PATRON DATA PRIVACY AND SECURITY IN THE CASINO INDUSTRY: A CASE FOR A U.S. DATA PRIVACY STATUTE

*Chandeni K. Gill**

INTRODUCTION

An excited man by the name of Joe eagerly awaits his plane's arrival to Las Vegas, Nevada, arguably, the gambling and adult entertainment capital of the world. Once the plane arrives, Joe is reunited with his long-time friends and heads straight to the famed Las Vegas Strip to gamble, eat, drink, and be merry. Joe finds himself at a blackjack table and is asked by the dealer if he has a player's card. Joe tells him, "No," and the dealer informs him that he may receive comps[1] based on his play and other promotional offers if he signs up at the nearby booth. Joe heads to the booth and signs up for a player's card. The booth representative asks for his driver's license and sets up his account. He is provided an embossed player's card with his name and player's card account number.

What information has Joe provided the casino? He presented his state-issued driver's license, and casinos commonly associate a player's card account with the following information: name, date of birth, home address, email address,[2] gender, driver's license number, the driver's license issuance and expiration date, and if provided on the patron's form of identification, his Social Security number.[3] However, the amount of Joe's personal information collected does not stop there. When Joe sits back down to play blackjack, the amount he wagers and how long he plays is tracked and recorded through his newly established player's card account.

---

* J.D. Candidate, May 2012, William S. Boyd School of Law, University of Nevada Las Vegas. I wish to acknowledge the assistance I received in developing this Note topic from the Corporate Internal Audit management team at Caesars Entertainment, and the invaluable resources provided to me by the Caesars Legal department. I would like to thank the members of the *UNLV Gaming Law Journal* editorial staff for their efforts in editing and revising this Note. Last, I would like to thank my friends and family members who have supported me throughout my academic endeavors. Most importantly, I would like to thank my best friend, love, and fiancé, Brandon C. Sendall.

[1] A comp is also known as a complimentary and signifies something given without charge.

[2] ROBERT L. SHOOK, JACKPOT! HARRAH'S WINNING SECRETS FOR CUSTOMER LOYALTY 228 (2003); Interview with Mike Effner, Information Technology Director, Western Division, Caesars Entertainment Corp., in Las Vegas, Nev. (Oct. 6, 2010) [hereinafter Effner Interview].

[3] Effner Interview, *supra* note 2.

Any additional information the casino obtains about Joe will also be linked to his player's card account; for example, if Joe requests a credit line through the casino, decides to play the slot machines, dines at one of the casino's restaurants, or occupies a room in the casino's hotel, all of the information will be tracked through his player's card.[4] Thus, by the time Joe is ready to depart Las Vegas and head home, enough information will be compiled on him to build a detailed profile of his gambling habits, a plan to incentivize his return, and an individual profit-and-loss projection by which the casino may gauge its future marketing investment in Joe.

Player tracking by casinos allows a value to be placed on a customer by forecasting repeat sales earned by the casino based on the assumption the customer will be loyal and continue gambling at the casino in the future.[5] Thus, casino marketing personnel use the data on Joe to make personalized marketing decisions on providing Joe comps and deciding what type of offers Joe will most favorably respond to based on his tracked gaming and non-gaming behavior.

Joe is not the only guest to receive such specialized attention. More than one in ten Americans holds a casino player's card.[6] Because of the large number of individuals using these player's cards and the vast amount of personal information possessed by casinos regarding these patrons, one might be concerned about the risks associated with these types of player tracking systems. What are the risks associated with obtaining, tracking, and maintaining such a large amount of data on millions of casino patrons? This Note will discuss the risks and potential costs to a casino and its patrons if personal information stored on a player tracking system is hacked and used by an unauthorized user to the detriment of casino patrons.

The development of information privacy law is significantly influenced by the progression of technology.[7] Over the years, information privacy has become known as one of the prevailing issues of our time.[8] In the United States today, there are hundreds of laws regarding privacy: "the common law torts, criminal law, evidentiary privileges, constitutional law, at least twenty federal statutes, and numerous state statutory laws across the fifty states."[9] Many times the development of new technology leads to more laws intended to address the increased risks associated with the collection, dissemination, and use of personal information.[10] In the casino industry, the current need for U.S. federal legislation regarding casino patron data security has arisen as breaches in security and the risk of exposure to information that personally identifies individuals have increased.[11]

---

[4] *Id.*; SHOOK, *supra* note 2, at 228-29.
[5] SHOOK, *supra* note 2, at 227.
[6] *Missouri . . . Be Aware*, CASINO WATCH, http://casinowatch.org/harrahs_patents/harrahs_patents_1.html, (last visited Oct. 9, 2011).
[7] Christopher Wolf, *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, 16827 P.L.I. CORP. & SEC. LAW LIBRARY, 1-3 (August 2008).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *See* Industry Notice from Randall E. Sayre, Member, Nev. Gaming Control Bd., to All Non-restricted Licensees Who Maintain Personal And/Or Financial Information of Patrons

The availability of personal data has increased dramatically with the ever-growing dominance of Internet and technology-fueled activities since the mid-1990s.[12] Due to improvements in technology and decreasing costs of processing and storage, data are exchanged without ever providing notice or transparency about the handling and storage of such information to those individuals whose personal data are involved.[13] Moreover, those entities that aggregate and maintain personal information in databases enjoy limited responsibility and accountability to individual patrons because of limited procedural protections.[14] Very few Americans realize that everyday commercial transactions disperse their personal information into the stream of commerce; including transactions such as purchases, subscriptions, and loyalty program memberships.[15] Even fewer Americans realize that once this data is stored, it exists forever.[16]

This Note will discuss the recent surge in patron data collected by casino player tracking systems and the increasing need to protect the confidentiality and security of patron Personally Identifiable Information (PII) through the implementation of federal privacy legislation. Part I discusses the rise of the casino player tracking database systems. Part II explains and defines PII. Part III outlines current U.S. privacy laws applicable to the casino industry, describes casino liability standards, and examines patron remedies for a potential breach in the security of patron PII. Part IV assesses the strengths and weaknesses of U.S. privacy laws applicable to the casino industry, compares those laws to European and Canadian data security laws, and describes how the application of international privacy law in the U.S. will improve the current casino industry data security laws. Finally, Part V suggests that the current industry-based U.S. privacy laws are ineffective, and a nationwide standard, as exemplified in European and Canadian privacy law, should be implemented in the U.S. to ensure appropriate patron PII data security in the U.S. casino industry.

I. The Rise of Casino Player Tracking - Patron Database Systems

The modern day era of database-driven information systems began in the 1970s.[17] In his 1971 book, *The Assault on Privacy*, Arthur R. Miller advised, "[T]he new information technologies seem to have given birth to a new social virus–'data-mania' . . . [and] . . . we must begin to realize what it means to live in a society that treats information as an economically desirable commodity and a source of power."[18] Technology's fast pace evolution has driven the creation

in a Computerized Database and Interested Persons, (Dec. 15, 2010) [hereinafter Industry Notice], *available at* http://gaming.nv.gov/documents/pdf/industry_ltr_252.pdf.

[12] Candice L. Kline, Comment, *Security Theater and Database-Driven Information Markets: A Case for an Ominbus U.S. Data Privacy Statute*, 39 U. Tol. L. Rev. 443, 448 (2007).

[13] *Id.* at 448-49.

[14] *Id.* at 449.

[15] *Id.*

[16] *Id.*

[17] *Id.* at 447.

[18] *Id.*

of the information systems.[19] Technology has allowed credit card companies and retailers to track personal data on most Americans to profile spending characteristics;[20] the casino industry is no different.

The future success and growth of casinos relies on those in the industry who embrace and encourage cutting-edge technology to improve customer service. Consequently, a sweeping new database industry emerged with the improved ability of casino corporations to develop sophisticated databases that capture, organize, and analyze growing amounts of individual personal data.[21] As computer technology continues to develop, the sophistication of casino loyalty programs also continue to grow.[22] Toward the late 1990s, casino corporations learned to link and share patron wagering data among multiple "sister properties" using a single patron loyalty program account.[23] By doing so, the technologically advanced system allowed casino patrons gambling at various properties owned by one casino corporation to accumulate all earned rewards on a single loyalty card.[24]

Innovation and precision in both tactical and strategic measures have become more sophisticated, allowing offers to be closely tailored to customer preferences.[25] Casinos no longer capture information simply for casino marketing purposes; rather, the information is captured for eventual use by all of a casino's employees, enabling them to perform their jobs more effectively.[26] However, access to customer data should generally be limited based on an employee's position and relative need for customer information.[27] The following section discusses the technological development and current use of casino player tracking database systems in the casino industry.

