

**UNITED STATES OF AMERICA  
BEFORE THE NATIONAL LABOR RELATIONS BOARD**

**INTERSTATE MANAGEMENT COMPANY, Case 28-CA-206663  
L.L.C. as agent for BRE NEWTON HOTELS  
PROPERTY OWNER, LLC d/b/a RESIDENCE  
INN BY MARRIOTT SANTA FE ALL-SUITES  
HOTEL**

**and**

**RESIDENCE MARRIOTT COMMITTEE**

**RESPONDENT'S BRIEF IN SUPPORT OF EXCEPTIONS  
TO ADMINISTRATIVE LAW JUDGE'S DECISION**

**TABLE OF CONTENTS**

- I. INTRODUCTION.....1
- II. STATEMENT OF THE CASE.....1
  - A. Background.....1
  - B. Respondent’s Business Code of Conduct .....2
    - 1. The Information Protection Policy Does Not Prevent Employees from Sharing Their Own Information or Otherwise Engaging in Protected Activity .....2
    - 2. The Government Investigations Policy Does Not Govern Employees’ Personal Interactions with Government Agencies and Does Not Otherwise Restrict Protected Activity.....5
    - 3. Respondent Communicates Employees’ Protected Rights .....7
- III. QUESTIONS PRESENTED .....8
- IV. THE ALJ ERRED BY CONCLUDING THAT RESPONDENT’S INFORMATION PROTECTION AND GOVERNMENT INVESTIGATIONS POLICIES VIOLATE SECTION 8(A)(1) OF THE ACT .....9
  - A. The Information Protection Policy Does Not Interfere with or Prohibit Employees from Disclosing Information About Themselves or Information About Other Employees That Was Lawfully Obtained.....11
    - 1. The Information Protection Policy, When Reasonably Construed, Is Lawful .....11
    - 2. The ALJ Incorrectly Disregarded Respondent’s Legitimate Business Justifications for its Information Protection Policy and Improperly Advocated for a More “Narrowly Tailored” Policy.....19
  - B. The Government Investigations Policy Does Not Interfere with or Prohibit Employees from Participating in Government Investigations, Including Those of the NLRB.....23
    - 1. The Government Investigations Policy, When Reasonably Construed, Is Lawful.....23
    - 2. The ALJ Incorrectly Disregarded Respondent’s Legitimate Business Justifications for its Government Investigations Policy and Improperly Advocated for a More “Narrowly Tailored” Policy .....27
- V. CONCLUSION .....31

**TABLE OF AUTHORITIES**

**Statutes**

5 U.S.C. § 552(b)(6). .....20

5 U.S.C. § 552a.....20

15 U.S.C. §§ 6101(3)-(4). .....20

15 U.S.C. §§ 7701-7713 .....20

29 U.S.C. § 157..... passim

Cal. Civ. Code § 1798.29(a). .....20

Cal. Civ. Code § 1798.82(a). .....20

Cal. Govt. Code §§ 7285.1-2 .....7, 29

Cal. Lab. Code § 90.2 .....7, 29

Los Angeles Municipal Code § 11.00(m).....28

Los Angeles Municipal Code § 41.49(2).....28

N.M. Stat. § 30-16-24.1(A)-(D).....20

N.M. Stat. §§ 57-12C-1 through 57-12C-12.....19

**U.S. Supreme Court Decisions**

*City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015). .....27, 28

*Nash v. Florida Industrial Commission*, 389 U.S. 235 (1967).....25

*Robbins Tire & Rubber Co.*, 437 U.S. 214 (1978) .....25

*United States Dep’t of Defense v. FLRA*, 510 U.S. 487 (1994).....20

**U.S. Federal Court of Appeals Decisions**

*Community Hosp. of Cent. Cal. v. NLRB*, 335 F.3d 1079 (D.C. Cir. 2003) .....18

*Reed v. NLRB*, 927 F.2d 1249 (D.C. Cir. 1991) .....20

**National Labor Relations Board Decisions**

*Ark Las Vegas Restaurant Corp.*, 335 NLRB 1284 (2001). .....11, 12

<i>Copper River of Boiling Springs, LLC</i> , 360 NLRB 459 (2014) .....	17
<i>DirecTV</i> , 359 NLRB 545 (2013) .....	24
<i>Gray Flooring</i> , 212 NLRB 668, 674 (1974).....	14, 15
<i>International Business Machines Corp.</i> , 265 NLRB 638 (1982) .....	16
<i>Laidlaw Transit, Inc.</i> , 315 NLRB 79 (1994) .....	25
<i>Lutheran Heritage Village-Levonina</i> , 343 NLRB 646 (2004) .....	25
<i>Macy’s, Inc.</i> , 365 NLRB No. 116 (2017) .....	15, 16, 24
<i>Mediaone of Greater Florida</i> , 340 NLRB 277 (2003). .....	17
<i>Metro Health Foundation, Inc.</i> , 338 NLRB 802 (2003).....	19
<i>Minteq Int’l, Inc.</i> , 364 NLRB No. 63 (2016) .....	12, 13
<i>Ridgley Mfg. Co.</i> , 207 NLRB 193 (1973).....	14, 15, 16
<i>Safeway, Inc.</i> , 338 NLRB 525 (2002).....	15
<i>The Boeing Company</i> , 365 NLRB No. 154 (2017).....	passim
<i>Troy Hills Nursing Home</i> , 326 NLRB 1465 (1998). .....	19

