THE EVOLUTION OF CYBER RISK: What Your Clients Need to Know

By Cassie Stratford & Theresa Guerra

By 2018, every gaming operator has come to terms with the fact that technology has had, and will continue to have, a remarkable impact on our industry. While some of the basics have not changed, the way services are offered, the way we learn about customers, and the way our industry is regulated have all been significantly impacted by advances in technology. Along with these exciting developments has come the need for businesses in our industry to understand the risks related to some of these technological advances and the emerging laws and regulations that are sure to continue to develop.

From an operational perspective, many of today's trends seem to have shifted heavily toward refining and customizing the overall guest experience to attract and retain customers. It is nearly impossible to discuss the current state of the gaming industry without some mention of how customer data is shaping marketing initiatives, analytics, and operational efficiencies or the newest technology offerings that promise increased customer interaction and engagement. A detailed and data-driven understanding of what specific offerings will appeal to each guest is critical. But with this increasing volume of data, comes the potential for serious consequences if your clients are not advised about cyber risks and how to mitigate them while driving business in today's market.

This article will highlight a few high-risk issues that gaming attorneys should be familiar with so they can help their clients identify them and, where appropriate, recommend further consultation with specialized counsel. Specifically, this article covers: (1) the recent changes following the European Union's General Data Protection Regulations; (2) the implications of customer and employee data collection; (3) third-party data sharing, and; (4) laws and regulations concerning data breach protocol.

General Data Protection Regulations

One of the more recent changes of international significance came on May 25, 2018, the effective date of the General Data Protection Regulations of the European Union, commonly referred to as GDPR. GDPR has received attention across a variety of industries, likely because it imposes some very challenging obligations, contemplates the possibility of staggering fines, and includes the potential for extremely broad application, even to international businesses that may not have a large European presence. GDPR, by its own terms, applies to all companies that hold data of individuals within the European Union, meaning that the law potentially reaches a broad range of U.S. companies, including large gaming companies that may have a significant international customer base.[1]

Although the EU has garnered attention as one of the first to institute a data protection law with such a huge potential reach, many U.S. states appear likely to follow suit. California recently signed into law fairly similar legislation titled the California Consumer Privacy Act of 2018 (the "Act") which will go into effect January 1, 2020.[2] The Act is akin to GDPR because it requires companies to be transparent and disclose to consumers how data is collected, processed, and to whom it is sold.[3] The law also includes a "right to be forgotten" and

affirmative consent requirements, however these aspects are somewhat more limited than the GDPR.[4] Indeed, California's new Act and increasing legislation in other states indicate that state and federal laws in the U.S. will continue to develop on this topic.[5] By staying generally familiar with these new laws and regulations you can help your clients proactively consider these potential requirements as they evaluate and implement any new initiatives that relate to the collection and usage of data. This may somewhat ease the challenges related to subsequently being required to become compliant as the scope of these regulations expand.

Customer and Employee Data

When it comes to collecting data from both customers and employees, many high-risk areas can be addressed by advising your clients to understand and consider all points of capture, related consent language, and applicable privacy policies. Aside from the increasing levels of customer data discussed above, in the employment context, gaming entities may have unusually large levels of data as well. In addition to the traditional employee personal information that virtually all employers collect and maintain, gaming entities often have information related to heightened background investigation obligations, tracking of gaming permits and licenses, and for key licensees. Thus, for gaming companies, the amount of personal data is likely to be somewhat uniquely voluminous, creating a greater need to take appropriate steps to mitigate the associated risks.