A. Harrah's Entertainment[28]: Total Rewards Player Tracking Program

In the late 1990s, technology and innovative marketing strategies rapidly changed how Harrah's Entertainment operated its casinos.[29] Harrah's began its Total Gold program in 1997.[30] The program was operated by a computerized database system, which recorded patron gambling activity and offered rewards to patrons based on their level of play at all Harrah's casino gaming locations.[31]

---

[19] *Id.*
[20] *Id.*
[21] Kline, *supra* note 12, at 447.
[22] Edward McKinley, *Betting on Better Customer Information*, CREDIT CARD MGMT., Apr. 2005, at 46, 46 (the big resort-casino chains have stacked the odds in their favor by using loyalty club cards to record every chip wagered at the gaming tables and every coin fed into the slot machines).
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Harrah's Entertainment, Inc. changed its official company name to Caesars Entertainment Corporation in November 2010.
[29] Dianne Avery & Marion Crain, *Branded: Corporate Image, Sexual Stereotyping, and the New Face of Capitalism*, 14 DUKE J. GENDER L. & POL'Y 15, 70 (2007) (explaining the history behind the Harrah's Entertainment patron loyalty program).
[30] *Id.*
[31] *Id.*

When Gary Loveman joined Harrah's in 1998 as its chief operating officer, the Harrah's system of tracking and rewarding patrons elevated to a new level of sophistication.[32] Loveman remodeled the Total Gold program from "a customer-recognition rewards program" to the "Total Rewards" program, which he described as "a loyalty program" that created "loyalty incentives" for customers to conduct a significant amount of their gaming at Harrah's properties.[33]

As the number of casinos under Harrah's ownership and management continued to grow, and the number of patrons rose, Loveman felt that in order to compete effectively in the gaming industry, it was important for Harrah's to reexamine its comping procedures.[34] With this in mind, the Total Rewards program began collecting the following information about each patron: age, gender, home address, gaming habits and history, and their consumption preferences-for restaurants, hotel accommodations, spa treatments, golf, and other such amenities.[35] In doing so, control over patron information was provided at the corporate level and taken away from employees.[36] This approach to comping patrons permitted Harrah's to provide individualized incentives and rewards to customers at all levels of play and at all affiliated properties.[37]

The reward points that casino patrons earn through their gaming and nongaming activity may be used for complimentary food, rooms, and entertainment at any Harrah's affiliated property.[38] These complimentary reward points are available to gamblers at all levels of wagering, not simply the high rollers, as was customarily granted by the casino.[39] In 2001, more than half of the revenue earned by Harrah's Las Vegas came from patrons participating in the Total Rewards program.[40] The CEO and President of Harrah's Entertainment, Gary Loveman, stated in an interview in 2003:

> We . . . collect a tremendous amount of information on what players do with us. We know when you arrive at a casino, what you do there, and when you leave. We have information on 26 million customers. And we measure everything . . . . We have the capacity to know rather than guess at something because we collect so much information about our customers.[41]

Harrah's has been enormously successful in its marketing and operating strategies. The Harrah's customer database grew from 5.3 million customers in 1995, to 23 million patrons in 2000, and 26.6 million patrons in 2002.[42] The year-end 2009 figures released by Harrah's Entertainment boasted more than

---

[32] *Id.* at 71.

[33] *Id.* at 72.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.* at 73.

[38] Richard McGowan & Timothy Brown, *Revenue Generation at Casino Resorts: The Use of "Comp-Based" Promotions*, 13 GAMING L. REV. & ECON. 363, 365 (2009).

[39] *Id.*

[40] *Id.* (citing Mike Beirne, *Dollars in the Desert*, BRANDWEEK, Apr. 1, 2002, at 19-20).

[41] Avery & Crain, *supra* note 29, at 74 (quoting Interview by David O. Becker with Gary Loveman, CEO, Harrah's Entm't, Inc.).

[42] *Id.* at 72.

40 million Total Rewards members in the loyalty program.[43] Additionally, in 2010, 74% of total gaming revenues and 58% of cross-market play[44] came from tracked play[45] in the twenty-eight Harrah's-owned casinos throughout twelve states.[46] The corporation's investment in its patented Total Rewards program has given it a significant competitive advantage in the gaming industry.[47] However, as the years passed from its initial implementation, other casinos have taken advantage of integrating similar multi-property player tracking systems to collect, track, and retain data on casino patrons.

B. MGM Resorts International: M life Players Club

In 2002, MGM Resorts International consolidated seventeen property-based loyalty programs by consolidating sixteen databases into a single entity called "The Players Club."[48] Before 2002, however, each MGM-owned casino offered two or three separate patron loyalty programs, conceivably one with points for slot-machine play, another for complimentary plays on table games, and a third with perks for high rollers.[49] Each of MGM's prior Players Club patron accounts built loyalty to one casino, however, none encouraged loyalty to the MGM brand universally because points accumulated at one casino property did not transfer to another.[50]

Consequently, MGM created a centralized MGM Players Club.[51] With the integration and centralization of MGM's initial property-based player's club accounts in 2002, a gambler could earn points or comps at Bellagio and present his or her player's club card at Luxor.[52] The company-wide information would pop up on a computer screen at Luxor, and the staff would recognize the patron's spending at a sister property and respond accordingly by offering rewards and providing increased hospitality service.[53] In April 2002, the MGM Player's Club patron database included more than 20 million names.[54]

More recently, MGM Resorts International has re-launched its Players Club loyalty program as M life Players Club.[55] The revamped program uses technology that is more refined and allows M life Players Club members to

---

[43] Caesars Entm't, *Investor Presentation*, Mar. 25, 2011, at 8, *available at* http://media.corporate-ir.net/Media_Files/IROL/84/84772/Caesars_Investor_Presentation.pdf.

[44] Cross-market play signifies a casino patron's gaming activities in sister properties across varying regional casino markets.

[45] Caesars Entm't, *supra* note 43, at 9.

[46] McKinley, *supra* note 22.

[47] Avery & Crain, *supra* note 29, at 76.

[48] McKinley, *supra* note 22.

[49] *Id.*

[50] *Id.*

[51] *See* Missouri . . . Be Aware, *supra* note 6 (citing Joe Weinert, *Casinos Urged to Embrace Technology*, THE PRESS OF ATLANTIC CITY, Nov 15, 2002).

[52] McKinley, *supra* note 22.

[53] *Id.* at 46-48.

[54] *Missouri . . . Be Aware*, *supra* note 6 (citing Joe Weinert, *Casinos Urged to Embrace Technology*, THE PRESS OF ATLANTIC CITY, Nov. 15, 2002).

[55] Amanda Finnegan, *MGM Resorts Launches M Life Rewards Program, Will Track Non-gaming Spending*, LAS VEGAS SUN, Jan. 11, 2011, *available at* http://www.lasvegassun.com/news/2011/jan/11/mgm-resorts-launches-m-life-rewards-program-will-t/.

customize their engagement with the program.[56] The program provides incentives to its players by utilizing a tiered system that rewards players with greater benefits the more they gamble and engage with the company's brands.[57] The M life rewards program launched in January 2011, but currently only tracks customer spending on the casino floor.[58] However, the company looks to begin the tracking of non-gaming patron expenditures by late 2011.[59]

C. Other Casino Player Tracking Database Systems

Other casinos have also implemented some form of a patron database system, including Sands Corporation, Boyd Gaming Corporation, Station Casinos, and Herbst Gaming.[60] On June 28, 2010, Boyd Gaming Corporation launched a nationwide, multi-property player loyalty program under the brand "B Connected."[61] The single brand provides more consistent rules and greater ease of use, which enables patrons to earn benefits as the program integrates a patron's accumulated points from all Boyd Gaming affiliated casino properties.[62] In April 1999, Station Casinos initiated its patron loyalty "Boarding Pass" program, which merges and links patron information for all eight Las Vegas-based Station Casinos properties on one Boarding Pass player's card account.[63] Thus, a patron may earn and spend Boarding Pass reward points at any of the Station Casinos properties.[64]

The varying casino patron loyalty programs are all based fundamentally on the same source of information: patron PII data. The information collected by casinos on patrons consists of the patron's name, gender, date of birth, home address, email address, driver's license or passport information, gaming and (at some casinos) non-gaming activity.[65] Additionally, the patron's personal information may be aggregated with other information acquired and maintained by the casino.[66] For example, a patron's financial credit history with the casino, any suspicious gambling activity by the patron, and the comp value or points balance earned by the patron on their loyalty card may be assessed for marketing analysis or other investigative purposes.[67]

Surely, many patrons would expect the casino to retain and protect loyalty card complimentary values or point balances. However, patron loyalty card

---

[56] *New Players Club for MGM Resorts International*, CASINO GAMING STOCK (June 18, 2010), http://www.casinogamingstock.net/news/new-players-club-for-mgm-resorts-international-mgm-903166.