**Administrative Law Judge Decisions**

<i>Blue Man Las Vegas LLC</i> , Case 28-CA-21126, 2008 NLRB LEXIS 225 (NLRB Div. of Judges, July 18, 2008).....	24, 27
<i>Legacy Charter</i> , 28-CA-201248, 2018 NLRB LEXIS 338 (NLRB Div. of Judges, Aug. 16, 2018) .....	16
<i>The Kroger Co of Michigan</i> , Case 07-CA-098566, 2014 NLRB LEXIS 279 (NLRB Div. of Judges, Apr. 22, 2014).....	27

**Regulations**

NLRB DIVISION OF JUDGES, BENCH BOOK § 12-800 (Jan. 2018).....	21
---	----

**Websites**

<a href="http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx">http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx</a> .....	19
<a href="https://apps.nlr.gov/eservice/efileterm.aspx">https://apps.nlr.gov/eservice/efileterm.aspx</a> .....	21

[https://www.osha.gov/recordkeeping/finalrule/finalrule\\_faq.html](https://www.osha.gov/recordkeeping/finalrule/finalrule_faq.html).....21

**Other Authorities**

General Counsel Memorandum 18-04, at 11 (Jun. 6, 2018).....16, 22

## **I. INTRODUCTION**

Despite the undisputed evidence and testimony provided by Respondent Interstate Management Company L.L.C. (Employer) as agent for BRE Newton Hotels Property Owner, LLC d/b/a Residence Inn by Marriott Santa Fe All-Suites Hotel (Hotel) and the Board's revised standard for evaluating facially neutral employer rules, Administrative Law Judge John T. Giannopoulos (ALJ) reached the erroneous conclusion that two of Respondent's Business Code of Conduct and Ethics (Code) policies violate Section 8(a)(1) of the Act. To reach this conclusion, the ALJ threw logic and reasonableness into the wind and paid only lip service to *The Boeing Company*.<sup>1</sup> In reaching this decision, the ALJ continued to apply a muddled and ambiguous standard which ultimately resulted in the impermissible conclusion that Respondent's policies should be more "narrowly tailored."

## **II. STATEMENT OF THE CASE**

### **A. Background**

This case originated from a charge, and amendments thereto, filed by the Residence Marriott Committee. The initial allegations related to a meeting Respondent's corporate director of human resources, Yamini Shankar, had with three employees at the Hotel on August 30, 2017, as well as various other Section 8(a)(1) and (3) allegations raised by the same three employees. (GX 1(a))<sup>2</sup> After the Regional Director found no merit to most of the allegations (RX 5), the charge was amended to include allegations challenging the Code and Respondent's Employee Handbook. (GX 1(c), (e)) The allegations concerning the Handbook were withdrawn by the General Counsel

---

<sup>1</sup> *The Boeing Company*, 365 NLRB No. 154 (2017).

<sup>2</sup> References to the Administrative Law Judge's Decision are cited herein as "ALJD" followed by the page number(s) and line number(s). General Counsel exhibits are cited herein as "GX" followed by the number(s). Respondent exhibits are cited herein as "RX" followed by the number(s). The Reporter's Transcript is cited herein as "T" followed by the page number(s).

at the commencement of the hearing. (GX 1(l)) Following the hearing and submission of post-hearing briefs, the ALJ dismissed the allegations relating to the August 30, 2017 meeting. (ALJD 21:45) Respondent's exceptions are directed toward the portions of the ALJ's decision addressing the Code.

**B. Respondent's Business Code of Conduct**

The Code is distributed to approximately 30,000 employees at 400 hotels in the United States. (ALJD 2:13-17; T 162, 177; GX 3) Joy Johnson, Respondent's vice president of compliance, is responsible for monitoring and ensuring that employees comply with applicable laws, policies, and procedures, including the Code. (T 162-63, 179; GX 3) She also assisted with drafting and revising the Code. (T 179)

**1. The Information Protection Policy Does Not Prevent Employees from Sharing Their Own Information or Otherwise Engaging in Protected Activity**

The ALJ found that the following Code provisions (in **bold**) violate Section 8(a)(1) of the Act.

**Section 6: Information Protection**

One of the Company's most valuable assets is information and the information systems we use to process and store that data. Keeping confidential our Company's non-public information is important to the success of our Company. **Confidential information includes, but is not limited to:**

- **personal information, which is defined broadly to include any information that can be associated with or traced to any information**, such as **the individual's name, address, telephone number, e-mail address**, bank and credit card information, social security number, etc. **The personal information covered by this Code could pertain to** a customer, potential customer, **associate, former associate**, owner or joint venture partner;
- information system user IDs, passwords, voice mail, and dial-up access numbers;

- proprietary information that provides our Company with an advantage over our competitors (e.g., email, financial systems, business intelligence site, development plans, revenue management techniques, etc.).