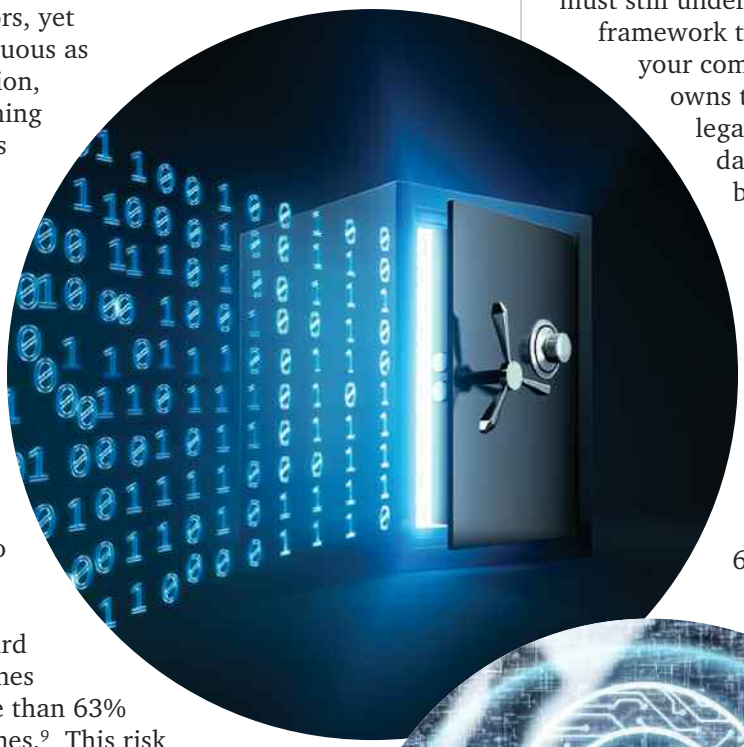
The first thing clients should consider is the point of capture or where they are obtaining personal data. Obvious points of capture include when a customer joins a loyalty program or when an employee joins the company. But as marketing and human resources teams creatively expand on how they interact with customers and employees, these points of capture can vary and the teams implementing these changes may not appreciate the critical nature of a consistent capture process. These points of capture could be via iPad-carrying marketing representatives at special events, recruiters collecting potential candidate information at job fairs, as part of a box office sales process, or via app-based non-gaming offerings. The possibilities are endless, and each point of capture may involve different information and different associated risks related to the security of that data, as well as the way it is used by the company.

The next important aspect to understand is consent language. While it may be widely understood that traditional website data capture must include appropriate consents, it is important to consider how to ensure appropriate consents each time this type of data is gathered—even during those in-person interactions where the customer is verbally providing data. If the data is making its way into any sort of database, the appropriate consents related to its use must be obtained and in many instances this consent must be confirmed in writing. Creating ongoing dialogue around the various points of capture can avoid improper collection and storage of data that was not obtained with appropriate consents. Maintaining a consistent approach to consent obtained at each point of capture will mitigate certain data related risks and may also help consistently ensure that your client is complying with various marking related laws as well.[6]

Finally, clients should schedule routine reviews of their privacy policy. The policy must always accurately reflect, among other things, how customer data is tracked and used, which will certainly change over time. Engaging in an open and ongoing dialogue with their marketing teams can help clients ensure that their privacy policy stays accurate and up to date. Gathering information around basic practices, as well as less obvious marketing activity like the use of tools that assist in behavioral and preference tracking, is the key to these conversations. Appropriately disclosing this type of activity can avoid unnecessary additional risk in this context.[7]

Third-Party Data Sharing

Many clients may not necessarily think they are "sharing" data with third parties if they are not directly partnering with companies that independently utilize the data. However, many of today's operational and analytics tools rely on cloud-based, subscription software, and many technology tools involve integration with third-party providers that must access certain data to provide their service. Some examples include the more obvious credit reporting agencies and marketing vendors, yet vendors as innocuous as heating, ventilation, and air conditioning (HVAC) suppliers may have access to company data.[8]



Third-party vendors with access to data, particularly those without sophisticated data security systems, pose a significant risk to clients. Indeed, one survey indicates that third party data breaches account for more than 63% of all data breaches.[9] This risk may be the most difficult to mitigate because the data is outside of your client's environment and control. However, there are important steps to take that can protect against these very real threats. First, make sure your clients understand which vendors may have access to data and that their data security personnel carefully reviews the security posture of these vendors before they are engaged. Further, ensure that the applicable contract allows for ongoing security review and that your clients are aware of and comfortable with how risks around data breaches are allocated, including how limits of liability would apply to those scenarios. Finally, if your client carries cyber insurance coverage, you should encourage them to confirm whether coverage would apply in the event data is compromised by way of a third-party service provider (as well as any other critical conditions of coverage, including time restrictions for claims reporting).