[57] *Id.*

[58] Finnegan, *supra* note 55.

[59] *Id.*

[60] *Las Vegas Players Club Card – Casino Sign Up List*, LAS VEGAS- THE HOW TO GUIDE, http://www.lasvegas-how-to.com/players-club-card-list.php (last visited Oct. 13, 2011).

[61] Boyd Gaming, *Boyd Gaming's 'B Connected' Players Club Goes Nationwide – Casinos Giving Away Millions to Celebrate Rollout*, PR NEWSWIRE (Jun. 28, 2010), http://boydgaming.mediaroom.com/index.php?s=43&item=58.

[62] *Id.*

[63] *How to get Station Casinos Boarding Pass*, LAS VEGAS- THE HOW TO GUIDE, http://www.lasvegas-how-to.com/station-casino-players-club.php (last visited Oct. 13, 2011).

[64] *Id.*

[65] SHOOK, *supra* note 2, at 228-29; Effner Interview, *supra* note 2.

[66] Effner Interview, *supra* note 2.

[67] *Id.*

information, linked and available with the patron's personal information and gaming history, may provide external hackers or dishonest casino employees the ability to use the patron's personal information to the detriment of the patron and casino.[68] Thus, exposure of patron information may lead to fraudulent redemptions of a patron's earned rewards or comps, potential identity theft, or unwanted public exposure of the patron's gaming activity or other personal information.[69] The casino may also suffer negative publicity, patron distrust, loss of business, or legal liability.[70]

II. Personally Identifiable Information (PII)

Unauthorized access, use, or disclosure of personally identifiable information (PII) on computer systems, storage media, or in physical paper form can seriously harm both parties involved.[71] The individual may suffer from identity theft, blackmail, or embarrassment, while the organization (e.g., casino corporation) may suffer from a reduction in public trust or legal liability.[72] As sensitive information is stored and shared in electronic, verbal, and paper form, safeguards are needed to address the security of data classification, handling, storage, and disposal.[73]

One example of the danger posed by stolen PII occurred in May 2006 when a U.S. Veterans Affairs Department laptop was stolen from a private residence.[74] The laptop contained 26.5 million personal records for military veterans and a significant number of their spouses' information, including names, Social Security numbers, and dates of birth.[75] The incident concerned both lawmakers and citizens alike.[76] According to a government official's statement, "the theft was an unprecedented loss of personal information . . . [P]ersonal information can include your financial data, your medical data, and, basically, your virtual identity. All valuable data could easily lead to identity theft and no one seems safe."[77]

A. Identifying PII

Personal information does not include any publicly available information that may be legally obtained by the public from any federal, state, or local

[68] Interview with Jerry Markling, Chief of Enforcement Div., Nevada Gaming Control Bd., in Las Vegas, Nev. (Oct. 18, 2010).
[69] *Id.*; Effner Interview, *supra* note 2.
[70] Effner Interview, *supra* note 2.
[71] McCallister et al., Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), 2-1 (U.S. Dep't of Commerce, NIST Special Publ'n 800-122, April 2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf; *see also* Michael Metzler & Paul Harker, Personally Identifiable Information (PII): A White Paper on Information Security, 3 (Version 1.6, Revised August 2008) *available at* www.savvis.net.
[72] McCallister et al., supra note 71, at 2-1.
[73] *Id.*
[74] Meltzer & Harker, supra note 71, at 3.
[75] *Id.*
[76] *Id.*
[77] *Id.* (quoting L. Wilbanks, *The Impact of Personally Identifiable Information*, IT Professional, 9 (4), 62-64, 2007).

government records or widely distributed media.[78] The following list contains examples of qualified PII, subject to heightened protective security measures:

- Name, such as full name, maiden name, mother's maiden name or alias;
- Personal identification number, such as Social Security Number (SSN), passport number, driver's license number, taxpayer identification number, and financial account or credit card number;[79]
- Address information, such as street address or email address,
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristics), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).[80]

PII is treated differently from publicly available data because it needs to be collected, maintained, and disseminated in accordance with applicable federal and state laws.[81] The Organization for Economic Co-operation and Development ("OECD") Privacy Guidelines are the most commonly accepted privacy principles in the world.[82] The Privacy Guidelines were endorsed by the United States Department of Commerce in 1981.[83] The OECD Fair Information Practices have guided privacy law and policy initiatives in many other countries as well, including Sweden, Australia, and Belgium.[84] The OECD identified the following Fair Information Practices:

- **Collection Limitation** – There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality** – Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose Specification** – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change or purpose.
- **Use Limitation** – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.

---

[78] *Id.*

[79] Partial identifiers, such as the first few digits or the last few digits of SSNs, are almost always considered to fall under the category of PII because they may also be used to identify a specific individual.

[80] MCCALLISTER ET AL., supra note 71, at 2-2.

[81] *Id.* at 2-3.

[82] *Id.*

[83] *Id.*

[84] *Id.*

- **Security Safeguards** – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
- **Openness** – There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation** – An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.
- **Accountability** – A data controller should be accountable for complying with measures, which give effect to the principles stated above.[85]

Effective privacy standards must expand beyond statutorily required protections and confidentiality of PII.[86] To establish a comprehensive privacy program, corporations must consider a broad variety of privacy issues and must understand the risks they will face.[87] Policies and procedures should be implemented by Congress to address the Fair Information Practices identified by the OECD.[88]

B. Patron PII Confidentiality and Assessing the Risk of a Database Breach

A casino corporation will lower the level of risk posed by possessing patron PII by improving the confidentiality and security of the information maintained in its player database systems. The potential harm to an individual patron includes a multitude of negative and unwanted effects (i.e., that may be socially, physically, or financially damaging), such as blackmail, identity theft, physical harm, discrimination, or emotional distress.[89] Casino corporations will likely experience harm in the form of, but not limited to, administrative burdens, financial losses, loss of public reputation and public confidence, and legal liability.[90]

In terms of individual patron harm, some PII is easily used to identify specific individuals, while other forms of PII are less likely to identify specific individuals.[91] For example, a database of PII consisting of individuals' names, patron account numbers, or Social Security numbers can be used to identify an individual instantly.[92] In contrast, PII data exclusively made up of individuals' ZIP codes and dates of birth can only indirectly identify individuals or greatly

---

[85] *Id.* at 2-3 to -4.
[86] *Id.* at 2-4.
[87] *Id.*
[88] *See id.*
[89] *Id.* at 3-1 to -2.
[90] *Id.* at 3-2.
[91] *Id.* at 3-3.
[92] *Id.*

reduce a large dataset in an attempt to identify a particular individual.[93] Similarly, data comprised of only individuals' area codes and genders would be unlikely to provide any direct or indirect association to a particular individual depending upon the context and sample size.[94] PII that is uniquely and directly identifiable presents a higher risk to a casino corporation and poses a greater threat to an individual patron, compared to PII that is not directly identifiable.[95] Thus, casinos should make a concerted effort to identify patrons without using patrons' names or other readily identifiable information. However, if casinos do identify patrons using PII, a comprehensive privacy program should be in place to protect against identity theft.

A casino organization must defend against identity thieves from within and outside the confines of the organization.[96] The development and maintenance of large databases holding PII requires casinos to employ highly principled individuals.[97] The larger a database, the more vulnerable it is to attack, and the more trusted individuals are required to maintain it.[98] Principled employees and 24-hour data surveillance monitoring procedures are necessary to ensure security measures are not breached and PII data is not stolen, resold, or misused.[99]

Unfortunately, security breaches by employees or sub-contractors who have passwords or access to the system have been common.[100] Therefore, as these vulnerable and increasingly valuable databases continue to grow, security procedures and related technologies must likewise develop to deter theft and unlawful manipulation of PII by employees, sub-contractors, or external hackers alike.[101] There are more opportunities for the confidentiality of PII to be compromised when it is readily accessible by more people and multiple systems.[102] Amassing large databases creates inherent vulnerabilities that attract hackers because a successful breach can prove to be both efficient and lucrative.[103]

Casinos must also protect PII data when third-party vendors, sub-contractors, or other systems, such as web applications, outside the direct control of the casino corporation access the PII maintained by a casino.[104] In addition, a casino might be taking an increased risk should it choose to store or regularly transport PII data off its premises because the casino lacks the ability to ensure

---

[93] *Id.* (referencing a MIT study showing 97% of the names and address on a voting list were identifiable using only ZIP code and date of birth. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection (May 2001) (unpublished Ph.D. dissertation, Mass. Inst. of Tech.) (as cited in Am. Statistical Ass'n, *Data Access and Personal Privacy: Appropriate Methods of Disclosure Control* (Dec. 6, 2008), *available at* http://www.amstat.org/news/statementondataaccess.cfm.); *see also* Effner Interview, *supra* note 2.