Every associate is responsible for utilizing the Company's information solely for authorized business purposes. In addition, every associate is responsible for protecting the Company's confidential information and information systems from unauthorized internal and external access.

(GX 1(g), 3, p. 3)

The Information Protection policy provides guidelines to protect confidential information, which includes information collected by Respondent from guests, employees, vendors, and other third parties and stored in Respondent's databases.<sup>3</sup> (T 164, 167) As the ALJ recognized, protection of such information is "necessary due to the Respondent's obligations under various state and/or federal laws involving data privacy." (ALJD 9:8-9; T 167, 171) The policy is also necessary to protect the personal safety of guests and employees. (ALJD 21:4-5; T 170)

Confidential guest information collected and stored by Respondent, which was given little weight by the ALJ,<sup>4</sup> includes each guest's name address, email address, brand rewards number, credit card information, and other information that hotels collect to do business, secure payment, and to communicate with the guest. (ALJD 20:10; T 164) Confidential employee information stored in Respondent's database includes each employee's name, address, email address, social security number, form I-9 information, tax information, bank account and payroll information, form W-2 information, health information, and information about employee dependents. (T 166-

---

<sup>3</sup> Respondent has not disciplined an employee for violating the Information Protection policy. (T 172)

<sup>4</sup> The ALJ specifically stated at the hearing, "Guests, I'm not interested in guests." (T 169)

67) Collectively, information covered by the policy is designated by Respondent as personally identifiable information (PII). (T 166-67)<sup>5</sup>

Contrary to the ALJ's finding, (ALJD 20:42-43), the policy does not prevent an employee from giving out his/her own information or information about other employees that is properly obtained. (T 167-68, 170-71) The ALJ misconstrued Johnson's testimony that "if [an employee's name] is tied to some other piece of information which could specifically identify the individual" then the name "would be considered confidential PII." (ALJD 9:21-24) Johnson testified that "if an associate wants to give out their own information, that's up to them what they give out" including information such as "name, address Social Security number, telephone number, email address." (T 171)

The Information Protection policy protects Respondent's legitimate business interests by prohibiting employees from downloading, collecting, using, or distributing PII obtained from Respondent's databases. (T 170-71) For example, if a human resources or payroll employee accessed another employee's PII in Respondent's databases and shared the PII with unauthorized persons, such conduct would violate the policy. (T 171) The Information Protection policy also prevents employees from sharing the PII in Respondent's database with a competitor.<sup>6</sup> (T 172) As Johnson explained, if an employee was involved in a domestic dispute and the perpetrator

---

<sup>5</sup> The "PII" designation is a specific term used by Respondent during its normal course of business to designate the type of confidential information protected by the Information Protection policy. (T 166-67) The term "PII" does not appear in the Code, as indicated by the ALJ. (ALJD 20:45-56, 21:1) However, it would be impossible for Respondent to include every single term of business lingo used by its employees throughout its 400 locations in the Code.

<sup>6</sup> The Information Protection policy protects the Respondent's business interest in its employees by preventing former managers from using information obtained from its databases to recruit Respondent's employees. (T 172) While this concern might be addressed by having employees or managers enter into non-compete agreements, Respondent does not use such agreements. (T 173)

attempted to obtain the employee's address or phone number from a hotel, the Information Protection policy would prohibit that information from being released. (T 170)

**2. *The Government Investigations Policy Does Not Govern Employees' Personal Interactions with Government Agencies and Does Not Otherwise Restrict Protected Activity***

The ALJ found that the following Code provisions (in ***bold***) violate Section 8(a)(1) of the Act.

**Section 16: Government Investigations**

We promote cooperation with law enforcement agencies and government agencies. However, rights of third parties, associates, customers, suppliers, and others may be affected. In most cases, the Company requires an official written request or a subpoena describing the requested information or documents and will ensure that the information requested is limited to information legitimately required for the agency's or party's purpose. ***Therefore, requests from the police, Internal Revenue Service and other regulatory authorities must not be answered without first obtaining clearance from our Legal Department.***<sup>7</sup>

(GX 1(g), 3, p. 6)

Contrary to the ALJ's conclusion, (ALJD 18:18-19), the Government Investigations policy provides guidance to employees about Respondent's cooperation with government investigations and ensures that Respondent provides an appropriate response to requests from law enforcement and government agencies.<sup>8</sup> (T 173, 175-76) Respondent does not expect its supervisors and employees to be experts in the law when it comes to police or government agency requests for information or documents from a hotel. (T 176) The policy provides for such requests to be reviewed by the legal department so that Respondent may appropriately respond. (T 176) Importantly, the Government Investigation policy does not apply to "an employee who decides

---

<sup>7</sup> Exhibit 2 at 5-6.

<sup>8</sup> Respondent has not disciplined an employee for violating the Government Investigation policy. (T 177)

that they want to make a claim against the Company or to cooperate on their own in providing information to the government.” (T 173).

