino boasts a bevy of high-tech details such as "smart rooms," room access via your smartphone, and menus that tabulate not only patron orders, but also every time a menu is viewed. John Scott Lewinski, *The High-Tech, Luxury, Surveillance Hotel*, POPULAR MECHANICS (Apr. 21, 2010), http://www.popularmechanics.com/technology/engineering/architecture/aria-high-tech-hotel.

[10] The Palazzo lures vacationers and convention goers with spa services, upscale retail, dining—and of course—gambling. Rob Hard, *The Palazzo in Las Vegas*, BUS. TRAVEL DESTINATIONS.COM (Oct. 17.2011), http://businesstraveldestinations.com/2011/10/the-palazzo-in-las-vegas-hotel-review-venetian/.

[11] According to a 2007 Environmental Protection Agency (EPA) report, "casino gambling (including land-based, riverboat, limited stakes, tribal, and racinos) was occurring in 38 states." EPA, CHP IN THE HOTEL AND CASINO MARKET SECTORS, ADDENDUM I: MARKET UPDATE at 5 (2007). Connecticut is home to the well-known Foxwoods Resort and Casino and the Mohegan Sun Casino and Hotel, both of which are owned by Native American Tribes. *Id.* at 8-9. Post-Hurricane Katrina gaming companies invested large amounts of capital to develop and reopen casinos along the Gulf. *Id.* at 1.

[12] Michael Kaplan, *The Machines . . . are Watching*, POPULAR MECHANICS (Feb. 1, 2010), http://www.popularmechanics.co.za/article/the-machines-are-watching-2010-02-01 ("Las vegas [sic] casinos are incubators of the world's most advanced surveillance tech. And the spy gear that helps sin city [sic] has taught everyone from government to big banks how to snoop more effectively.").

[13] For example, the Rivers Casino's security efforts include a staff of employees to monitor live camera feeds from over 1,000 cameras. Gruetze, *supra* note 2. In addition to the constant overview, the touch screen monitors allow security analysts to zoom in for a closer view of any seemingly suspect activity. *Id.*

counters.[14] Many of the cameras are contained within black bubbles that loom from the ceiling and sweep the room with a 360-degree view.[15] The black bubbles create omnipresent features that reinforce the tacit understanding that someone is always watching.[16]

With the countless eyes and ears piercing through the smoke-filled casino floors, the questions become: what information are they capturing and what are they doing with it? It might surprise casino goers to learn that the Vegas-sized surveillance is not just to monitor the room for an unscrupulous gambler or two. It is not just that every camera in a casino is connected to recorders that document the life of a casino nonstop.[17] Specialized software tracks chips and specific cards.[18] Pit bosses know which tables are turning a profit and which ones are losing.[19] Moreover, casino patrons can be tracked via player's club cards.[20] The player's club cards—similar to airline loyalty programs—allow subscribers to earn credits each time the card is used in a casino that participates in the program.[21] Cardholders can put credit on the card and use it in lieu of cash to gamble. Purveyors of the cards urge participants to keep the card inserted in the slot machine or to hand it off to a dealer for table games.[22]

But the cards are more than just a means to earn points toward hotel nights, free dinners, and spa treatments. Casinos track their customers' habits and preferences by monitoring the card.[23] The cards may also be linked to records that maintain the customer's win/loss history and even his or her credit rating.[24] Some casinos go so far as to take players' pictures for the cards, and at some casinos, even fingerprints.[25] Even casino employees cannot escape the scrutiny of casino technology. Employee identification cards come equipped with chips that transmit the employee's location as they pass through different

---

[14] Kaplan, *supra* note 12.

[15] Gruetze, *supra* note 2.

[16] *See id.*

[17] Joseph Harrison, *Eye in the* Sky, 3 CASINO CONNECTION (2006), *available at* http://www.casinoconnectionac.com/articles/Eye_In_The_Sky.

[18] *Id.*

[19] *See id.*

[20] DAVID L. OLSON & DURSUN DELEN, ADVANCED DATA MINING TECHNIQUES 6 (2008). For example, Harrah's Entertainment, Inc., utilizes a "Total Gold" card that operates similar to the discount cards issued by grocery and drug store chains. *Id.* Patrons use the card to gamble, buy food and drinks, etc. *Id.* The customer receives dividends redeemable toward other services in exchange. Trump, Bellagio, and Mandalay Bay all have similar programs, which operate to "identify high rollers, so that these valued customers can be cultivated." *Id.*

[21] *How to Get Caesars Total Rewards Card in Las Vegas*, LAS VEGAS HOW-TO, http://www.lasvegas-how-to.com/total-rewards.php (last visited Mar. 1, 2012).

[22] *Id.*

[23] *See* Harrison, *supra* note 17; *see also* Andre Szykier, *Cracking the Code: Behavioral Targeting for the Gaming Industry*, CLEAR PEAK, http://clear-peak.com/wp-content/uploads/2011/09/Cracking-the-Code-Behavioral-Targeting-for-the-Gaming-Industry.pdf (last visited Mar. 3, 2012).

[24] The data mining firm Clear Peak is one company to offer this product. *See* Szykier, *supra* note 23.

[25] Harrison, *supra* note 17.

doorways.[26] Thus, the pit boss may know if an employee has a tiny bladder or takes an extra smoke break.[27]

The information that casinos collect on both their customers and employees does not always remain within the doors of the casino. Systems such as the Surveillance Information Network managed by Biometrica Systems[28] and corresponding programs like the Non-Obvious Relationship Awareness ("NORA") allow casinos to share information between and among themselves.[29] In one case, a casino in Atlantic City disseminated information about a man cheating on roulette (by distracting dealers and putting bets down after the ball dropped).[30] Because of information sharing among casinos on a global scale, the man was discovered rigging the same game in Lithuania, where he was arrested.[31]

The information sharing extends beyond the confines of the casino community. For instance, casinos can gain access to law enforcement databases that support its facial recognition software—pioneered by the gaming industry to follow suspected card counters, thieves, and other unscrupulous scoundrels.[32] Moreover, the flow of information is a two-way street, as law enforcement agencies in areas with robust gaming frequently borrow from casino files (and technology) as well.[33] The NORA software permits casinos to determine quickly if a player and dealer suspected of colluding have ever had a mutual phone number, split a room at the casino hotel, or lived at the same address.[34] Although the NORA software was initially created for the gaming industry, the United States Department of Homeland Security adapted it to detect connections between suspected terrorists.[35]