[94] MCCALLISTER ET AL., supra note 71, at 3-3.

[95] *Id.*

[96] Kline, *supra* note 12, at 455.

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] MCCALLISTER ET AL., supra note 71, at 3-5.

[103] Kline, *supra* note 12, at 455.

[104] MCCALLISTER ET AL., supra note 71, at 3-5.

the information is securely stored at all times.[105] PII data stored on a corporation's property, within its secured physical boundaries, is less likely to be lost or stolen than similar data stored and maintained offsite.[106]

Another security problem in existing and newly formulated large database systems is the complexity and unpredictability of system designs.[107] As one security expert noted, "complexity is the worst enemy of security."[108] Large databases are difficult to secure because they are generally maintained in a disorderly mode and therefore are more unpredictable and more susceptible to catastrophic failures.[109] The number of records breached may have varying consequences, not only in terms of the collective harm to individuals, but also in terms of harm to the casino corporation's reputation.[110] The cost to the corporation that fails to address and prevent such data breaches can be enormous and irreversible. The following section illustrates several ways in which a casino can protect itself from security breaches.

C. PII Confidentiality Safeguards

PII can be protected through multiple procedures, including operational defenses, specific information technology safeguards, and security controls.[111] In addition, employee awareness, training, and education are critical measures that can serve to reinforce desired PII security practices and ensure the success of an organization's privacy and security programs.[112] With the recent increase in PII data breaches, a growing number of federal and state regulations now require businesses, private organizations, and government agencies that handle personal information on individuals (such as employees or customers) to implement security practices to protect PII and related sensitive data.[113] Failure to apply reasonably adequate measures to deter a potential breach in PII data places an organization at risk of negative publicity, reputational damages, loss of customer or employee trust, potential litigation, and a possibility of bankruptcy or closure.[114]

Most organizations are required to protect PII through application of federal laws, regulations, and other mandated prevailing procedures.[115] Violation of applicable federal or state legislation can result in civil or criminal penalties against organizations,[116] including casino corporations. Additionally, many casino corporations are obligated through their own policies, standards, or management directives to protect patrons' PII.[117] Although these mandated measures provide some level of PII data protection, the U.S. does not currently

---

105 *Id.*
106 *Id.*; *see also, e.g.*, Effner Interview, *supra* note 2.
107 Kline, *supra* note 12, at 455.
108 *Id.*
109 *Id.* at 455-56.
110 MCCALLISTER ET AL., supra note 71, at 3-3.
111 *Id.* at 4-1.
112 *Id.* at 4-2.
113 MELTZER & HARKER, supra note 71, at 3.
114 *Id.*
115 MCCALLISTER ET AL., supra note 71, at 3-4.
116 *Id.*
117 *Id.*

have a nationwide data privacy regulation for casino corporations to follow regarding PII confidentiality standards.[118]

III. U.S. Case Law & Regulations Regarding Privacy: Potential Casino Liability and Patron Remedies for a Breach in the Player Tracking System

Patron information is crucial to the success and evolution of innovative products and services as the economy continues to become ever more digital and innovative every day.[119] The use of this information allows patrons to receive personalized offers tailored to their liking.[120] Many companies utilize safety measures to ensure the protection of consumer information; however, some do not.[121] Not only must the industry as a whole do better, but also privacy should be a basic consideration for every business, similar to other essential business practices.[122] The following study illustrates how the careless treatment of consumer information poses a serious threat and requires a comprehensive U.S. law to provide a fundamental structure for businesses to advance individual privacy interests.[123]

According to a 2008 benchmark study, the costs associated with data breaches in the U.S. continue to escalate.[124] The Fourth Annual U.S. Cost of Data Breach Study ("Study") reported the average cost of a data breach increased from $138 per individual record lost or stolen in 2005 to $202 in 2008.[125] In addition, more than 250 million customer records containing confidential personal information have been lost or stolen since 2005.[126]

The Study reviewed forty-three U.S. companies that experienced a breach involving the loss or theft of individual customer or consumer data in 2008.[127] Each of the companies reviewed experienced a data breach associated with the loss or theft of 4,200 to 113,000 records.[128] The estimated cost in each instance ranged from a minimum of $613,000 to a maximum of $32 million, providing an average cost of $6.65 million per company affected.[129] The Study found that as the number of individual data records compromised increased, the cost of the data breach to the company proportionally grew as well.[130] Additional facts noted by the Study included the following:

---

118 *See id.*

119 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers, i, (Dec. 2010).

120 *Id.* at ii.

121 *Id.* at i.

122 *Id.*

123 *Id.*

124 S. Montaye Sigmon, *2008: Study: Cost of Data Breaches Continues to Rise*, Privacy L. Blog (Feb. 25, 2009, 1:00 PM), http://privacylaw.proskauer.com/2009/02/articles/data-breaches/2008-study-cost-of-data-breaches-continues-to-rise/.

125 *Id.*

126 *Id.*

127 *Id.*

128 *Id.*

129 *Id.*

130 *Id.*

- Approximately 35% of all data breach incidents involved lost or stolen laptop computers or other mobile data devices;
- More than 88% of all cases in the 2008 Study involved insider negligence;
- Data breaches involving malicious acts are more expensive than breaches involving negligent acts, costing some $26 more per customer record; and
- First-time data breaches are more expensive than subsequent breaches, costing some $243 per customer record versus $199 per customer record for companies that have experienced previous data breaches.[131]

The problems associated with identity theft are similar to those concerning database-driven information systems.[132] As data breaches and identity theft risks continue to increase, the American public will likely convey greater concerns regarding PII data privacy.[133] These concerns can be primarily traced to the inadequate privacy protection laws in the United States.[134] In 2002 and 2003, approximately ten million Americans were victims of identity theft, resulting in estimated costs of $53 billion.[135] Identity theft has been the most common complaint received by the Federal Trade Commission ("FTC"), totaling 39% of all complaints in 2004 and 36% in 2006.[136] When a problem such as identity theft becomes so prevalent in society, the issue of legal protections for personal data privacy becomes even more pressing.[137]

The following section discusses federal and state U.S. privacy laws applicable to the casino industry and its security measures surrounding collection, maintenance, and use of patron database systems. The current case law regarding security data breaches and identity theft in non-casino based organizations is reviewed to compare similar potential harms to the casino industry, specifically to those patrons whose data resides in casino player database systems.

A. Federal Privacy Case Law & Regulations

The United States has long sustained an industry-specific approach toward privacy of personal information, relying on a patchwork application of federal and state laws.[138] The U.S. courts have done little to define PII and promote comprehensible laws regarding data privacy in the public and private sector. Regardless of purpose or intent, courts have rarely intervened to protect individuals once data has been released to third parties.[139] These courts are generally complacent and deferential to the construction and operation of information databases.[140] Similarly, substantive law procedures and standards applicable to the right to privacy provide limited personal data protections and inadequately address the complex nature of modern data privacy issues.[141]

---

131 *Id.*
132 Kline, *supra* note 12, at 458.
133 *Id.* at 457.
134 *Id.*
135 *Id.* at 458.
136 *Id.*
137 *Id.* at 457-58.
138 *See* Ariane Siegel et al., *Survey of Privacy Law Developments in 2009: United States, Canada, and the European Union*, 65 BUS. LAW. 285, 287 (2009).
139 Kline, *supra* note 12, at 458.
140 *Id.*
141 *Id.*

Casino patrons have few means to protect themselves effectively from identity theft crimes. All of the information held on the casino player database systems is potentially at risk.[142] Identity thieves and other criminals recognize casino patron database systems are lucrative targets because of the vast amounts of personal data maintained on a central database system.[143] They recognize the limitations in database-driven information markets and take advantage of several factors: "(1) lack of individual control of personal data, (2) third-party dominance, (3) an inability to seek adequate legal remedies, and (4) a complete lack of transparency on data use."[144] These shortfalls in data privacy show the need for legal remedies to address data security risks and for other methods of encouraging responsible database management practices.[145]

The modern third-party problem in database-driven information systems does not comport with the traditional form of rival relationships (in litigation).[146] This is primarily because an individual's right to privacy under the Fourth and Fifth Amendments of the U.S. Constitution are not held to apply to third-party data disclosures because of weak interpretations by American courts.[147] For example, the U.S. Supreme Court requires both "subjective and objective expectations of privacy" in Fourth Amendment jurisprudence, creating a narrow view of the right to privacy.[148] The Court has found there is no finding of either subjective or objective privacy once an individual releases his information into the stream of commerce.[149] Also, efforts by a plaintiff to amass a privacy-based tort case are generally held ineffective against the strong protections of the First Amendment, which often weigh in favor of third-party commercial or publication interests.[150] Therefore, U.S. constitutional law offers little protection to those individuals seeking a right to data privacy,[151] including those patrons voluntarily disclosing personal information to a casino in return for obtaining a player's card.

