AERSTONE

Hospitality Industry Privacy Whitepaper

Presented by Jason Winder & Greg Levine

Table of Contents

1.0. INTRODUCTION

By the end of 2013, the hotel industry had become a $163 billion industry in the United States alone – including more than 52 thousand properties, just over 4.9 million guest rooms, and an average occupancy rate of 62%.[1] Without any doubt, the hospitality industry is incredibly competitive, and in order to attract and retain patronage, it's an industry that thrives on customer service and personalization. This combination of competitiveness and customization has inevitably led the players in this industry to collect enormous amounts of information on their guests, so that they can both encourage and personalize their guests' stays. Especially in the upper-end properties, it's become clear that a higher touch leads to more return business.

Alongside the growing attempt to collect information, there is a growing public concern that the data being collected might lead to an invasion of personal privacy, or in worst-case scenarios, identity theft. In a survey performed by Deloitte of 1000 frequent travelers, 76% stated that they worry about online security breaches, while only 33% indicated that they believed their information to be secure.[2] Noting that there were approximately 2 billion domestic person trips (business and leisure) in 2013, according to the U.S. Travel Association[3], one may conclude that a tremendous number of travelers believe their personal data to be at risk – a concern that reaches all the way to the highest corridors of political power.

2.0. MAPPING THE PROBLEM

The risk of a guest's personal information falling into the hands of an unauthorized actor can lead to more serious issues than just a stolen credit card number, or even identity theft. Any personal data collected may have value from many angles, including corporate espionage, blackmail, or identity theft. Note that this is not to imply that national hotel chains might use stored information in this manner; the risk is what might happen when (and not "if") this information falls into the wrong hands.

In terms of what kind of information is in play, we note that hospitality providers are in a unique position to collect an enormous amount of data on hotel guests, including personally identifiable information ("PII"), signals intelligence ("SIGINT"), human intelligence ("HUMINT"), and geospatial intelligence ("GEOINT")

2.1. PERSONALLY IDENTIFIABLE INFORMATION (PII)

Hotels routinely gather significant amounts of PII on their guests, at several stages of the guest's stay:

- At Reservation Time. Information gathered at reservation time usually includes data like name, address, phone number and email address – and may include other information, such as nationality or age. Most properties additionally require a credit card number to secure a room reservation. Some larger companies allow guests to keep credit card numbers on file, to facilitate future reservation making. These data may or may not be stored securely, which presents a challenge in terms of both data at rest and data in motion.

[1] http://www.ahla.com/content.aspx?id=36332
[2] http://www.latimes.com/business/la-fi-travelers-worry-about-data-breach-20140926-story.html
[3] http://www.ustravel.org/sites/default/files/page/2010/12/ForecastSummary_5152014.pdf

- During Check-In. Information gathered at check-in may include a passport number, make and model of car, license plate number, handwriting samples, etc. – as well as any observable personal characteristics. Most properties also require a credit card at check-in, to cover damage and incidentals, or fast checkout. This card may be processed electronically, or a paper imprint may be taken – either option presenting risks of credit card skimming, as well as manual capture of credit card numbers. In the future, guests may have the option to opt-in for facial recognition, so staff will be alerted and can greet guests on a more personal level – while also creating a risk specific to safeguarding stored biometric data.[4]
- During the Stay. A wide variety of other personal characteristics and behaviors can be ascertained in passing by hotel staff throughout a guest's stay, including sex, race, age, ethnicity, disability, likes and dislikes, personality, etc. Personal health information (PHA) might also be gathered through a variety of means, and new technologies, like Amazon's Alexa for Hospitality[5], may further facilitate unknowing data collection and storage.

2.2. SIGNALS INTELLIGENCE (SIGINT)

Signals Intelligence ("SIGINT") is intelligence-gathering by interception of signals, whether communications between people (i.e., communications intelligence, or "COMINT") or from electronic signals not directly used in communication (i.e., electronic intelligence, or "ELINT"). Hotels are in an excellent position to gather a substantial amount of SIGINT on hotel guests, for example:

- Hotels may store the metadata of phone calls placed using room phones, and may record entire conversations or retain voicemail messages;
- Hotels may monitor rooms electronically;
- Hotels may intercept and retain downloaded email;
- Hotels may proxy SSL tunnels, and intercept secure communications;
- Hotels may archive personal documents, including files downloaded or printed, or faxes sent or received;
- Hotels may store public area surveillance video and photographs; and
- Hotels may retain a record of websites visited, and movies rented.