This high degree of data collection and information sharing conjures up images of George Orwell, Big Brother, and the ever-eroding sense of privacy and anonymity.[36] Indeed, casinos are powerhouses of information gathering and distribution and use their surveillance activities to police, protect, and profit. The private information does not exist in a vacuum; casinos share it with other casinos and, in some cases, law enforcement. But who protects the consumer in the event that the information is breached or the company is sold or files for bankruptcy? Are there restrictions on the information that casinos may share with law enforcement? This Article argues that the intricate, vast amounts

---

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *See* Ellen Nakashima, *From Casinos to Counterterrorism*, WASH. POST, Oct. 22, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/10/21/AR2007102101522_pf.html.
[30] Harrison, *supra* note 17.
[31] *Id.*
[32] Gruetze, *supra* note 2.
[33] Detroit law enforcement is one example. Santiago Esparza & George Hunter, *Cameras Put Focus on Safety Downtown*, DETROIT NEWS, Aug. 13, 2011, at A1. Detroit Police network with private security cameras, including casinos. *Id.* This network allows the officers to monitor camera images and then use facial recognition to search for felons. *Id.* Likewise, casinos turn to law enforcement to augment their own databases. Gruetze, *supra* note 2.
[34] Kaplan, *supra* note 12.
[35] *Id.*
[36] *See* Harrison, *supra* note 17.

of consumer information compiled through casino structured intelligence ("CSI") require greater protection and oversight in the contexts of both bankruptcy and law enforcement. Section II examines the various types of casino technology and information gathering that casinos perform. Section III considers the available protections of private information in terms of security breaches, law enforcement sharing, and sales in the context of a bankruptcy. Section IV discusses additional safeguards and ethical concerns that should be considered as casinos continue to increase their data mining efforts. Finally, Section V concludes that, minimally, consumers are entitled to more candid disclosures and a meaningful opportunity to protect their own privacy.

II. Casino Technology and Information Gathering

[E]very word you say. Every game you play, every night you stay. I'll be watching you.[37]

Since their inception, casinos have devoted large portions of their budgets to security. With large sums of money exchanging hands, security is a high priority. Consequently, casino heists are few and far between because their vaults are heavily guarded and secured.[38] It is no secret that casinos watch what their customers do.[39] The cameras are unavoidable, and there are signs that warn gamblers "that by entering the casino, they are giving the casino permission to videotape their activities."[40] The surveillance at casinos, however, is much more than a bank of cameras operated in a little room by three guys sitting in front of a pod of television monitors.

Long gone are the days of the menacing pit boss that roamed from table to table hoping to catch a card counter in the act or a dealer on the take. Nonetheless, in the chronology of casino security, the pit boss plays an important role. A pit boss, or "gaming supervisor," is the prominent figurehead associated with the Vegas of old. Typically, a pit boss supervises a particular group of casino dealers running different games simultaneously.[41] The pit boss embodies an expertise with all of the casino games and is primarily charged with making sure that operations run smoothly.[42] This includes observing gamblers, deal-

---

[37] The Police, *Every Breath You Take*, *on* Synchronicity (A&M 1983).

[38] For example, in 2010 there were only ten reported casino robberies in Las Vegas. Jackie Valley, *Bellagio Bandit Gets $1.5 Million in Gambling Chips,* Las Vegas Sun, Dec. 14, 2010, http://www.lasvegassun.com/ news/2010/dec/14/police-robbery-bellagio/. One of the largest and most widely reported involved the theft of approximately $1.5 million in chips. *Id.* Anthony Carleo was arrested shortly after the crime and eventually pleaded guilty. Mike Schultz, *Casino Bandit Anthony Carleo Sentenced to 3-11 Years*, Sports Interaction (Aug. 24, 2011), http://news.sportsinteraction.com/casino/casino-bandit-anthony-carleo-sentenced-to-3-11-years-51413/. Even if Carleo had not been apprehended, tracking technology in the chips would have made it nearly impossible for him to exchange them for anything of value. *Id.*

[39] Kaplan, *supra* note 12 ("Enter a major Las Vegas casino, and you might as well be walking into a complex computer built to study your relationship with money, your motivation for gambling, even your taste in food. Cameras capture your every move . . . .").

[40] Harrison, *supra* note 17.

[41] *Casino Pit Boss Jobs,* Casino Jobs 411, http://www.casinojobs411.com/casino-jobs-pit-boss.html (last visited Mar. 3, 2012).

[42] *Id.*

ers,[43] and perhaps even the associated bystanders that may never place a single bet. In effect, a pit boss continually shuffles a game of human cards to keep the pace moving. Dealers rotate between tables, and players are given drink and food comps—all in an effort to keep the dice rolling and the cards turning.[44]

The pit boss served as both a casino's first line of defense and an ambassador of goodwill; doling out punishments and rewards. The pit boss identified the high rollers and the debt-ridden chronic gamblers.[45] The pit boss also performed accounting tasks: overseeing the bets in play, the chips won and lost, and the cash boxes moving into and out of the casino floor.[46] Perhaps most important, the pit boss kept the peace by handling problem players with the discretion needed to keep any disruption to a minimum.[47] All told, the pit boss was the most visible form of customer service that a casino offered.[48] The advent of technology, however, has dramatically decreased the need for a pit boss to constantly traverse the casino floors.[49]

A. Policing Beyond the Cameras: Bet on the House

"Las [V]egas casinos are incubators of the world's most advanced surveillance tech."[50] The thousands of cameras housed in the ceiling of a casino can pan over more than eighty percent of the room, and some offer full 360-degree views of the floor.[51] "Computer-vision systems" robotically sweep for signs of suspicious activity in the casino, such as people unnecessarily congregating in unusual spaces, unattended bags, cheating players, and dealer errors.[52] Surveillance cameras, however, are primitive compared to the facial recognition technology being utilized by more casinos. One such program, Visual Casino (developed by Biometrica), is one of the leading applications used by casino

---

[43] *See id.*

[44] *See* Anonymous, CASINO CONFIDENTIAL 6, at 169 (2008); *see also* Al Moe, *Casino Pit Boss – What a Pit Boss Does*, ABOUT.COM, http://casinogambling.about.com/od/casinos101/a/Casino-Pit-Boss-Job.htm (last visited Mar. 3, 2012).