Similarly, judicial deference to the markets and its promotion of individual choice in commercial transactions limits individual data privacy rights available through contract and property law.[152] Under these principles, any applicable regulation on the free trade of personal data would require statutory formation.[153] However, legislative actions have provided limited legal protection in the data privacy domain based on inconsistency and lack of form.[154] These legislative problems highlight an essential issue with United States data

---

142 Chris Sieroty, *Casinos Cautioned to restrict access to player card information*, LAS VEGAS REV.-J. Jan. 19, 2011, http://www.lvrj.com/business/casinos-cautioned-to-restrict-access-to-player-card-information-114193164.html.

143 *See id.*

144 Kline, *supra* note 12, at 458.

145 *Id.*

146 *Id.*

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.* at 458-59.

151 *Id.* at 459.

152 *Id.*

153 *Id.*

154 *Id.*

privacy law: the lack of an omnibus data privacy statute.[155] As noted, the judicial deference given to privacy issues furthers the gap in security over personal data by allowing minimal judicial oversight of personal data use and allowing data users to utilize database-driven information markets freely for almost any commercial, investigative, or other private purpose.[156]

Although a variety of federal laws relate to identity theft, none include a private right of action.[157] Therefore, plaintiffs seeking damages for alleged identity theft must look to applicable state law measures.[158] Unfortunately, plaintiffs attempting to seek civil recoveries at the state level have been largely unsuccessful due to the inherent difficulties in proving actual harm.[159] The courts have accepted the general standard that an alleged increase in risk of future injury is not an "actual or imminent" injury in cases of identity theft.[160] Consequently, the cases brought forward involving identity theft or claims of negligence and breach of confidentiality have often found that plaintiffs do not have standing, or the courts have granted summary judgment for failure to establish the necessary harm and associated damages.[161]

The applicable laws do not appear to take into account lost opportunities associated with identity theft when evaluating a plaintiff's harm.[162] Some victims of identity theft suffer by: having to spend thousands of dollars and years dealing with credit bureaus and debtors; losing out on job opportunities; being denied loans for education, housing, or cars because of negative information on their credit reports; and in rare cases, are arrested for crimes identity theft victims did not commit.[163]

The FTC began its efforts to protect consumer privacy at the federal level in 1970 with the passage of the Federal Credit Reporting Act ("FCRA").[164] The FCRA limited the FTC's review to the regulation of consumer reporting agencies and their use of individuals' credit-related information.[165] The FTC's primary source of legal authority derives from Section 5 of the FTC Act, which empowers the FTC to take action against deceptive or unfair acts or practices.[166] The FTC has applied two primary models in the context of data privacy law: the "notice-and-choice" and "harm-based" models.[167]

The "notice-and-choice" model encourages companies to design privacy notices for consumers describing the process and general procedures regarding their information collection and use practices, so they may make informed

155 *Id.*
156 *Id.*
157 Denis T. Rice, *Trends in Security and Privacy Breach Litigation: is the Liability Expanding?*, *in* PRACTICING L. INSTITUTE, 507, 544 (2010).
158 *Id.*
159 *Id.*
160 *Id.*
161 *Id.*
162 Brian Krebs, *New Federal Law Targets ID Theft, Cybercrime, Security Fix*, WASHINGTON POST (Oct.1, 2008, 4:33 PM), http://voices.washingtonpost.com/securityfix/2008/10/new_federal_law_targets_id_the.html.
163 *Id.*
164 FED. TRADE COMM'N, *supra* note 119, at ii.
165 *Id.* at 3.
166 *Id.* at 3-4.
167 *Id.* at iii.

choices.[168] The "harm-based" model focuses on protecting consumers from specific harms such as physical security, economic injury, and unwanted intrusions caused by unforeseen exploitation of their personal data.[169] Although each model has significantly advanced the FTC's goal of protecting consumer privacy rights, each model has also received ample criticism.[170]

The FTC's "notice-and-choice" model has led to long and nearly incomprehensible privacy policies that an average American consumer does not typically read or even understand.[171] Similarly, the "harm-based" model has been criticized for failing to recognize privacy-related risks and consumer concerns beyond financial harms, including harm to an individual's reputation and fears of being monitored.[172] In addition, both models struggle to keep pace with the speedy rise of technologies and business models that allow companies to collect and utilize individuals' personal information in a way unknown to the individual.[173] Meanwhile, industry efforts to enhance privacy through self-regulation are slow and have failed to provide adequate and meaningful data privacy protections.[174]

Beginning in the mid-1990s, in reaction to the passage of new consumer privacy laws, the FTC began to examine privacy issues beyond the scope of the FCRA.[175] The FTC focused its attention toward enforcing multiple sector-specific statutes, including the Gramm-Leach-Bliley Act (GLBA) enacted in 1999.[176] The primary purpose of the GLBA is to enhance efficiency in the financial services industry.[177] The GLBA allows financial institutions to share the "nonpublic personal information" within its company sub-parts with no obligation to restrict the sharing of customer information; however, a company must notify its customers of any outside information sharing activities it performs.[178] Thus, individuals have no right to stop companies from sharing their personal information when it is shared within the company.[179] However, any information shared by the company with a third party must be disclosed to the customer, and the customer must be given the right to opt-out of such information sharing practices.[180]

It has been argued that casino corporations may qualify under the GLBA as a "financial institution."[181] However, the FTC and other federal governmental entities have not applied the definition of "financial institutions" as codified in the GLBA to include casino corporations.[182] As a result, no federal data

168 *Id.*
169 *Id.*
170 *Id.* at iii.
171 *Id.*
172 *Id.*
173 *Id.*
174 *Id.*
175 *Id.* at 3.
176 *Id.* at 4.
177 *See* 15 U.S.C. § 6801 (2006).
178 *Id.* at § 6802(a).
179 *Id.*
180 *Id.*
181 Interview with Lisa Mathis, Senior Corporate Counsel, Legal Dep't, Caesars Entm't Corp., in Las Vegas, Nev. (Sept. 16, 2010).
182 *Id.*

privacy regulations directly apply to the casino industry regarding the maintenance and security of patron database systems.[183]

In 2000, the FTC used its authority to bring actions against several non-gaming companies that engaged in unfair or deceptive information practices.[184] Most of the early cases that came before the FTC involved misleading company statements in privacy notices sent to consumers regarding the collection and use of their data.[185] These cases encouraged the FTC to shift its concern toward offline data privacy threats and the increasing integration of online and offline data systems.[186] Thus, the FTC's privacy approach evolved to incorporate specific consumer harms as the principal means of tackling individual consumer privacy concerns.[187] Instead of applying the costly "notice-and-choice" standards for all applications of information, the FTC used the "harm-based" model, focusing on organizational processes that caused, or were likely to cause, physical or economic harm to individual consumers.[188]

The "harm-based" model effectively provided individual consumer protections in a variety of areas, including data security, identity theft, spam, and other related contexts.[189] Further, the FTC has applied its given authority under multiple statutes (including the FCRA, the GLBA, and Section 5 of the FTCA), to bring twenty-nine cases against businesses that allegedly failed to protect consumers' personal information in 2001.[190] The cases brought forth by the FTC were against well-known, recognized companies, such as Microsoft, ChoicePoint, TJX, and LexisNexis.[191] The companies were alleged to have failed to, "(1) comply with posted privacy policies, (2) take appropriate steps to protect against common vulnerabilities, (3) dispose of data properly and (4) take reasonable steps to ensure that they do not share customer data with unauthorized third parties."[192]

ChoicePoint, a data broker with more than nineteen billion records on almost every American, sold personal data in 2005 to identity thieves operating a fraudulent business.[193] The personal data sold included names, addresses, and Social Security numbers of 163,000 individual records.[194] The ramifications of the ChoicePoint breach resulted in potentially 1,400 cases of identity theft against the company.[195] The breach came to light when ChoicePoint mailed notification letters to inform only the 30,000 California residents that were affected, but failed to notify the residents of other states of the situation.[196] The disclosure letters were distributed pursuant to California's security breach

---

183 *Id.*
184 *See* FED. TRADE COMM'N, *supra* note 119, at 8.
185 *Id.* at 8-9.
186 *Id.* at 9.
187 *Id.*
188 *Id.*
189 *Id.* at 10.
190 *Id.*
191 *Id.*
192 *Id.* at 10-11.
193 Kline, *supra* note 12, at 456.
194 *Id.*
195 *Id.*
196 Wolf, *supra* note 7, at 1-45.