Johnson provided several practical examples of how the Government Investigations policy is applied at Respondent’s hotels:

***Badge flashing.*** It is common for law enforcement, such as local police or the FBI, to visit hotel properties, flash a badge, and request information from the hotel about a guest or employee. (T 173) Often, the first employee a law enforcement officer has contact with is a front desk agent or manager who might be intimidated by the badge and may not consider the privacy and/or legal rights at stake. (T 173-74) The policy provides such employees with a standard response that Respondent will cooperate, but first they need to check with the legal department. (T 174-75) As the ALJ recognized, these situations are “very intimidating” and this procedure “alleviates pressure from workers by giving them a standard response” and ensures that information is not provided without a valid subpoena or search warrant. (ALJD 10:21-22; T 174-75)

***Government investigations and audits.*** When one of Respondent’s hotels is subject to a government investigation or audit, the policy ensures that Respondent’s compliance and cooperation with the investigation or audit is appropriate. (T 174-75) For example, when one of Respondent’s properties underwent a payroll audit by the Department of Labor (DOL), a hotel manager provided payroll information to the DOL without checking with Respondent’s legal department. (T 175-76) Although the information was accurate, it was provided in the incorrect format, resulting in a DOL fine. (T 175-76) Had the manager communicated with the legal department as required by the policy, the information would have been provided in the proper format, and a fine avoided, as the ALJ acknowledged. (ALJD 10:17-19; T 175-76)

*Conflicts between state and federal law.* California Government Code Sections 7285.1 and 7285.2 prohibit employers from voluntarily permitting federal Immigrations and Customs Enforcement (ICE) officials to enter places of private employment or to obtain certain employee records without a subpoena or warrant. California Labor Code Section 90.2 requires employers to give employees and their representatives 72 hours' prior written notice of a government audit of employee work authorization records. As acknowledged by the ALJ, there are "conflicts between state and federal law regarding the type of information an employer can provide to the Department of Homeland Security Immigration and Customs Enforcement Agency." (ALJD 10:13-15) This policy provides a procedure for a hotel receiving an ICE, DOL, or other government agency request to contact the legal department to ensure that Respondent responds in a manner that complies with both state and federal law. (T 176)

### **3. *Respondent Communicates Employees' Protected Rights***

Respondent's employees' ability to provide their own information to third parties and government agencies is in no way restricted by the Information Protection or Government Investigation policies of the Code. Respondent posts in English and Spanish all legally mandated government information posters at all locations in a non-conspicuous place. Such posters include the contact numbers for the corresponding government agencies and are available for every employee to reference. Employees are also assured that they are protected from retaliation for exercising such rights. (RX 2-3)

For example, the EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT notice is posted at the Hotel in Spanish and English (T 125-28; RX 2-3) Employees are advised by the poster that they have the right to, among other things, (i) discuss wages and benefits and other terms and conditions of employment or union organizing with co-workers or a union; and (ii) take

action with one or more co-workers to improve working conditions by, among other things, raising work-related complaints with Respondent or with a government agency, and to seek help from a union. (RX 2-3)

Thus, employees are not dissuaded from sharing their own PII or from filing claims or cooperating with government agencies, as illustrated by the numerous claims former employee Lluvia Ramirez-Orozco filed with various agencies (GX 1(a), 1(c), 1(e); T 113-15), as well as Marixenia Brandt, Maria Orona, and Ramirez-Orozco participating in Region 28's investigation, providing affidavits, and testifying at the hearing in this matter. (T 47, 98, 129) Nor did Respondent's policies prevent Brandt, Orona, and Ramirez-Orozco from sharing their own information with Somos un Pueblo Unido and forming a workers committee "to improve working conditions" with Somos. (T 73, GX 6, p.2)

The ALJ's contrary assertion that "in practice, Respondent's rule would require employees to identify themselves to Interstate as having been contacted by a Board agent" is simply not based in fact. (ALJD 18:21-23)

### **III. *QUESTIONS PRESENTED***

1. Whether the ALJ erred by concluding Section 6 (Information Protection) of the Code, when reasonably interpreted, prohibits or interferes with employee rights and whether any potential adverse impact on employees' protected rights is outweighed by Respondent's legitimate business justifications?

2. Whether the ALJ erred by concluding Section 16 (Government Investigation) of the Code, when reasonably interpreted, prohibits or interferes with employee rights and whether any potential adverse impact on employees' protected rights is outweighed by Respondent's legitimate business justifications?

**IV. THE ALJ ERRED BY CONCLUDING THAT RESPONDENT’S INFORMATION PROTECTION AND GOVERNMENT INVESTIGATIONS POLICIES VIOLATE SECTION 8(A)(1) OF THE ACT**

The ALJ impermissibly read the challenged policies out of context and discounted Respondent’s legitimate business justifications to conclude that the policies violate Section 8(a)(1) of the Act.. (ALJD 17-21)