[45] *See Casino Pit Boss Jobs*, *supra* note 41.

[46] *Id*.

[47] *Id.*

[48] *See id.*

[49] Liz Benston, *List: Disappearing Las Vegas Casino Jobs*, LAS VEGAS SUN, Jul. 20, 2011, http://www.lasvegassun.com/news/2011/jul/20/list-disappearing-las-vegas-casino-jobs/.

[50] Kaplan, *supra* note 12.

[51] *Id.*

[52] *See, e.g.*, Press Release, Biometrica Sys., Inc., Viisage Technology and Biometrica Systems Achieves 50th Facial Recognition Installation at Mirage Resort, Las Vegas (Mar. 29, 2000), *available at* http://www.gamingfloor.com/pressrel/Press_bio5.htm.

> The Visual Casino product suite additionally includes the Casino Information Network and the Casino Information Database, as well as unique copyright training tools that assist operators in learning to recognize faces stored on a casino's database. The Casino Information Network is the secure, closed-loop; non-Internet network used by surveillance and security departments to exchange timely information and queries about casino suspects. The Casino Information Database, published by CVI, LLC, is the state-of-the-art subscription database of casino undesirables, and comes with updated data and photographs the [sic] are facial recognition ready.

Id.; *see also* Kaplan, *supra* note 12.

surveillance operators to identify cheaters, other "undesirables," and even gambling VIPs.[53]

The Visual Casino application permits casinos to generate an individual database that houses digital pictures, information, and subsequent actions taken.[54] Once a casino obtains a digital image, the picture is processed using facial recognition technology.[55] Return customers can later be identified by comparing surveillance camera footage to images already in the casino database.[56] In a matter of seconds, the person recognized by the system pops up on a screen along with the additional information the casino may have collected on that individual, including the record of wins and losses.[57]

Recent advances in the technology now allow casinos to catalogue their own set of "rap sheets" on known undesirables and scams, including "active professional card counters, slot and table game cheats (along with known associates), exclusion lists, gaming scams and cheating devices."[58] The database updates daily with intelligence collected from the stable of subscribing casinos.[59] In a nod to the rise of mobile technology, Biometrica offers a "mobile database access module" that enables casino security to send photos and data to smartphones or tablets.[60]

While facial recognition software is impressive, a casino's "spy gear" goes far beyond matching up new pictures against old ones.[61] For example, NORA searches for commonalities among phone numbers, addresses, aliases, and other identifiers in order to establish links and patterns that a casino security employee might otherwise miss.[62] The host of technology tools that casinos employ converges toward one overriding goal: protecting and promoting profits. And for casinos, chips are money.

In some casinos, surveillance is more stealth than the cameras in the room. The chips—the currency of casino game tables—house their own tracking devices.[63] Embedded within each chip is a tiny microchip that contains radio frequency identification (RFID) transmitters.[64] RFID technology is also used in law enforcement.[65] While casinos were among the earliest adopters, counterterrorism and Homeland Security agencies have embraced the technology.[66] Pass-

---

[53] The company released the latest version of its popular "Visual Casino" product on November 11, 2011. *See Visual Casino Suite 6*, BIOMETRICA, http://www.biometrica.com/products.html (last visited Mar. 3, 2012).

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *See* Tyler Grady & Kory Felzien, *Privacy and Casinos: What they Know About You*, *in* PRIVACY IN TRANSPARENT WORLDS 48, 53 (2007), *available at* http://www.ethicapublishing.com/7CH6.htm.

[58] *Visual Casino Suite 6*, *supra* note 53.

[59] *Id.*

[60] *Id.*

[61] *See* Kaplan, *supra* note 12.

[62] *Id.* (NORA uncovered a scam between a dealer and a regular customer at the Venetian Resort Hotel Casino.).

[63] Nakashima, *supra* note 29.

[64] *Id.*

[65] *Id.*

[66] *Id.*

ports and EZPasses for toll roads now contain RFID chips as well.[67] The RFID chips permit the casino to track the money being wagered on a specific roulette number or craps roll.[68] RFID-enabled chips may soon be the norm rather than the exception. In addition to tracking cash flow at the tables, they also allow security to detect counterfeit chips.[69]

RFID chips and cameras combine in the TableEye21 technology that utilizes overhead cameras and video analysis software paired with RFID technology.[70] This system swiftly recognizes "advantage" players who can beat the house and cost casinos profits.[71] Advantage players rely on legal strategies, namely, card counting and shuffle tracking, to predict "clumps" of favorable cards. TableEye21 provides a report of the player's skill level, the amount of money a casino can expect to win from that player, and whether there are dealer errors present.[72] Knowing such information about a player not only pads a casino's pockets, but also alerts it to a talented card counter who might go unnoticed for a longer period of time.

In addition to smart tables and chips, other technological advances aid in casino security. Server-based computerized slot machines empower casinos to change games and set odds remotely, and then push games out to each machine from a central command area.[73] When used with a customer loyalty card, the machine can stalk betting patterns and supply the player with a customized game.[74] Incidentally, this same technology is also used in sophisticated cryptography to protect government and corporate secrets with encryption tools.[75] Aside from the in-house technology that identifies players and cheats, "many casinos know who you are before you even walk through the door."[76] Some casinos have high-resolution video cameras that scan the license plates of vehicles as they enter valet and parking areas.[77] Pictures of the license plates are then uploaded into optical character-recognition software that matches a name to a vehicle.[78] If the license plate identifies the driver as a member of the "undesirables" database, that person may be turned away from the casino before he or she even sets foot in the door.[79]

There are limits, however, to customer tolerance of casino surveillance.[80] Several years ago, MindPlay hit the market.[81] The product contained fourteen