notice requirement.[197] Soon thereafter, other states' governing bodies began to demand their respective state citizens affected receive notification as well.[198] ChoicePoint then proceeded to notify all who had been affected throughout the country.[199] As of January 17, 2008, the ChoicePoint 2005 data breach was estimated to result in the disclosure of more than 217 million records comprising personal data.[200]

A breach in individual personal data held by an organization may also result in corporate liability.[201] In January 2009, Heartland Payment Systems, the sixth-largest payment processor in the United States, disclosed that an undetermined number of its consumers were exposed to potential fraud due to a breach in its processing systems.[202] The repercussions of the breach came to surface when more than 625 financial institutions disclosed that their consumer cards were jeopardized from the Heartland data breach.[203] As a result, three types of class action suits were filed against Heartland.[204] Consequently, Heartland announced that it would install a complete encryption system in 2009 to protect its processing network better.[205] These events gave renewed awareness to the ever-increasing concerns and costs associated with identity theft—a crime that affects an estimated ten million Americans each year.[206] However, the distribution of liability to an organization and the third-party hacker in data breach cases remains an unsettled area of law.[207] It is unclear if a data breach were to occur in a casino patron database system what, if any, federal laws would apply. Further, it is uncertain if the federal court system would hold the casino liable for damages sought by patrons.

B. State Privacy Case Law & Regulations

Over time, states have continued to enact new data privacy and security legislation to protect their citizens' PII.[208] The majority of states, including California, Connecticut, Illinois, Missouri, Nevada, New York, and Texas, have enacted laws that limit business use and disclosure of personal information,

---

197 *Id.*;

> Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . .

S.B. 1386, codified at CAL. CIV. CODE § 1798.82(a).

198 Wolf, *supra* note 7, at 1-46.

199 *Id.*

200 Kline, *supra* note 12, at 457.

201 Siegel et al., *supra* note 138, at 294.

202 *Id.*

203 *Id.*

204 *Id.*

205 *Id.*

206 Wolf, *supra* note 7, at 1-45.

207 *See* Jeremy Feigelson & Camille Calman, *Liability for the Costs of Phising and Information Theft*, J. INTERNET L., Apr. 2010, at 1, 22.

208 Siegel et al., *supra* note 138, at 288.

especially in the use of Social Security numbers.[209] Most states mandate companies to enact and enforce valid security procedures and practices to protect PII; furthermore, to notify individuals adversely affected by an unlawful breach of PII held by the company.[210] These state laws were enacted in response to consumer fears of identity theft, heightened by highly publicized data security breaches taking place across the country.[211] The privacy laws largely mirror California's first-in-the-nation data security breach notification law; however, there remain significant differences in the requirements between each of these state laws.[212] Federal legislation, which would set a minimum uniform standard across all states, has seriously been considered since 2005; however, no action has been taken.[213]

California has taken the lead on being one of the most active states to create measures regarding privacy and protecting its citizens.[214] The Security Breach Information Act, also commonly referred to as S.B. 1386, requires customer notification for all security breaches related to personal information; the law was the first of its kind to be passed in the United States.[215] The California law requires notification to individuals after unauthorized possession of computerized data that "jeopardizes the security, confidentiality, or integrity of personal information that is maintained by the person or business experiencing the breach."[216] Additionally, a third-party maintaining data on behalf of an entity must notify the entity of any data security breach immediately upon discovery of an occurrence of data breach.[217]

A California court, ruling under S.B. 1386, found that a plaintiff that had his PII stolen, had standing to sue.[218] In *Ruiz v. Gap, Inc.*,[219] a laptop computer that held unencrypted personal identification information of 750,000 job applicants was stolen from a Gap processing vendor.[220] The Gap notified the applicants whose information was stolen and offered twelve months of free credit monitoring.[221] Ruiz did not register for the free credit monitoring offered by the Gap; instead, he filed a complaint against the company for negligence.[222] A negligence claim under California law requires the claim be based on "appreciable non-speculative, present harm."[223] However, the harm asserted in Ruiz's claim was based on a future (rather than present) risk of identity theft.[224] Thus, the court held that an increased risk of identity theft "does not rise to the level of . . . harm necessary to assert a negligence claim under California law," and

[209] *Id.*
[210] *Id.*
[211] Wolf, *supra* note 7, at 5-26.
[212] *Id.*
[213] *Id.*
[214] *Id.* at 5-3.
[215] *Id.* at 5-26.
[216] *Id.* at 5-26 to -27.
[217] *Id.* at 5-27.
[218] Siegel et al., *supra* note 138, at 294.
[219] *See* 622 F. Supp.2d 908 (N.D. Cal. 2009).
[220] *Id.* at 910; Siegel et al., *supra* note 138, at 294-95.
[221] Siegel et al., *supra* note 138, at 295.
[222] *Id.*
[223] *Id.*
[224] *Id.*

dismissed the case.[225] However, the *Ruiz* finding did endorse a plaintiff's standing to sue if his or her PII is stolen and if actual harm is suffered; thus, potentially exposing business entities to longer and more costly litigation.[226]

Although most states generally follow California's breach notification framework and regard it as adequate, they also include their own derivative containing subtle distinctions and provisions regarding notification procedures.[227] Some go as far as mandating additional measures beyond security breach notification requirements with the goal of developing a comprehensive legal standard to deter identity theft.[228] Some of the additional legislative measures include mandating the implementation of procedures to safeguard personal information, and others specify data destruction requirements.[229]

Nevada is one of forty-six states that enacted legislation requiring notification of security breaches involving personal information.[230] Nevada Revised Statutes ("NRS") 603A.210 "Security Measures" and NRS 603A.220 "Disclosure of Breach of Security System Data, Methods of Disclosure," describe in detail the security measures required by state law.[231] In addition, these statutes discuss required notifications in cases where unauthorized persons access private information.[232]

Nevada Regulation 5.011 provides a list of actions and omissions that may be considered unsuitable methods of operation; subsection 8 specifically notes the Nevada Gaming Commission's discretion to interpret statutes:

> Failure to comply with or make provision for compliance with all federal, state and local laws and regulations pertaining to the operations of a licensed establishment . . . . The Nevada Gaming Commission in the exercise of its sound discretion can make its own determination of whether or not the licensee has failed to comply with the aforementioned, but any such determination shall make use of the established precedents in interpreting the language of the applicable statutes. Nothing in this section shall be deemed to affect any right to judicial review.[233]

The Nevada Gaming Control Board ("Board") is obligated to ensure gaming is conducted consistent with the State's public policy and not in a way "[i]nimical to the public health, safety, good order and general welfare . . . ."[234] In addition, Nevada law enables the Board and Nevada Gaming Commission to consider certain acts or omissions performed by a gaming licensee, which include a licensee's non-compliance with all federal, state, and local laws, as unfit methods of operation.[235]

The Board issued an industry notice to all non-restricted gaming licensees who utilize and maintain personal or financial information of patrons in a com-

---

225 *Id.* (quoting Ruiz v. Gap, Inc., 622 F. Supp.2d 908, 913 (N.D. Cal. 2009)).
226 *See id.*
227 Wolf, *supra* note 7, at 5-29.
228 *Id.* at 5-45.
229 *Id.* at 5-45 to -46.
230 Industry Notice, *supra* note 11.
231 *Id.*
232 *Id.*
233 *Id.*
234 *Id.*
235 *Id.*

puterized database on December 15, 2010.[236] In the notice, the Board acknowledged that particular gaming licensees maintain large databases that contain casino patron personal or financial information.[237] The industry notice was intended to serve as a reminder to all casino licensees who maintain patron personal or financial information to conduct periodic reviews of existing security measures in place and verify compliance with the security and breach disclosure requirements provided in NRS 603A.[238]

With respect to casino patron database systems, the Board has recently investigated several incidents where such databases have been maintained, and the potential for improper disclosure of PII and identity theft existed.[239] In addition, the Board stressed that casinos will almost certainly become an even greater target for cyber-criminals as more and more information is stored on these databases.[240] Although the Board's industry notice did not provide details as to the matters investigated, two recent incidents became public involving the theft of personal information in Las Vegas, Nevada.[241] In July 2010, a hacker received information about attendees at Cisco Live 2010, a computer industry event at Mandalay Bay.[242] The information stolen, however, was not linked to Mandalay Bay's database.[243] Similarly, the Desert Rose Resort also reported that an "unspecified number" of guests at the hotel between June 2010 and October 2010 had their debit and credit card information stolen by a malicious software virus.[244] These two attacks serve as early warning signs as to the gravity and invasive nature of cyber-criminal attacks and their ability to acquire personal information held by casino corporations.[245]

All businesses face a certain level of inherent threat to maintaining databases that store personal and financial information.[246] Casinos are exceptionally professional about the collection and storage of personal information and generally utilize multiple layers of security to protect the data they hold, including measures to encrypt the data held.[247] Although there are no easy solutions when it comes to ensuring the safety and security of PII, doing so has become an inherent cost of business.