2.3. HUMAN INTELLIGENCE (HUMINT)

Human Intelligence ("HUMINT") is intelligence gathered by means of interpersonal contact. Hotels are ideally suited to gather an extraordinary amount of HUMINT on hotel guests, either in person or via CCTV, including (for example):

[4] https://vulcanpost.com/56461/guests-check-hotels-facial-recognition-next-big-thing/ https://vulcanpost.com/56461/guests-check-hotels-facial-recognition-next-big-thing/ https://www.usatoday.com/story/travel/roadwarriorvoices/2015/09/15/facial-recognition-tech-is-set-to-keep-an-eye-on-hotel-guests/83328668/

[5] https://www.usatoday.com/story/travel/hotels/2018/06/20/amazon-has-new-alexa-hotels-new-way-order-room-service/716900002/

- What guests eat and drink
- Whether guests smoke or drink alcohol, and how much
- Who guests meet with, and for how long
- Who guests bring to their rooms
- When guests leave and arrive
- Where guests go within the hotel and when
- How long and how frequently guests stay
- What guests wear
- What guests purchase
- How much guests tip
- Whether guests gamble, and how much
- Whether guests exercise, and how
- General personality traits
- General likes and dislikes

Due to the vast amount of information collected, these data could potentially be used in ways beyond just identify theft – for example, as part of hacking or blackmail schemes. In that regard, it's also worth mentioning that guests are frequently in a position to gather much of the same HUMINT on other guests, which raises an interesting question about hotel liability.

2.4. GEOSPATIAL INTELLIGENCE (GEOINT)

With intimate knowledge of guest comings and goings, and noting the proliferation of mobile check-in apps, guest movements can easily be tracked. This risk is further underscored by the existence of frequent-traveler loyalty programs, which make guests more likely to stay within a particular hotel chain's network of properties. This makes it possible to map guest activities in a way that may support additional GEOINT analysis of customer movements, to further bolster SIGINT or HUMINT data.

Add the fact that hotels can also capture a guest's home address during reservation or check-in time, and an alarming picture of guest movements starts to come into focus.

In a more recent twist, some hotel brands are beginning to pilot the use of a mobile application for both check-in and room access. Depending on how such an app is designed, and the GPS location settings on the phone itself, such an app might allow the hotel to track a guest's location both inside and outside of the hotel, for as long as the app is left running.

3.0. THE REGULATIONS

There are no government regulations that apply directly to the hotel industry, in terms of safeguarding guest data. And whereas the American Hotel & Lodging Association (AH&LA) enforces self-regulation of

many aspects of the hotel industry, these regulations typically fall into one of three main categories, none of which specifically addresses guest privacy:

- Engineering and environmental issues, via the Engineering and Environment Committee
- Health, safety, and security issues, via the Loss Prevention Committee
- Issues affecting insurance rates for the lodging industry, via the Risk Management Committee

There are also third-party regulations such as Payment Card Industry Data Security Standard (PCI DSS) that cover the safeguarding of credit card information. Specifically missing from any of these regulations, however, is standard guidance specific to guest privacy. And although it's true that many large hotel brands post extensive privacy policies on their websites, and provide some civil recourse for violations, these policies do not always fully articulate the breadth and depth of information collected, nor do most policies adequately address how data are stored and protected.

The European Union General Data Protection Regulation (GDPR), which took effect in May of 2018, and is specifically designed to strengthen and unify data protection and privacy for all citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data, and to simplify the regulatory environment for international business by unifying the regulation within the EU. Non-EU companies should be aware that they must comply with GDPR regulations if they offer services to EU citizens. This is especially true and enforceable if they do business in EU member countries, which is certainly true of most large American hotel brands, and which could face exceptionally hefty fines for non-compliance (4% of annual global revenue, up to €20 Million). GDPR compliance is still in the process of being codified, however basic compliance requires:

- Data protection by design and by default. Data protection measures must be designed into the development of business processes for products and services.
- Right of Access. This conveys consumers' right to access their personal data and information about how this personal data is being processed.
- Right to Erasure. This guarantees the right to request erasure of personal data on any one of a number of grounds within 30 days of the request.

4.0. IN CONCLUSION

Aerstone believes that the hospitality industry should take the lead on developing its own regulations for guest privacy, in advance of the inevitable government oversight in this area. Current regulations are weak--to-nonexistent and rely on the requirements of different organizations and standards, which presents a liability for hotels operating in a gray area of privacy protection. New European Union (EU) General Data Protection Regulation[6] (GDPR) privacy requirements almost certainly applies to hotels worldwide, however it's too early to understand the legal implications of these regulations for the U.S. hospitality market.

Ultimately, we believe that the first hotels that implement robust privacy standards will have a market advantage over hotels that don't, which may prove especially important in attracting the highly desirable

[6] https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation

and lucrative business traveler market. We further believe that the go-forward path is for the AH&LA to develop a privacy standard similar to the standards that regulate other industries, such a HIPAA (in the healthcare industry) or FERPA (in the education industry). This hotel privacy standard should include a limited number of security controls, against which hotels should be periodically audited by an independent third-party assessor.