---

[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] Kaplan, *supra* note 12.
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.* Casinos also use customer information to tailor ads and promotions to each customer based upon their known interests. *See* Lewinski, *supra* note 9.
[75] Kaplan, *supra* note 12.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *See e.g.*, Joshua Tompkins, *For the Pit Boss, Some Extra Electronic Eyes*, N.Y. TIMES, Mar. 25, 2004, http://www.nytimes.com/2004/03/25/technology/for-the-pit-boss-some-extra-electronic-eyes.html?pagewanted=all&src=pm.
[81] *Id.*

miniscule cameras that monitored the cards that came out of the blackjack shoe.[82] After some rapid-fire analysis of the cards dealt and the likely cards remaining, the system's software notified dealers in real time whether the game was hot or cold—meaning whether the remaining cards favored players or the house.[83] If the odds tipped toward the players, the dealer might conveniently need to shuffle the deck. After MindPlay received some press coverage detailing how the system gives the house a significant and rather unfair advantage, players complained to the Gaming Control Board.[84] By 2010, MindPlay was no longer in use.[85]

B. Big Brother Watching the Big Spender

Surveillance helps casinos prevent losses, thereby increasing their profits. The former utilizes more "traditional," although highly advanced, methods such as cameras and facial recognition software. With more frequency, the latter relies upon recent advances in customer research and data mining.[86] Through expansions in database marketing and tracking, casinos promote loyalty programs through "operationalizing player data in order to target rewards at specific consumer segments."[87] According to a study on complimentary rewards in Las Vegas casinos, these reward programs essentially seek three main goals: (1) attract new patrons, (2) maintain and enhance existing customer relationships, and (3) recover inactive or defecting players.[88] The programs then segregate the customers by their predicted profitability—determined by pooling "demographic, psychographic, or performance data."[89]

To accomplish this, casinos collect volumes of information about the cardholders.[90] At Caesars Palace—part of the Caesars Entertainment Corpora-

---

[82] *Id.* A "shoe" holds multiple decks of cards from which the dealer "pitches" them to the player. ANONYMOUS, *supra* note 44, at 37. Traditionally, blackjack was played with a single deck; the shoe and its many decks were apparently introduced to foil counters. *Id.*

[83] Tompkins, *supra* note 80.

[84] Kaplan, *supra* note 12. The Gaming Control Board (GCB) regulates Nevada's gaming industry, thus providing some oversight and protection of gamblers' rights. *State Gaming Control Board Information Page*, NEV. GAMING COMM'N AND STATE GAMING CONTROL BD. http://gaming.nv.gov/about_board.htm#top (last visited Mar. 3, 2012). Their mission statement is:

> The Nevada Gaming Commission and the State Gaming Control Board govern Nevada's gaming industry through strict regulation of all persons, locations, practices, associations and related activities. We protect the integrity and stability of the industry through our investigative and licensing practices, and we enforce laws and regulations, while holding gaming licensees to high standards. Through these practices, we are able to ensure the proper collection of taxes and fees that are an essential source of revenue for Nevada.

Id.

[85] Kaplan, *supra* note 12.

[86] *See, e.g.*, OLSON & DELEN, *supra* note 20, at 6.

[87] Katharine S. Meczka, Complimentary Rewards in Las Vegas Casinos: A Literature Synthesis and Recommendations for Profitable Complimentary Reward Programs 14 (Aug. 1, 2010), *available at*, http://digitalcommons.library.unlv.edu/cgi/viewcontent.cgi?article=1555&context=thesesdissertations (professional paper selected for publication by the University of Las Vegas.

[88] *Id.*

[89] *Id.* (internal citations omitted).

[90] Nakashima, *supra* note 29.

tion[91]—thousands of people willingly divulge personal information—name, address, birthday—and permit the casino to track their gambling habits in order to win free show tickets and hotel rooms.[92] Since its 1997 birth, more than forty million[93] people have signed up for Caesars Entertainment's Total Rewards loyalty card, and more than ten million remain active users.[94]

In fact, in 2009 alone, the Total Rewards program generated $6.4 billion—roughly eighty percent of the corporation's annual revenue.[95] Total Rewards is an industry darling that represents the "next tier of sophistication" in customer data mining.[96] Caesars Entertainment communicates with its Total Rewards members regularly through 250 million pieces of mail a year.[97] Good customers (i.e., heavy gamblers) may receive up to 150 pieces of mail a year from casino hotels across the Caesars brand.[98] Millions of emails also find their way into customer inboxes each month.[99] In 2009, the Caesars brand had "60,000 slots, 2,000 tables, 40,000 hotel rooms, 390 restaurants, bars and clubs and 240 retail shops" that produced a wealth of consumer data to track.[100] To strike an ominous tone, one casino executive observed, "We know if you like golf . . . chardonnay, down pillows, if you like your room close to the elevator, which properties you visit, what games you play and which offers you redeemed."[101] As the "industry leader in data mining for marketing," Caesars Entertainment softens that big brother attitude by customizing the player's experience.[102] For instance, if a guest inserts the player's card into a slot machine on her birthday, a promotions manager might sneak up with a birthday treat.[103]

The player's card, however, is much more than a birthday card from casino management. The developer of NORA, whose lab is conveniently next to the Vegas Strip, acknowledged that "[e]very time a player registers for a loyalty card or a hotel room . . . the player's name, address and other data are sent to NORA," where it is analyzed with other data in building customer profiles.[104] To that effect, casinos have spawned a "surveillance society."[105]

---

[91] Caesars' parent company operated under the Harrah's Entertainment name until late 2010 when Harrah's changed its corporate name to Caesars Entertainment Corporation. Howard Stutz, *Harrah's to Become Caesars Entertainment*, LAS VEGAS REV.-J., Nov. 5, 2010, http://www.lvrj.com/business/harrah-s-prices-ipo-in—15—17-range-106772163.html; *see also Company Information*, CAESARS ENTM'T, http://www.caesars.com/corporate/index.html (last visited Mar. 3, 2012).

[92] Nakashima, *supra* note 29.