A growing number of fraud cases in Las Vegas arise primarily out of point stealing schemes and involve casino patron database systems and the cards used by patrons.[248] The Enforcement Division of the Board has investigated multiple instances of patrons' player's club points being stolen.[249] As the controlling gaming regulatory system in the State of Nevada, the Board has

---

236 *Id.*
237 *Id.*
238 *Id.*
239 *Id.*
240 *Id.*
241 Sieroty, *supra* note 142.
242 *Id.*
243 *Id.*
244 *Id.*
245 *See id.*
246 *See id.*
247 *Id.*
248 *Id.*
249 *Id.*

reminded casino licensees of their responsibilities to maintain security of customer databases.[250] All of these threats support the need for stronger safeguards and regular review of the existing policies and laws in place to ensure compliance and protection of PII from unauthorized access.[251] Although Nevada state legislators have enacted very strict laws regarding customer confidentiality, other jurisdictions across the country have not.[252] As a result, compliance from multi-jurisdictional businesses, including casino corporations, has been much more piecemeal and difficult in its application.

IV. Models for an Omnibus U.S. Privacy Law Applicable to Casino Patron Database Systems: The EU Data Privacy Directive and Canadian PIPEDA

Database-driven information systems contain inherent imperfections and require adequate regulatory safeguards and monitoring.[253] In contrast to the more piecemeal approach to data privacy in the United States, Canada and the European Union have adopted a comprehensive umbrella privacy policy that address the many facets of data collection and storage.[254] Comprehensive data privacy regulations modeled after the European Union Data Protection Directive ("EU Directive") and the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA") are needed in the U.S. to protect individual privacy interests. Through greater recognition of individual data privacy rights, a U.S. data privacy statute could create additional incentives to improve the accuracy and integrity of casino database-driven information markets, as well as all U.S. industry information markets, while also ensuring remedial measures would be available to those individuals whose PII is breached.[255] This section explores the right to privacy concept in the U.S. and compares U.S. data privacy law to Canadian and European Union privacy law.

A. EU Data Protection Directive

The European Union Data Protection Directive 95/46/EC ("EU Directive") went into effect in October 1998, with the intent to create coordinated national laws throughout the EU to ensure the movement of personal information was protected with respect to the processing of personal information.[256] European privacy regulators apply a broad interpretation to the EU Directive statutory language; thus adopting a very expansive view of the applicable privacy laws.[257] The EU Directive regulates and oversees the "collection, use, and transfer of individually identifiable personal information about employees and

---

[250] *Id.*
[251] Industry Notice, *supra* note 11.
[252] *See* Sieroty, *supra* note 142.
[253] Kline, *supra* note 12, at 443.
[254] Siegel et al., *supra* note 138, at 295, 299.
[255] *See* Kline, *supra* note 12, at 443.
[256] Nixon Peabody, LLP, *European Union Data Protection Directive and U.S. Safe Harbor: An Employer Update*, 1, 1 Privacy Alert (Sept. 7, 2004), http://nixonpeabody.com/linked_media/publications/PrvcyAlert_09072004.pdf.
[257] Siegel et al., *supra* note 138, at 300.

consumers, such as name, address, telephone number, and marital status."[258] In addition, it also covers information relating to salary, bonuses, terms of an employment contract, and performance appraisals.[259]

The U.S. should look to the EU Directive as a useful framework to emulate in implementing a nationwide privacy statute that addresses privacy rights and concerns in database-driven information systems.[260] The EU Directive maintains strict regulations for the processing of individual personal data.[261] It also describes data processing broadly to include almost all database-driven information system activities as:

> [A]ny operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[262]

The EU Directive encompasses all practical procedures for collecting and processing private information: manual, automatic, online, and offline.[263] However, it is important to note that the EU Directive is "framework legislation" and establishes minimum standards each member state shall incorporate to their privacy-related laws.[264] Although the EU Directive sets a floor in some instances, it does not prohibit deviations among member state privacy laws that allow higher and stricter standards.[265]

Each member state is mandated to form an independent Data Protection Authority ("DPA") to oversee the collection and appropriate security of personal data.[266] An employer or organization notifies the DPA when they wish to process data, or they must register with the DPA prior to processing any data, unless the employer fits within an exemption.[267] To register with the DPA, an employer or organization must provide the following information on "(i) the purpose of the processing, (ii) the categories of individuals whose data are being processed and types of related data, (iii) the categories of recipients, (iv) proposed transfers to third countries, and (v) security measures."[268]

The gaps and inconsistencies found in U.S. privacy laws have been minimized in comparable EU laws by the EU Directive's use of a broad and consistently applied approach to regulating database-driven information systems.[269] The EU Directive therefore regulates, but does not prohibit, database-driven information systems.[270] The availability of personal information has become more readily available over time as commercial trade flows increase and data

---

[258] Nixon Peabody, LLP, *supra* note 256, at 1 (emphasis omitted).
[259] *Id.*
[260] Kline, *supra* note 12, at 488.
[261] Nixon Peabody, LLP, *supra* note 256, at 2.
[262] Kline, *supra* note 12, at 489.
[263] Nixon Peabody, LLP, *supra* note 256, at 1.
[264] *Id.*
[265] *Id.* at 3.
[266] *Id.*
[267] *Id.*
[268] *Id.*
[269] *See* Kline, *supra* note 12, at 489.
[270] *Id.*

processing technology continues to advance.[271] The EU Directive advances the use of database-driven information systems while balancing individual privacy rights in personal data.[272] The EU Directive protects personal privacy rights by acknowledging the free-flow of personal data and exercises restrictions over such flows with rules that improve data accuracy and ensure sensitivity to individual data privacy rights in data-processing.[273] Compliance with the EU Directive places modest additional costs on the industry and government.[274]

The EU Directive successfully maintains a balance in regulation and personal privacy rights by establishing five basic rule categories.[275] Those categories are: "(1) data accuracy and quality; (2) legitimate data processing practices; (3) additional protection for sensitive personal data; (4) right to notice for data subjects; and (5) affirmative individual rights to access, to object, and to seek a judicial remedy for any breach of applicable Member State privacy laws."[276] The EU Directive further ensures these rules are not avoided through outsourcing or transfer of job operations to third-party countries that fail to ensure appropriate levels of protection.[277] The third-party transfer provision established in the EU Directive makes certain global attention and compliance to the EU Directive guidelines.[278]

B. The Canadian PIPEDA

Although Canada first enacted private sector privacy laws in the early 1990s, privacy regulation did not make its way into mainstream Canadian culture until 2000, when the federal government introduced the Personal Information Protection and Electronic Documents Act ("PIPEDA").[279] PIPEDA is different in its structure to the EU Directive because many of its operative provisions are included in a set of relatively general personal information protection guidelines for businesses, referred to as Schedule I.[280] Schedule I incorporates ten basic privacy principles, which can be summarized as follows: accountability, identifying purposes, consent, limiting collection and use, disclosure and retention, accuracy, safeguards, openness, individual access, and challenging compliance.[281]

PIPEDA applies to an entire organizational group, thus, unlike the United States' federal GLBA that allows corporations to exchange PII data between multiple entities within a corporate group, the PIPEDA maintains no such exception.[282] This principle has most often applied in situations involving organizations that offer individual customer data to affiliates for marketing pur-

---

[271] *Id.*
[272] *Id.* at 489-90.
[273] *Id.* at 489.
[274] *Id.* at 490.
[275] *Id.*
[276] *Id.*
[277] *Id.*
[278] *Id.*
[279] Wolf, *supra* note 7, at 13-85.
[280] *Id.* at 13-87.
[281] *Id.* at 13-89 to -91.
[282] *Id.* at 13-117.

poses.[283] PIPEDA requires that "organizations obtain an individual's consent when they collect, use, or disclose the individual's personal information in the course of commercial activities, and that the personal information be used or disclosed only for the purposes for which it was collected."[284]

Most of the operative portions of PIPEDA attempt to specify when consent is or is not required and how an individual can withdraw their consent.[285] An organization that collects personal information has an obligation to safeguard and not use or disclose the information to third parties without consent.[286] This includes the use or disclosure of personal information for marketing.[287] PIPEDA requires that, at a minimum, the organization must give notice of such uses to customers and must give them an opportunity to opt out of receiving marketing materials from those affiliates.[288]