It is understood that guest privacy may occasionally have to be violated due to health concerns, hotel security, public safety, or for necessary maintenance – although it's worth mentioning that some lawsuits have already been filed in the United States, because of hotel privacy violations that went beyond any expected safety issues. An example of this involved ESPN sports reporter Erin Andrews, who was allegedly videotaped in secret by another guest in an adjoining room, which led to a negligence suit against Marriott, and ultimately resulted in a $55M award.[7] In another recent case, a shareholder filed suit against the Wyndham Worldwide Corporation, alleging they "failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner" after its site suffered three breaches between 2008 and 2010.[8] In a similar case, the Federal Trade Commission (FTC) recently filed suit against Wyndham for its failure to protect customer data on the same basis, in violation of its own stated privacy policy.[9]

Some of these cases are still ongoing, and their outcomes are uncertain, however it is certain that similar cases are sure to follow, as awareness over privacy concerns continues to receive heightened attention in the press and in popular culture. One interesting an unanswered question is the tradeoff between security and safety, and customer privacy. In the wake of the 2017 shooting on the Las Vegas Strip, some hotels are now scanning bags and using predictive behavior analytics that some people may deem personally intrusive.[10] At the least, such cases – along with the raised awareness of how much data is actually being collected – represents negative publicity, which may damage room occupancy rates for hotels that do not take a strong and compelling stance on the protection of guest privacy.

5.0. ABOUT AERSTONE

Aerstone is a service-disabled veteran-owned small business (SDVOSB) that provides subject matter expertise and software development services in the field of advanced cybersecurity. We are also a certified vulnerability assessor under the NSA's NSCAP CIRA program – one of just five companies in the world. Our products and services touch all aspects of cybersecurity, including architecture, systems design, software development, training, assessment, and forensics.

[7] http://money.cnn.com/2016/04/25/media/erin-andrews-hotel-settlement/index.html
[8] https://www.reuters.com/article/us-wyndham-ftc-cybersecurity/wyndham-settles-ftc-data-breach-charges-idUSKBN0TS24220151209
[9] https://www.washingtonpost.com/business/economy/2012/06/26/gJQATDUB5V_story.html?noredirect=on&utm_term=.2a0da0523c6a
[10] http://www.travelandleisure.com/travel-tips/travel-warnings/hotel-security-future-las-vegas

6.0. REFERENCES

- 2013 Lodging Industry Profile, Prepared by the American Hotel & Lodging Association http://www.ahla.com/content.aspx?id=36332.
- Brooks, Matt (December 7, 2011). ESPN reporter Erin Andrews refiles $10 million lawsuit in peephole videotape incident. Obtained on August 12, 2014 from http://www.washingtonpost.com/blogs/early-lead/post/espn-reporter-erinandrews-files-10-million-lawsuit-in-peephole-videotapeincident/2011/12/07/gIQAaIWAdO_blog.html.
- Martin, Hugo (September 28, 2014). Travelers worry about data breach from loyalty programs, survey finds. Obtained on October 2, 2014 from http://www.latimes.com/business/la-fi-travelers-worry-about-data-breach-20140926-story.html.
- Mayerowitz, Scott (November 2, 2014). Skip Check-In; Latest Hotel Room Key is Your Phone. Obtained on November 3, 2014 from http://www.msn.com/enus/news/corner-office/skip-check-in-latest-hotel-room-key-is-your-phone/ar-BBcF2gJ.
- McGarvey, Robert (October 6, 2014). 10 Biggest Data Breaches of 2014 (So Far). Obtained on October 15 from http://www.cutimes.com/2014/10/06/10-biggest-databreaches-of-2014-so-far?page=2.
- Miller, Jason (June 11, 2012). Do Not Disturb: Fourth Amendment Expectations Of Privacy In Hotel Rooms. Obtained on August 12, 2014 from http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1048&context=circuit_review.
- Robinson, Teri (May 7, 2014). Shareholder sues Wyndham board members over data breaches. Obtained on August 12, 2014 from http://www.scmagazine.com/shareholder-sues-wyndham-board-members-overdata-breaches/article/345989/.
- Summary of Articles contained in the GDPR. Obtained on October 30, 2017 from http://www.eugdpr.org/article-summaries.html.
- Trejos, Nancy (June 20, 2018). Amazon has developed a new Alexa for hotels; Marriott and others are testing it out. Obtained on June 28, 2018 from https://www.usatoday.com/story/travel/hotels/2018/06/20/amazon-has-new-alexa-hotels-new-way-order-room-service/716900002/.
- Galdies, Peter. A Summary of the EU General Data Protection Regulation. Obtained on June 28, 2018 from https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation.
- GDPR FAQs. Obtained on May 13, 2019 from https://eugdpr.org/the-regulation/gdpr-faqs/.