In *The Boeing Company*, the National Labor Relations Board overruled its prior *Lutheran Heritage* “reasonably construe” standard for analyzing facially neutral employer rules.<sup>9</sup> “The Board will no longer find unlawful the mere maintenance of facially neutral employment policies, work rules and handbook provisions based on a single inquiry, which made legality turn on whether an employee ‘would reasonably construe’ a rule to prohibit some type of potential Section 7 activity that might (or might not) occur in the future.”<sup>10</sup> Instead, “the Board will evaluate two things: (i) the nature and extent of the potential impact on NLRA rights, and (ii) legitimate justifications associated with the requirement(s).”<sup>11</sup> Under the new standard, the Board categorizes employment policies as follows:

- *Category 1* will include rules that the Board designates as lawful to maintain, either because (i) the rule, when reasonably interpreted, does not prohibit or interfere with the exercise of NLRA rights; or (ii) the potential adverse impact on protected rights is outweighed by justifications associated with the rule. Examples of Category 1 rules are the no-camera requirement in this case, the “harmonious interactions and relationships” rule that was at issue in *William Beaumont Hospital*, and other rules requiring employees to abide by basic standards of civility.
- *Category 2* will include rules that warrant individualized scrutiny in each case as to whether the rule, when reasonably interpreted, would prohibit or interfere with the exercise of NLRA rights, and if so, whether any adverse

---

<sup>9</sup> *The Boeing Company*, 365 NLRB No. 154, slip op. at 7.

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*, slip op. at 14.

impact on NLRA-protected conduct is outweighed by legitimate justifications.

- *Category 3* will include rules that the Board will designate as unlawful to maintain because they would prohibit or limit NLRA-protected conduct, and the adverse impact on NLRA rights is not outweighed by justifications associated with the rule. An example would be a rule that prohibits employees from discussing wages or benefits with one another.<sup>12</sup>

Here, the only issues to be addressed are (i) whether the challenged policies, when reasonably interpreted,<sup>13</sup> would prohibit or interfere with Section 7 rights; and (ii) if so, whether the potential adverse impact on protected rights is outweighed by the justifications for the policies.

In finding that Sections 6 (Information Protection) and 16 (Government Investigation) of the Code would prohibit or interfere with Section 7 rights, the ALJ disregarded the following in the introduction to the Code:

[Respondent] has adopted this [Code] to *promote honest and ethical conduct*, including fair dealing and the ethical handling of conflicts of interest, *to promote compliance with applicable laws and government rules and regulations*, *to ensure the protection of the Company's legitimate business interests*, and to deter wrongdoing.

....

This Code outlines the broad principles of legal and ethical conduct by which the Company expects its associates to abide. It is not a complete list of legal or ethical issues that an associate might face in the course of his or her employment with the Company. When faced with any issue, *the Company expects its associates to conduct themselves using good judgment and common sense*.<sup>14</sup>

---

<sup>12</sup> *Id.*, slip op at 3-4, 15 (footnote omitted). The new standard applies to the allegations here, given that the Board held it applied retroactively to the challenged Boeing policy and “to all other pending cases.” *Id.*, slip op. at 17.

<sup>13</sup> *Id.*, slip op. at 4 n.16 (“this is an objective standard, and the reasonable interpretation of the rule is conducted from the perspective of a reasonable employee”).

<sup>14</sup> GX 3, p. 1 (emphasis added).

**A. *The Information Protection Policy Does Not Interfere with or Prohibit Employees from Disclosing Information About Themselves or Information About Other Employees That Was Lawfully Obtained***

**1. *The Information Protection Policy, When Reasonably Construed, Is Lawful***

The Information Protection policy provides guidelines to protect personally identifiable information (PII) that Respondent collects from guests, employees, vendors, and other third parties. As Johnson explained, this information must be protected to ensure compliance with state and federal privacy laws, to protect Respondent’s business interests, and to protect the personal safety of Respondent’s employees. Johnson provided several examples of prohibited use of PII, such as an employee accessing PII in Respondent’s database and sharing it with unauthorized persons, sharing PII with one of Respondent’s competitors, or jeopardizing an employee’s safety by sharing PII with a third party.

Contrary to the ALJ’s conclusion, the Information Protection policy could not be reasonably interpreted to prohibit employees from discussing information about themselves or other employees. Indeed, Brandt, Orona, and Ramirez-Orozco did not interpret the policy as interfering with their ability to share their own information with Somos un Pueblo Unido and to form a workers committee “to improve working conditions” with Somos.<sup>15</sup>

The Board recognizes that “an employer has a substantial and legitimate interest in maintaining the confidentiality of private information—guest information, recipes, contracts with vendors, and the like.”<sup>16</sup> Here, the Information Protection policy is designed to safeguard PII and similar confidential data that is collected by Respondent and stored in its database.

---

<sup>15</sup> T 73; GX 6, p. 2.