[93] *Id.*

[94] Michael Bush, *Why Harrah's Loyalty Effort is Industry Gold Standard*, ADVER. AGE (Oct. 5, 2009), http://adage.com/article/news/harrah-s-loyalty-program-industry-s-gold-standard/139424/.

[95] *Id.*

[96] *See generally id.*

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] Nakashima, *supra* note 29.

[103] *Id.*

[104] *Id.*

[105] *Id.*

The omnipresent features of casino surveillance have been embraced and borrowed by law enforcement. This proved true in December 2003, when a terror alert popped up on the radar targeting Las Vegas.[106] The Federal Bureau of Investigation (FBI) asked casinos, hotels, rental-car agencies, and airlines for access to their customer data.[107] Some businesses flinched, but others yielded and turned over the data—either voluntarily or in response to a subpoena.[108]

III. Trading In Consumer Data: The House Always Wins

Despite the apparent willingness to freely provide a great deal of information to competitor casinos and law enforcement, much of the gathered information is actually a valuable asset to the casino. A casino in bankruptcy, whether attempting to reorganize or facing liquidation, will probably seek to cash-in on this important commodity. The Bankruptcy Code recognizes the need to capitalize on estate property outside the ordinary course of business. Section 363 governs these types of transactions and permits either a trustee or debtor-in-possession to use, sell, or lease property of the estate, outside the ordinary course of business.[109]

Although 11 U.S.C. § 363(b) gives the debtor considerable freedom in the sale of property, some restrictions apply—especially when the property at issue is customer information.[110] This code section is particularly relevant to casino bankruptcy sales because such sales often involve customer data.[111] The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 ("BAPCPA") created a restriction for cases (filed on or after October 17, 2005) that involve property containing personally identifiable consumer information.[112] Under § 363(b)(1), if the debtor offered consumer products or services subject to a privacy policy still in effect on the petition date, then the trustee or debtor-in-possession's ability to sell the data is limited.[113] The sale must be consistent with the existing policy; otherwise, the Code imposes additional limitations.[114] When the sale does not comport with the privacy policy, selling the information requires: (1) appointment of a consumer privacy ombudsman ("CPO"), (2) subsequent notice and a hearing, and (3) court approval. When determining whether to authorize the transfer, the Code directs the court to "giv[e] due consideration to the facts, circumstances, and conditions of such sale or such lease;

---

106 *Id.*

107 *Id.*

108 *Id.*

109 *See* 11 U.S.C. § 363 (2006).

110 *See id*. § 363(b).

111 *See, e.g.*, *In re* Adamar of N.J., Inc. No. 09-20711, 2009 Bankr. LEXIS 5191 at *41 (Bankr. D.N.J. Nov. 4, 2009) (approving the transfer by the casino debtors of all "personally identifiable information about individual persons to the extent not inconsistent with the Debtors' policy prohibiting the transfer . . . and the Specified Parties, as applicable, shall abide by the Privacy Policy.").

112 *See generally*, Bankruptcy Abuse Prevention and Consumer Protection Act of 2005, Pub. L. No. 109–8, 119 Stat. 23 (2005).

113 11 U.S.C. § 363(b)(1) (2006).

114 *See id.* § 363(b)(1)(B).

and find[ ] that no showing was made that such sale or such lease would violate applicable nonbankruptcy law."[115]

By virtue of the amendment to § 363(b)(1)(B), BAPCPA also added § 332 to the Bankruptcy Code, which provides in pertinent part:

> (a) If a hearing is required under section 363(b)(1)(B), the court shall order the United States trustee to appoint, not later than 7 days before the commencement of the hearing, 1 disinterested person (other than the United States trustee) to serve as the consumer privacy ombudsman in the case and shall require that notice of such hearing be timely given to such ombudsman.
>
> (b) The consumer privacy ombudsman may appear and be heard at such hearing and shall provide to the court information to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale or lease of personally identifiable information under section 363(b)(1)(B). Such information may include presentation of—
>
> (1) the debtor's privacy policy;
>
> (2) the potential losses or gains of privacy to consumers if such sale or such lease is approved by the court;
>
> (3) the potential costs or benefits to consumers if such sale or such lease is approved by the court; and
>
> (4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers.
>
> (c) A consumer privacy ombudsman shall not disclose any personally identifiable information obtained by the ombudsman under this title.[116]

BAPCPA further added a definition for "personally identifiable information" in § 101(41A).[117]

These amendments were not the result of an abundance of caution. Rather, the catalyst appears to be the rapid rise and failure of dot-com companies. In *In re Toysmart.com, L.L.C.*, the Federal Trade Commission (FTC) sued a bankrupt online toy retailer that sought to auction the personal information it had collected from its customers.[118] The FTC alleged that the sharing of personal information in connection with an offer for sale constituted a deceptive practice because the company had represented in its privacy policy that such information would never be shared with third parties.[119]

Specifically, the FTC alleged that the sale ran afoul of the assurances Toysmart.com had made in its privacy notice resulting in deceptive trade prac-

---

[115] *Id.*

[116] *Id.* § 332.

[117] 11 U.S.C. § 101(41A) defines "personally identifiable information" as the person's name, address, email address, telephone number, the person's social security number (or another account number), a credit card number, birthday, as well as "any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically." *Id.* § 101(41A)(A)-(B).

[118] Order, *In re* Toysmart.com, L.L.C., No. 00-13995 (Bankr. D. Mass. July 26, 2000) (No. 156); Order, *In re* Toysmart.com, L.L.C., No. 00-13995 (Bankr. D. Mass. Jan. 25, 2001) (No. 325); *see also* Lisa J. Sotto et al., *Emerging Privacy Issues in Bankruptcy*, GC N. Y. (June 10, 2010), *available at* http://www.hunton.com/lisa_sotto/?op=publications&ajax=no.