Another important third-party player to understand is third-party data storage. If your client outsources data storage, they should be familiar with the basics of the storage company's structure. Your client's contract with its data storage company should take into account: (1) how quickly and how often your client needs to access the data; (2) how long your client needs to retain the data; (3) how secure your client requires the data to be; and (4) what regulatory requirements bind your client.[10] Additionally, it is important to remember that entities that turn to third-party storage providers still have a high level of responsibility over data storage and security. Even if your client uses a third-party to store and protect data, you should remind them that they must still understand the basics of what type of storage framework the vendor uses and what kind of data your company is storing. Ultimately, the party that owns the data carries serious reputational and legal risks related to a breach involving that data, even if it occurs as a result of a data breach of the third-party storage vendor.

Laws and Regulations Concerning Data Breach Protocol

Finally, there are an increasing number of laws and regulations around data security. Like any business, your clients must comply with federal and state laws surrounding data "breach" events. NRS 603A.020 defines a "breach of the data security of the system data" broadly as "unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the data collector."[11] In addition, most gaming jurisdictions now have, at a minimum, self-reporting obligations in the event of a "breach" scenario.[12] Specifically, Nevada requires data collectors to disclose data breaches "in the most expedient time possible and without unreasonable delay" to state residents whose data is reasonably believed to have been compromised.[13] Nevada also specifies which methods of notification are appropriate and which standards each method must meet.[14]

Additionally, the Nevada Gaming Control Board (the "Board") lays out regulations for data security in its Minimum Internal Control Standards ("MICS"). The Information Technology MICS require gaming companies to, among other things, notify patrons of privacy policies, protect personally identifiable information, and maintain

secure firewalls and routers. Importantly, each gaming company must demonstrate that it has a notification process to inform the Board's Enforcement Division in the event of a breach.[16] Your clients should be advised of these laws and regulations and further advised to seek specialized counsel to formulate appropriate incident response plans that address these unique gaming regulatory obligations. If your client is publicly traded, they should also be counseled as to SEC regulations on the issue.

We live in a thrilling age where rapid technological advances are the new norm, allowing our operators to constantly refine the customer experience in not only gaming offerings, but also in terms of the overall entertainment experience. Along with that comes a need to carefully monitor the legal and compliance related risk so your clients are best prepared to avoid potentially staggering fines, class action lawsuits, and disastrous reputational damage that could result in the event of a data breach or fines related to non-compliant practices.

Gaming lawyers can add significant value simply by assisting their clients in identifying some of the key risks specific to gaming clients and data security. This will best position your clients to make well-informed decisions about where and when it may be necessary to engage additional specialized counsel to ensure on-going compliance with laws and regulations that are certain to continue to develop in this exciting age of technology.

Cassie Stratford is Vice President of Legal Affairs and Assistant General Counsel for Boyd Gaming Corporation (NYSE: BYD), where she provides legal support for a wide variety of corporate and operational functions, including various technology and data security related initiatives.

Theresa Guerra is a JD candidate in the Class of 2019 at William S. Boyd School of Law, University of Nevada, Las Vegas where she is a member of the Society of Advocates moot court team and is an Articles Editor for the Gaming Law Journal.

[1] *See* Ivana Kottosova, *GDPR is Here: What You Need to Know About Europe's New Data Law*, CNNTECH, May 24, 2018, http://money.cnn.com/2018/05/24/technology/gdpr-eu-rollout/index.html.

[2] *Id.*

[3] *See* Eversheds Sutherland, *Legal Alert: California's GDPR Has Become Law*, June 29, 2018, https://us.eversheds-sutherland.com/NewsCommentary/Legal-Alerts/212630/Legal-Alert-Californias-GDPR-has-become-law.