<sup>16</sup> *Ark Las Vegas Restaurant Corp.*, 335 NLRB 1284, 1290 (2001). In that case, the employer’s confidentiality policy stated:

*As Johnson testified, nothing in the policy prohibits employees from revealing their own PII or other information to other employees or third parties.* Rather, the policy states that employee are “responsible for using the *Company’s information*” for authorized purposes and prohibits employees from revealing “*our Company’s non-public information,*” such as the PII of others, that Respondent stores in its databases. The Board in *Boeing* recognized the importance of protecting employee PII when it upheld the challenged no-camera rule and explained, that the “rule limit[ed] the risk that employees’ personally identifiable information will be released.”<sup>17</sup>

In *Minteq, Int’l*,<sup>18</sup> the Board found a confidentiality policy to be lawful where it prohibited employees from disclosing confidential information that included “software, technical, and business information relating to the Company . . . and *any other information which is identified as confidential by the Company.*”<sup>19</sup> The administrative law judge found that employees would reasonably interpret the policy as prohibiting protected activity because the phrase “any other information which is identified as confidential by the Company” is so ambiguous that “it could reasonably be read to include wages and benefits.”<sup>20</sup> However, the Board disagreed, holding that such a finding could only be supported if the phrase was impermissibly read in isolation. The policy defined “confidential information” as “any proprietary or confidential information or know-

---

It is our policy to ensure that the operations, activities, and affairs of Ark Las Vegas and our clients are kept confidential to the greatest possible extent. If, during their employment, employees acquire confidential or proprietary information about Ark Las Vegas or its clients, such information is to be handled in strict confidence and not to be discussed. Employees are also responsible for the internal security of such information.

*Id.* at 1290.

<sup>17</sup>*Boeing*, 365 NLRB No. 154, slip op. at 6.

<sup>18</sup>*Minteq Int’l, Inc.*, 364 NLRB No. 63 (2016).

<sup>19</sup>*Id.*, slip op. at 6.

<sup>20</sup>*Id.*

how belonging to the company,” that is “not generally known in the relevant trade or industry,” and which the employee “obtained from the Company . . . in the scope of [his or her] employment.”<sup>21</sup> It was then followed by examples that illustrated its scope and meaning. Thus, the Board determined that “employees reading the concluding phrase, ‘any other information which is identified as confidential by the Company,’ would reasonably understand it to refer to the preceding examples of proprietary information and trade secrets, not information related to employees’ wages or working conditions.”<sup>22</sup>

Here, similar to *Minteq*, the ALJ impermissibly read certain words in the Information Protection policy in isolation and parsed words from their surrounding context.<sup>23</sup> Properly read in context, the Information Protection policy explains the value to Respondent of “information and the information systems we use to process and store that data,” as well as the need to keep “our Company’s non-public information” confidential. It then lists examples of confidential information, including various forms of PII, regardless of whether it pertains to “a customer, potential customer, associate, former associate, owner or joint venture partner.” The policy also lists other examples of confidential and proprietary information (with which neither the General Counsel nor the ALJ took issue) before concluding that such information is “the Company’s” and may be used “solely for authorized business purposes” and protected “from unauthorized internal and external access.”

These repeated references to the Company’s information throughout the policy are consistent with Johnson’s testimony that only information stored in the Company’s databases

---

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> ALJD 20:1-7.

which is collected for business operations is confidential.<sup>24</sup> Somehow, in spite of the plain language of the policy and testimony to the contrary, the ALJ found that “in no way is the rule explicitly limited to company non-public information contained in Respondent’s databases.”<sup>25</sup>

In support of his erroneous conclusion, the ALJ relies on distinguishable Board precedent. In *Ridgley Manufacturing*, an employee memorized his fellow employees’ names from timecards that were located near the employee timeclock and was terminated for his activity.<sup>26</sup> The Board recognized that “protection for such activity depend[ed] on the question of whether timecards located by the timeclock fall into the category of private or confidential records of the Employer or constitute[d] information available to all employees in the course of their normal work relationship.”<sup>27</sup> Ultimately, the employee’s conduct fell into the latter classification. However, unlike in *Ridgley Manufacturing*, the employee information Respondent seeks to protect with its Information Protection policy, e.g. company information stored in its databases, is not information available in the course of employees’ normal work relationship.

The ALJ also relies on *Gray Flooring*, where an employee was terminated for copying employee names and phone numbers from cards left out in the open on a supervisor’s desk.<sup>28</sup> The Board determined the termination was unlawful because the employee was not on notice that such information was private or confidential, nor was the information treated as such.<sup>29</sup> Here, however,

---

<sup>24</sup> T 167, 170.

<sup>25</sup> ALJD 21:7-10.

<sup>26</sup> *Ridgley Mfg. Co.*, 207 NLRB 193, 196–97 (1973) *enf’d* 510 F.2d 185 (D.C. Cir. 1975).

<sup>27</sup> *Id.* at 197.

<sup>28</sup> *Gray Flooring*, 212 NLRB 668, 674 (1974).

<sup>29</sup> *Id.* at 669.

Respondent has deemed the company information stored in its databases as private and confidential and treats the information as such.