[119] Order, *In re* Toysmart.com, L.L.C., No. 00-13995 (Bankr. D. Mass. July 26, 2000) (No. 156); Order, *In re* Toysmart.com, L.L.C., No. 00-13995 (Bankr. D. Mass. Jan. 25, 2001) (No. 325); Sotto et al., *supra* note 118.

tice that violated §5 of the FTC Act.[120] Toysmart.com later reached a settlement with the FTC to allow the sale, but the attorneys general of more than forty states objected to the settlement.[121] The unyielding opposition led Toysmart.com to eventually withdraw the customer lists from the auction and destroy the information.[122] Given the amount of data that consumers began to share with retail and financial companies, Congress passed the consumer privacy amendments to the Bankruptcy Code in order to "prevent future cases like Toysmart.com."[123]

Regarding the qualifications for appointing a consumer privacy ombudsman, § 332 seems to require only that the ombudsman be disinterested.[124] Nothing more is statutorily required. That aside, it seems only logical that the court would prefer a candidate with a robust background in consumer privacy law. Privacy practices and policies can be intricate affairs; one can only assume the court would prefer the United States trustee to select an ombudsman with, at a minimum, experience and knowledge in privacy matters. Ideally, the appointed ombudsman would have familiarity specific to the debtor's business and industry practices related to privacy. Nonetheless, beyond the disinterestedness requirement, the United States trustee retains the discretion to appoint any person it deems fit to serve as the ombudsman.[125] Section 332 does not require the court to endorse the appointment.[126]

Consequently, the CPO, similar to an examiner, functions much like an independent officer of the court.[127] Indeed, the statute specifically requires that the ombudsman be a disinterested person. This independence is evidenced by the fact that the CPO has no client, and parties in interest do not direct the ombudsman's inquiries or actions.[128] Moreover, the ombudsman does not serve at the pleasure of the court or the United States trustee.[129] The ombudsman is, however, subject to court orders, and the related fees are subject to court approval and trustee objections.[130] This scant oversight provides the lone check on the ombudsman's otherwise apparent omnipotence. The absence of other statutory directives means the ombudsman is effectively an independent functionary in the bankruptcy case. Based on the language of §§ 330, 332, and 363(b)(1)(B), which describe the title, compensation, and duties of the ombudsman, the primary purpose of an ombudsman is to protect the private

---

120 F.T.C. v. Toysmart.com, L.L.C., No. 00-11341-RGS, 2000 WL 34016434, at *1 (D. Mass. July 21, 2000).

121 *See* F.T.C. v. Toysmart.com, L.L.C., No. 00-CV11341RGS, 2000 WL1523287, at *1 (D. Mass. Aug. 21, 2000) (denying Texas's motion to intervene in part because more than forty states also requested permission to intervene).

122 Justine Young Gottshall, *Privacy Issues Tangle the Web*, THE INDUS. PHYSICIST, June/July 2001, at 30.

123 151 Cong. Rec. S1781 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

124 11 U.S.C. § 332(a) (2006).

125 *See id.*

126 *Id.*

127 *See id.* § 1104(c) (permitting the bankruptcy court to appoint a trustee at the request of either the trustee or a party in interest).

128 *See id.* § 332.

129 *See id.*

130 *Id.* § 330(a).

and personally identifiable information that consumers provide when doing business with the debtor.[131]

Despite the gravity and importance of this task, given the Code's terseness, the sentiment surrounding the CPO's recommendations seems to be either permissive cooperation or tacit disregard. At least, that is the sentiment where an ombudsman is even appointed. Appointment seems to be a spotty practice. With the enormous dragnets of consumer data employed by casinos, those businesses seem an obvious fit for regulation of the transfer of consumer information. Yet, casino bankruptcies often fail to utilize a CPO. In the recent Chapter 11 reorganization of Station Casinos, the bankruptcy court authorized the sale of "primary customer data."[132] The buyer was given exclusive rights over the information.[133] The bidding agreement contained no mention of supervision or concern about the customers' privacy.[134] Indeed, the only restriction placed on the bidding order was the exclusion of the debtor from post-sale use of such information.[135]

Similarly, Adamar of New Jersey, Inc., operator of the popular Tropicana Casino and Resort in Atlantic City, went through Chapter 11 reorganization in 2009.[136] Not surprisingly, Adamar also sold customer data in the restructuring attempt.[137] Although a CPO was not appointed, the bankruptcy court did make specific reference to the existing privacy policy.[138] Presumably, Adamar's sale complied with the first provision of § 363.[139] One cannot help but query, however, how the transfer and sale of customer data to a third party does not necessarily violate the existing policy. The lack of any meaningful oversight in either of these cases is disheartening, to say the least, given the vast amounts of intricate data collected and cataloged by casinos. At minimum, a CPO should be appointed to attempt to ensure that transferees respect and protect the rights of consumers.[140]

---

131 *See generally*, *id.* §§ 330, 332, 363(b)(1)(B).

132 *In re* Station Casinos, Inc. No. BK-09-524477, 2010 Bankr. LEXIS 5673, at *17-18 (D. Nev. June 4, 2010).

133 *Id.* at *18.

134 *See id.*

135 *See id.*

136 *See In re* Adamar of N.J., Inc. No. 09-20711, 2009 Bankr. LEXIS 5191 at *41 (Bankr. D.N.J. Nov. 4, 2009).

137 *Id.*

138 *Id.* (making no reference to a CPO, approving the transfer by the casino debtors of all "personally identifiable information about individual persons to the extent not inconsistent with the Debtors' policy prohibiting the transfer . . . and the Specified Parties, as applicable, shall abide by the Privacy Policy.").

139 11 U.S.C. § 363(b)(1)(A) (2006).

140 Granted, these reorganizations often involve transfers to related corporate entities. *See, e.g.*, Chris Sieroty, *Station Casinos Emerges from Bankruptcy*, LAS VEGAS REV.-J., June 17, 2011, http://www.lvrj.com/business/station-casinos-emerges-from-bankruptcy-124086429.html (noting that founders of Station Casinos, the Fertitta family, will maintain a forty-five percent ownership interest post-restructuring). Thus, it is possible that in some instances customer data only nominally change owners. Despite this possibility, with the tremendous amounts of data involved it seems foolhardy to simply assume, or hope, that the restructuring does not involve breaches of consumer security. The minor administrative cost of requiring a CPO arguably far outweighs the potentially huge cost to consumers should their privacy be jeopardized.