Under PIPEDA, organizations are required to implement their own privacy policies and practices.[289] Many organizations have concentrated on the general privacy policy requirements and have failed to develop actual privacy practices and procedures for the handling of personal information.[290] Privacy issues, generally, will often occur due to a lack of proper privacy practices rather than a lack of proper privacy policies.[291] Some examples of appropriate privacy procedures that must be implemented are included in the PIPEDA Principle 4.1.4.[292] The procedures discuss how to receive and respond to complaints and inquiries to train staff, how to effectively communicate information about the organization's privacy policies and practices to employees and agents, and last, how to explain the organization's policies and procedures to customers or other third-parties.[293]

Under PIPEDA, "organizations must employ security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification."[294] The type of safeguards imposed will vary depending on the sensitivity, amount, and distribution methods of the information that has been collected.[295] The methods of protection, according to PIPEDA, should include "physical measures (locked filling cabinets and restricted access to offices), organizational measures (security clearances and limiting access on a 'need-to-know' basis), and technological measures (passwords and encryption)."[296]

Canada's PIPEDA and general system of privacy law has served as an example to other countries in establishing guidelines on data breach notification

---

283 *Id.*
284 Siegel et al., *supra* note 138, at 296.
285 Wolf, *supra* note 7, at 13-119.
286 Siegel et al., *supra* note 138, at 296.
287 *Id.*
288 Wolf, *supra* note 7, at 13-87.
289 *Id.* at 13-154.
290 *Id.*
291 *Id.*
292 *Id.*
293 *Id.*
294 *Id.* at 13-155.
295 *Id.*
296 *Id.*

and reporting standards.[297] To a significant extent, Canada's data breach notification guidelines have influenced the implementation of similar regulations adopted in New Zealand and Australia.[298] The Canadian PIPEDA should also serve as a comprehensive data privacy law that the United States can emulate as a guide in the creation of an omnibus U.S. data privacy law.

C. Benefits of Applying International Privacy Laws in the U.S.

Legal developments in the areas of data protection and privacy are in a state of flux worldwide. It is imperative that the U.S. eliminates the industry-based approach and provides a nationwide data privacy statutory framework in order to provide appropriate protection and relief to consumers in the United States. Current federal requirements are weak and simply require "reasonable" measures be taken according to the type of industry. The U.S. maintains no comprehensive PII data privacy policy and offers no judicial remedy to those injured by a breach in PII data security. Canadian and European Union privacy laws require much more advanced and specific measures, including required customer or employee consent to maintain PII, PII data breach notification, comprehensive PII data security safeguard standards, and mandatory implementation of organizational PII data security policies and procedures.

A compelling way to confront the inconsistencies and lack of federal privacy law in the U.S. is to adopt a comprehensive data privacy law modeled after the EU Data Directive and Canadian PIPEDA.[299] Congress, privacy advocates, and the business sector appear to share a desire to clarify the standard practices and procedures when it comes to balancing privacy interests with database-driven information systems.[300] Leading technology companies publicly advocate for a comprehensive federal privacy statute.[301] In addition, as the Chief Marketing Officer of ChoicePoint acknowledges, society must make a decision regarding the use of private information in the marketplace and seriously consider the creation of a better national framework.[302] Thus, given the U.S. Supremacy Clause, federal legislation would provide uniformity to the multi-state, mixed level of privacy laws currently enacted across the nation.

A comprehensive federal privacy statute would provide a safe harbor provision, similar to the existing safe harbor agreement allowing U.S. corporate adherence to the EU Directive. A federal privacy statute can provide the needed flexibility if compliance would require either extended implementation time or flexibility in certain industries.[303] Implementation of a U.S. data privacy statute will impose stricter liability standards upon casino, and other business industries; however, reasonable time will be provided to those entities to allow effective and efficient conformity to new privacy laws imposed.[304]

---

297 Siegel et al., *supra* note 138, at 299.
298 *Id.*
299 Kline, *supra* note 12, at 493.
300 *Id.* at 493-94.
301 *Id.* at 494.
302 *Id.*
303 *Id.* at 493.
304 *Id.*

Large data brokerage companies, credit companies, and other corporate and government stakeholders argue that an omnibus data privacy statute providing similar protections to those offered in the EU Directive and the Canadian PIPEDA is unnecessary.[305] Their justification relies primarily on three arguments: "(1) [the] industry can effectively self-regulate and protect individual privacy interests; (2) the current industry serves important functions that benefit society; and (3) the freedom with which Americans surrender data suggests little public concern for privacy protections."[306] Further, these anti-data privacy advocates reason international data privacy regulations such as the Canadian PIPEDA and EU Directive would shut the database-information industry down, eliminate jobs, and take value out of the economy.[307] However, these rationales are unfounded and based on fear.

Like most new regulations, new burdens would initially be placed on the industry; however, many of these costs should already be accounted for by each organization as part of a well-crafted business model.[308] It is vital to maintain data accuracy and reliability for any organization.[309] Identity thieves thrive in database-driven information markets by searching for and manipulating weaknesses in PII database systems.[310] Inadequate data management practices today may lead to significant economic costs that jeopardize our economy in the future.[311] Public opinion must unite and demand stricter privacy legislation and greater industry regulations as data breaches and instances of identity theft continue to increase.[312] Specifically, proactive measures must be taken by the industry today to determine the necessary level of safe guards required in the future as these database systems continue to develop in capability and expand in size over time.[313]

The purpose of the EU Directive is the uniformity of data protection laws across the EU Member States.[314] Similarly, the purpose of the Canadian PIPEDA is to apply minimal data privacy standards across all Canadian provinces to achieve consistency and equivalence. These approaches are in direct contrast with the U.S., which has taken an industry-based approach, relying on industry specific legislation, government regulation, and self-regulation by corporate entities.[315] The potential benefits to the U.S. in adopting the EU and Canadian omnibus data privacy regulatory approach include: (1) a uniform data privacy standard applicable to all private, public, commercial sectors (including the gaming industry); (2) the improvement of database-driven information systems through clearly defined guidelines to data privacy; (3) effective leverage of individual data subjects to address database accuracy; and (4) enhanced indi-

---

305 *Id.* at 494.
306 *Id.*
307 *Id.*
308 *Id.*
309 *Id.*
310 *Id.*
311 *Id.*
312 *Id.*
313 *See id.* at 494-95.
314 *Id.* at 488.
315 *Id.*

vidual awareness of privacy interests and expectations.[316] The EU Data Directive and Canadian PIPEDA address imperfections in the database-driven information markets worldwide and are models for improving database-driven information systems in the United States.[317]

Thus, the EU Data Directive and Canadian PIPEDA offer practical privacy frameworks because they provide workable definitions of database-driven activities and ensure affirmative rights for an individual's right to privacy.[318] A U.S. data privacy statute would provide comprehensive protection for individuals by establishing across-the-board regulatory expectations for the federal government, states, corporations, and individuals.[319] The implementation of such a statute would also address the various weaknesses and inconsistencies that currently exist in federal and state data privacy laws.[320]

A U.S. data privacy statute would protect individuals against the weak Supreme Court interpretations of the Fourth Amendment and expand privacy protections to the private sector.[321] Courts would benefit from a U.S. data privacy statute that moves away from the out-dated theories regarding the right to privacy, and establishing a statutory scheme that clearly expresses a data protection standard.[322] An omnibus statutory standard would comprehensively regulate the large database-driven information systems with efficiency, consistent guidance, and maximum coverage, without imposing too harsh a burden on the aggregators of information.[323]

CONCLUSION

The U.S. should embrace a properly adapted version of the EU Directive and Canadian PIPEDA because increased utilization of database-driven information systems in the casino industry requires new legislation to improve the organizational security of personal data. A uniform, nationwide privacy policy will not only benefit the casino industry, but all commercial, government, and group enterprises that utilize information markets. A comprehensive U.S. privacy statute would address harmful imperfections in our privacy laws, recognize an affirmative right to data privacy, and revive an expectation of privacy within individuals; an expectation currently weakened by the actions of both the Supreme Court and Congress.

A comprehensive U.S. data privacy statute is the best way to restore individual privacy rights and bolster the long-term viability of database-driven information systems in the casino industry and in all U.S. business commerce. The statute should include improved data accuracy requirements, notice and consent requirements, and appropriate measures to transfer the risk back to the entities responsible for casino database system control in order to better deal

316 *Id.*
317 *Id.*
318 *Id.* at 495.
319 *Id.*
320 *Id.*
321 *Id.*
322 *Id.*
323 *Id.*

with data theft and misuse. These provisions will ensure viable and robust database-driven information systems for the future, ultimately benefiting the data brokerage industry, the government, and corporate interests (including casino corporations), and promote greater individual participation in database-driven PII systems.