Unlike the obvious employee information (names and phone numbers) at issue in *Ridgley Manufacturing* and *Gray Flooring*, here, a reasonable interpretation of the policy's reference to an employee's PII means ***the Company must protect this information in this era of identity theft, phishing scams, and other forms of cyber misconduct.*** This conclusion is supported by other examples of confidential information referenced in the Information Protection policy, which include an individual's "bank and credit card information, social security number, etc."<sup>30</sup> It is entirely unreasonable, given the context, for the ALJ to interpret Respondent's policy any other way.<sup>31</sup>

---

<sup>30</sup> In *Macy's, Inc.*, 365 NLRB No. 116, slip op. at 1 (2017), the Board upheld a rule that prohibited employees from disclosing information about customers, including "documents that show social security numbers or credit card numbers," obtained from the employer's confidential records. No exceptions were filed in that case to the administrative law judge's findings that the employer's policy that broadly prohibited sharing of any personal data with "any third party." *Id.* slip op. at 1 n.1, 2, 13. Here, in contrast, the Information Protection policy does not prohibit an employee from sharing his/her own information with third parties.

<sup>31</sup> In *Safeway, Inc.*, 338 NLRB 525 (2002), the Board upheld the following rule: "Confidential, restricted or sensitive information must be kept safe and never given to an unauthorized person or organization. Such information includes (but is not limited to) computer-access passwords, procedures used in producing computer or data processing records, ***personnel and medical records, and payroll data.***" *Id.* at 525 (emphasis added). The Board reasoned that a finding that the references in the rule to personnel records and payroll data "had a chilling effect on employees' exercise of Section 7 rights depends on a chain of inferences upon inferences." *Id.* at 527. Specifically, it would require:

that the employees would infer that the reference to personnel and payroll records, in the context of the rest of the rule, referred to their own wages, hours, and working conditions, and that employees would further infer that the ban on disclosure to "unauthorized" persons or organizations encompassed their coworkers and the Union. It is highly improbable that the employees in this unit, who had been represented by the Union for several years, would draw these inferences under the circumstances of this case.

*Id.*

In *Macy's, Inc.*, the Board explained that the Act “does not protect employees who divulge information that their employer lawfully may conceal.”<sup>32</sup> Accordingly, “the Board has repeatedly held that employees may be lawfully disciplined or discharged for using for organizational purposes information improperly obtained from their employer’s private or confidential records.”<sup>33</sup>

For example, in *International Business Machines Corp.*, the Board upheld the termination of an employee who shared the wage data of other employees that he obtained from his employer’s confidential database after the employer reminded the employee that “you are to see that these [Company] confidential documents are not published or given unauthorized distribution.”<sup>34</sup> Unlike the ALJ’s misinterpretation of the Information Protection policy, the Board in *International Business Machines* did not interpret the policy in that case to prohibit employees “from compiling or determining wage information on their own” or “muzzling” employees from discussing their wages with others.<sup>35</sup> Here, likewise, the Information Protection policy does not prohibit an employee from sharing information about other employees that is lawfully obtained from other sources, such as the other employees themselves.

---

<sup>32</sup> *Macy's, Inc.*, 365 NLRB No. 116, slip op. at 4 (citing *International Business Machines Corp.*, 265 NLRB 638 (1982)). The General Counsel also agrees that “employees do not have a right under the Act to disclose employee information obtained from unauthorized access/use of confidential records, or to remove records from the employer’s premises.” General Counsel Memorandum 18-04, at 10 (Jun. 6, 2018).

<sup>33</sup> *Id.* (internal citations omitted); see also *Flex Frac Logistics, LLC*, 360 NLRB 1004, 1005 (2014)).

<sup>34</sup> *International Business Machines Corp.*, 265 NLRB at 638, 641.

<sup>35</sup> *Id.* at 638. See also *Legacy Charter*, 28-CA-201248, 2018 NLRB LEXIS 338 \*50 (NLRB Div. of Judges, Aug. 16, 2018) (the administrative law judge, applying *Boeing*, concluded an employer rule which deemed “personnel information” confidential did not violate the Act when read in context with the surrounding prohibition against disclosing non-public information about the employer).

In *Mediaone of Greater Florida*,<sup>36</sup> the Board upheld a confidentiality rule that prohibited disclosure of, among other things, “customer and *employee information*, including organizational charts and databases.”<sup>37</sup> The administrative law judge and the Board both found the rule to be reasonably read as “prohibiting only disclosure of the Respondent’s information assets and intellectual property, which is private business information that the Respondent has a right to protect.”<sup>38</sup> The Board emphasized that the rule did “not explicitly prohibit the discussion or disclosure of wages, hours, working conditions, or any other terms and conditions of employment, nor [did] it forbid conduct that clearly implicates Section 7 rights.”<sup>39</sup>

In *Copper River of Boiling Springs, LLC*, Judge Keltner Locke upheld a rule that prohibited the “[u]nauthorized dispersal of sensitive Company operating materials or information to any unauthorized person or party. This includes but is not limited to policies, procedures financial information, manuals, or any other information contained in Company records.”<sup>40</sup> In finding the rule to be lawful, Judge Locke acknowledged that “the reference to ‘financial information’ might be construed to include wage and benefit rates.”<sup>41</sup> However, he reasoned that “the rule itself does not refer to wage or benefit rate and its prohibition is limited to the dispersal of ‘sensitive Company’ materials and information.”<sup>42</sup>

---

<sup>36</sup> *Mediaone of Greater Florida*, 340 NLRB 277 (2003).

<sup>37</sup> *Id.* at 278 (emphasis added).