Probably due to the anger following Toysmart.com's bankruptcy, retail is the one area where an ombudsman is appointed with some regularity. Unlike the aforementioned casino bankruptcies, the bankruptcies of lesser-known retailers often include an ombudsman. Bereft retailers as varied as BI-LO, L.L.C. (a grocery chain),[141] S & K Famous Brands, Inc. (an online purveyor of men's clothing),[142] and Michael Anthony Management (online retailer and message board owner)[143] all had CPOs to make recommendations regarding customer data in their bankruptcies. It seems almost comical that BI-LO's bankruptcy merited oversight, while Station Casinos did not. As valuable as a customer's toilet paper and yogurt preferences may be, casinos are at the head of the pack in data mining. Consequently, their customers' information deserves at least the protections afforded to shield one's shirt size or dog food preference.

Sadly (perhaps as a result of the Code's apparent ambivalence towards a CPO), the effect of appointing an ombudsman can vary dramatically. Chrysler and Borders provide two contrasting examples of the ways in which the appointment can have vastly different outcomes. In *In re Chrysler, L.L.C.*, the debtor sought bankruptcy court approval "to sell substantially all of its assets to a Fiat S.p.A. affiliate."[144] The company proposed the sale of large amounts of consumers' personal information. In addition to consumers' names, mailing addresses, email addresses, and telephone numbers, the sale was also to include financial information consumers provided on various Chrysler websites and through Chrysler's independent dealers. Chrysler's privacy notice promised consumers that the information would not be distributed or sold to anyone other than affiliated entities. As a result of the existing privacy policy, the bankruptcy court appointed a consumer privacy ombudsman under 11 U.S.C. § 332.[145] The ombudsman was to examine and provide recommendations on the proposed sale of Chrysler customers' personal information.[146]

The Chrysler CPO recommended court approval only if the sale was subject to substantial restrictions. Specifically, the ombudsman recommended that: (1) Chrysler sell the information to a buyer operating a similar business, (2) the buyer agree to adopt and comply with the Chrysler's privacy notice, (3) Chrysler and the buyer deliver the notice of the proposed sale to consumers whose personally identifiable information was subject to the sale, and (4) Chrysler and the purchaser give consumers an opportunity to opt out of the transfer of the information to the purchaser. Finally, the ombudsman recom-

---

[141] *In re* BI-LO, L.L.C., No. 09-02140 (HB), 2010 Bankr. LEXIS 4628, at *1 (Bankr. D. S.C. Aug. 5, 2010) (approving the CPO's fees).

[142] *In re* S & K Famous Brands, Inc., No. 09-30805 (KRH), 2009 Bankr. LEXIS 5374, at *1-2, *41; (Bankr. E.D. Va. Dec. 4, 2009) (approving the sale of customer data, and authorizing the U.S. Trustee to appoint a CPO to oversee the sale of customer data such as phone, email, home address, and order history during bidding process for a bankrupt online retailer).

[143] *In re* Michael Anthony Mgmt., No. 10-55755, 2010 Bankr. LEXIS 6189, at *6 (Bankr. N.D. Cal. Sept. 29, 2010). In the case of Michael Anthony Management, a CPO was appointed *and* the buyer agreed to abide by the existing privacy policies. *See id.*

[144] *In re* Chrysler L.L.C., et al., No. 09-50002 (AJG) (Bankr. S.D.N.Y. Apr. 30, 2009); *see also* Sotto et al., *supra* note 118.

[145] *In re* Chrysler L.L.C., et al., No. 09-50002 (AJG) (Bankr. S.D.N.Y. Aprl 30, 2009).

[146] Sotto et al., *supra* note 118.

mended that the bankruptcy court order the destruction of any financial information collected from consumers, such as Social Security and bank account numbers.[147] Chrysler seemed to accept these conditions.[148]

On the other hand, in the recent bankruptcy of Borders, Barnes & Noble (purchaser of Border's customer records) drew ire from the privacy ombudsman by failing to adhere to his recommendations.[149] Michael St. Patrick Baxter was selected to oversee the transfer of consumer data, including purchasing records and contact information.[150] Baxter originally imposed customer consent as a condition to transfer of the consumer information.[151] Barnes & Noble balked, wanting unfettered use of the data of nearly fifty million consumers.[152] Baxter agreed to a compromise.[153] The personal information could be sold absent consent, but customers were to receive full disclosure of the transfer and their ability to opt-out.[154] Following this concession, Barnes & Noble purchased the information from the now defunct Borders bookseller for nearly $14 million.[155] In light of Baxter's recommendations, the bankruptcy court ordered Barnes & Noble to inform former Borders customers of the opportunity to opt-out of the impending transfer of their personal information.[156] Baxter was provided a scant two hours in which to review the court-ordered message.[157] Executives sent out the court-mandated email, but virtually ignored all of Baxter's substantive changes.[158] The final version limited Baxter's input to a single word and his suggested subject line.[159] It bears asking, what is the purpose of appointing privacy overseers if their recommendations are allowed to go practically unheeded?

IV. Bubble Wrap for Data Mining and Surveillance

In the abstract, many people express discomfort with the Orwellian notion of clandestine cameras constantly monitoring our daily lives. We recoil when news headlines broadcast the horrors of network security breaches and Nigerian bank account scams. At the same time, however, we voluntarily (and almost unconsciously) provide our personal information to a variety of business enter-

147 *Id.*

148 *See* Order (I) Authorizing the Sale of Substantially all of the Debtor's Assets Free and Clear of all Liens, Claims, Interests, and Encumbrances, (II) Authorizing the Assumption and Assignment of Certain Executory Contracts and Unexpired Leases in Connection Therewith and Related Procedures and (III) Granting Related Relief at 23-24 *In re* Chrysler L.L.C., et al., No. 09-50002 (AJG) (Bankr. S.D.N.Y. Apr. 30, 2009).

149 *See* Katy Stech, *Barnes & Noble Email to Borders Customers Rattles Privacy Watchdog*, Wall Street J., Oct. 4, 2011, http://blogs.wsj.com/bankruptcy/2011/10/04/barnes-noble-email-to-border-customers-rattles-privacy-watchdog/.