[4] *See id.*

[5] California is not alone in its efforts to update its data security laws. In 2017, five other states, New York, Maryland, Indiana, New Mexico, and Alabama introduced more comprehensive data security bills. *See* Douglas Kelly, *Five States Introduce New Data Security Laws*, LAWROOM, Mar. 7, 2017, http://blog.lawroom.com/data-security/five-states-introduce-new-data-security-laws/. As of today, all fifty states have some form of legislation governing what happens in the event of a data security breach. *See* National Conference of State Legislatures, *Security Breach Notification Laws*, National Conference of State Legislatures, Mar. 29, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#1.

[6] The Telephone Consumer Protection Act, for example, sets out specific consent language for telephone-based marketing such as requiring the consumer to indicate that he or she is authorizing telemarketing and acknowledging that he or she is not required to sign the agreement as a condition of purchasing goods or services. *See* Alan S. Kaplinsky et. al., *FCC Issues Citations for Violations of TCPA Consent Requirement for Autodialed or Prerecorded Telemarketing Calls*, Ballard Spahr LLP, Sept. 21, 2015, https://www.ballardspahr.com/alertspublications/legalalerts/2015-09-21-fcc-issues-citations-violations-tcpa-consent-require-auto-prerecord-telemarketing-calls.aspx. The Telephone Consumer Protection Act is codified at 47 U.S.C. § 227.

[7] Specifically, Nevada has enacted Senate Bill 538, which requires websites or online services that collect personal information to disclose how that data is used to their consumers. California, Delaware, and Connecticut have also beefed up their privacy policy requirements. *See* National Conference of State Legislatures, *State Laws Related to Internet Privacy*, National Conference of State Legislatures, Mar. 26, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

[8] *See* Tara Seals, *Home Depot: Massive Breach Happened Via Third-Party Vendor Credentials*, Info Security Magazine, https://www.infosecurity-magazine.com/news/home-depot-breach-third-party/ (last accessed May 20, 2018).

[9] *See* Mahmood Sher-Jan, *Surprising Stats on Third-Party Vendor Risk and Breach Likelihood*, The Privacy Advisor, Aug. 21, 2017, https://iapp.org/news/a/surprising-stats-on-third-party-vendor-risk-and-breach-likelihood/.

[10] *See* Jennifer Lonoff Schiff, *14 Things you Need to Know About Data Storage Management*, CIO, Sept. 11, 2013, 8:00 AM, https://www.cio.com/article/2382585/virtualization/14-things-you-need-to-know-about-data-storage-management.html.

[11] Nev. Rev. Stat. § 603A.020.

[12] California gaming entities can find notice requirements under Cal. Code Regs. tit. 4, §§ 12290(c)(2) and Cal. Civ. Code § 1798.29. Hawaii gaming entities can find notice requirements under Haw. Rev. Stat. § 487N-2. Illinois gaming entities can find notice requirements under 815 Ill. Comp. Stat. § 530/10. Indiana gaming entities can find notice requirements under Ind. Code § 4-1-11. Iowa gaming entities can find notice requirements under Iowa Code § 715C.2. Kansas gaming entities can find notice requirements under Kan. Stat. § 50-7a02. Louisiana gaming entities can find notice requirements under La. Rev. Stat § 51:3074. Mississippi gaming entities can find notice requirements under Miss. Code § 75-24-29. Nevada gaming entities can find notice requirements under The Nevada Gaming Control Board's Minimum Internal Control Standard 46 or Nev. Rev. Stat. § 603A.220. Missouri gaming entities can find notice requirements under Mo. Rev. Stat. § 407.1500. Ohio gaming entities can find notice requirements under Ohio Rev. Code. § 1349.19. Pennsylvania gaming entities can find notice requirements under 73 Pa. Cons. Stat. § 2303.

[13] Nev. Rev. Stat. § 603A.220

[14] *Id*. § 603A.220

[15] *See* Nev. Gaming Control Board, Minimum Internal Control Standards: Information Technology, 12–14 (Version 8, Jan. 1, 2018).

[16] *See id*. at 14.