150 *Id.*

151 *Id.*

152 *Id.*

153 *Id.*

154 *Id.*

155 *Id.*

156 *Id.*

157 *Id.*

158 *Id.*

159 *Id.*

prises vis-à-vis loyalty programs. Consider the amount of cards dangling from key rings that we scan weekly or monthly: grocery stores, pharmacies, pet stores, and, of course, casinos. The ease of access afforded by signing into websites through Facebook or LinkedIn usually comes with the proviso that users' information will be provided by simply clicking an "allow" link.[160] The bankruptcy provision related to the protection of personal information is an important one in the larger debate over the use, sale, distribution, and protection of private data. Consider that in 2002, the amount of data stored on computers on a global scale amounted to five exabytes, equivalent to five billion gigabytes.[161] Just seven years later, in 2009, the data soared to 988 exabytes—the distance to Pluto and back if all of that data were printed out and stacked in a pile.[162]

Thus, in that morass of data, there needs to be a meaningful attempt not only to address the collection and use of personal data, but also to educate consumers about just what sort of information they are freely giving away. It is doubtful that many of the millions of customers who belong to Caesars Entertainment's Total Rewards have taken the time to peruse the privacy policy. In pertinent part, the policy explains that upon visiting its website, Caesars Entertainment automatically tracks and collects: "(i) IP address, (ii) domain server, (iii) type of computer, and (iv) type of Web browser."[163] Caesars acknowledges that this information is anonymous and is used for marketing purposes and website improvement.[164] The privacy policy further details that Caesars may "collect and use Customer information we believe is necessary to administer our business and provide you with the most personalized service and experience."[165] That necessary information includes data received when a customer books a reservation, registers for email notifications, enters an online promotion, requests information, submits an employment application, or fills out a feedback survey.[166] The particular data goes beyond a customer's name and Total Rewards number to include birth dates, addresses, email addresses, phone numbers, credit card numbers, and even social security numbers (the latter for employment applications).[167]

While the type of information collected appears typical and almost routine in the grand context of the data collection in the marketplace, the more significant piece of the privacy policy is the sharing of information with affiliated and third-party entities. In addition to sharing such information (in predictable fashion) with its other casinos under the Caesars Entertainment brand, the information is also shared with "credit bureaus, collection agencies, and other non-

---

[160] *See Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/legal/terms (last updated Apr. 26, 2011).
[161] Stephen J. Rancourt, *Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information*, 18 TEX. WESLEYAN L. REV. 183, 184 (2011).
[162] *Id.*
[163] *Privacy*, CAESARS ENTM'T, http://www.totalrewards.com/privacy.html#top (last updated Jan. 6, 2011).
[164] *Id.*
[165] *Id.*
[166] *Id.*
[167] *Id.*

affiliated third parties only as permitted by law."[168] Caesars also notes that it shares "certain limited information" about its customers with other businesses, including the likes of financial services companies, insurance companies, airlines, car rental agencies, and retailers.[169] Other casino loyalty programs have similar privacy provisions.[170]

The amount of data mining and surveillance that occurs in casinos is astounding. The two combined effectively turn casino security teams into a collection of mini law enforcement agencies, except they have better technology and perhaps even better pay. Through the tiny window of supervision that bankruptcy law provides in this context, it can be seen that the protection of personal information trumps business judgment and the maximization of profit. Section 363(b)(1) expressly contains a significant exception to a debtor's largely unrestricted ability to use or sell property at its discretion.[171] The State of Nevada's own laws further reflect the sanctity of personal data.

Perhaps as a response to the amount of data that casinos collect and the potential for abuse and theft, Nevada passed strict security measures for the protection of private information. The Security of Personal Information Law of 2008 was a groundbreaking piece of legislation that became the first such law in the United States to require the encryption of personal data.[172] The law mandates that all data collectors—including casinos—must encrypt personal information.[173] This encryption requirement is a unique one among the states.[174] Importantly, it cannot be just any encryption mechanism. Rather, it must be one that has been adopted by an established standards setting body such as the National Institute of Standards and Technology's Federal Information Processing Standards that codes data into indecipherable sequences that require the proper cryptographic key to unlock the data.[175]

While it seems there is an overarching interest in protecting customer data, that same instinct does not appear to apply to the use of advanced surveillance technology. Moreover, as casinos continue to be on the forefront of technology that is later adopted by law enforcement, there seems to be little concern in the swell in "monitorization" across all facets of business and law enforcement: web use is tracked, vehicles have stealth GPS devices, and our telephones track our moves.[176] Consequently, the law cringes at the notion of customer data collection, but it seems reticent to call "monitorization" into question. As technology advances, this could become a larger problem in just the next few years because consumer data collection has far outpaced the laws meant to protect against the wrongful dissemination of that information.

---

168 *Id.*
169 *Id.*
170 *See Privacy Policy*, MGM RESORTS INT'L, www.mgmresorts.com/privacy.htm (last updated July 1, 2011) *and Privacy Policy*, WYNN, http://www.wynnlasvegas.com/contact-us/privacy-policy.aspx (last visited Mar. 3, 2012).
171 11 U.S.C. §363(b)(1) (2006).
172 NEV. REV. STAT. § 603A.215(a) (2009).
173 *Id.*
174 *See* Rancourt, *supra* note 161, at 213.
175 NEV. REV. STAT. § 603A.215(5)(b)(1) (2009).
176 *See* Lori Andrews, *Is Your Cell Phone Listening in on You?* TIME MAG. (Dec. 15, 2011), http://ideas.time.com/2011/12/15/is-your-cell-phone-listening-in-on-you/.

V. Conclusion

The digital resources of casinos encompass both data mining and surveillance. The former is often the product of a voluntary, if uninformed, consumer relationship with the casino. The latter, on the other hand, is the product of taciturn acceptance of the nature of the business. While there are provisions that require casinos to manage customer information responsibly, that does not necessarily apply to the surveillance angle of a casino's business. Whether it is unfairly tilting the odds toward the house or facilitating the free flow of information between casinos and law enforcement, there should be basic legal devices that (at the very least) promote the responsible and transparent use and sharing of technology and the information that it yields. While this is somewhat a question of privacy, it is also one of basic human relationships and the transition to more digitized personal interactions.