<sup>38</sup> *Id.* at 278-79. Similar to the ALJ’s reading of the Information Protection policy here, the General Counsel in *Mediaone* incorrectly alleged the rule could “reasonably be read by employees to prohibit discussion among employees about their wages, hours, or working conditions and to forbid disclosure of such information to unions.” *Id.* at 278.

<sup>39</sup> *Id.* at 279.

<sup>40</sup> *Copper River of Boiling Springs, LLC*, 360 NLRB 459, 469 (2014).

<sup>41</sup> *Id.* at 472.

<sup>42</sup> *Id.*

Similar to *Mediaone*, the reference in Respondent’s Information Protection policy to an employee’s PII must be interpreted to protect the unauthorized disclosure of Respondent’s “information assets.” Additionally, like the lawful policies in *Mediaone* and *Copper River*, the policy here does not explicitly prohibit the discussion or disclosure of wages, hours, or any other terms and conditions of employment, nor does it forbid conduct that clearly implicates Section 7 rights and its prohibition is limited to “protecting the Company’s confidential information and information systems”—facts which were entirely ignored by the ALJ.

Further, given that the Code expressly states that Respondent “expects its associates to conduct themselves using good judgment and common sense,” it is unreasonable for the ALJ to interpret the Information Protection policy as prohibiting an employee from revealing his/her own PII.<sup>43</sup> The Information Protection policy does not prohibit an employee from divulging his/her own name, address, telephone number, or email address to other employees or third parties, or such information about other employees if it has been lawfully obtained from a source other than Respondent’s databases.<sup>44</sup> Rather, the policy prohibits employees from disclosing the PII and other confidential information in Respondent’s databases. The policy, when reasonably interpreted, does not interfere with or prohibit employees from exercising their Section 7 rights.

---

<sup>43</sup> In *Community Hosp. of Cent. Cal. v. NLRB*, 335 F.3d 1079 (D.C. Cir. 2003), *denying enf. in relevant part to University Medical Center*, 335 NLRB 1318 (2001), the court upheld an employer rule that prohibited the “release or disclosure of confidential information concerning patients or employees.” *Id.* at 1088. The court explained that a “reasonable employee would not believe that a prohibition upon disclosing information, acquired in confidence, ‘concerning patients or employees’ would prevent him from saying anything about himself or his own employment. And to the extent an employee is privy to confidential information about another employee . . . he has no right to disclose that information contrary to the policy of his employer.” *Id.* at 1089.

<sup>44</sup> Employees at all of Respondent’s locations are exposed to all required government postings, which provide information to employees about their rights under various state and federal laws along with contact information for the applicable government agencies. (RX 2-3)

2. *The ALJ Incorrectly Disregarded Respondent’s Legitimate Business Justifications for its Information Protection Policy and Improperly Advocated for a More “Narrowly Tailored” Policy*

Assuming *arguendo* that the Information Protection policy could somehow be interpreted to have an adverse impact on protected rights, any adverse impact is outweighed by the Respondent’s justifications for protecting PII. Respondent could not remain in business, much less lawfully operated 400 properties across the United States, if it could not protect PII and other confidential information—such as competitive strategies and financial data, computer passwords, and revenue management techniques—from being disclosed to third parties who could use the information to harm Respondent, employees, guests, and others.<sup>45</sup> Given the frequent cyber-attacks on company databases—in which hackers seek PII and other confidential information listed in the policy—the Respondent is compelled to protect such information.

Indeed, all state laws require employers to protect PII.<sup>46</sup> For example, New Mexico requires anyone owning or licensing PII to “implement and maintain reasonable security procedures and practices” to protect PII “from unauthorized access, destruction, use, modification or disclosure.”<sup>47</sup>

---

<sup>45</sup> The Board has long recognized the need for confidentiality with respect to social security numbers and certain employer financial data, such as tax returns. *Metro Health Foundation, Inc.*, 338 NLRB 802, 803 n.2 (2003); *Troy Hills Nursing Home*, 326 NLRB 1465, 1466 n.2 (1998).

<sup>46</sup> On April 6, 2017, New Mexico became the 48th state to enact a data breach notification law, requiring security measures for storage of PII, proper disposal of PII, and notification of security breaches of PII. N.M. Stat. §§ 57-12C-1 through 57-12C-12.

As of March 29, 2018, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring protection of PII and notification to individuals of security breaches. See <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

<sup>47</sup> N.M. Stat. § 57-12C-4.

In New Mexico, the felony of identity theft is committed by anyone “willfully obtaining, recording or *transferring [PII] of another person without the authorization or consent of that person* and with the intent to defraud that person or another or with the intent to sell or distribute

California has one of the most stringent data security laws that requires notification be given to individuals when “unencrypted personal information” was or is reasonably believed to have been acquired by an “unauthorized person” or when “encrypted personal information” was or reasonably could have been acquired by an “unauthorized person” in a manner that renders “personal information readable or useable.”<sup>48</sup>

Similarly, the courts and Congress have recognized that disclosure of an employee’s:

- *home address* “would constitute a clearly unwarranted invasion of personal privacy”,<sup>49</sup>
- *telephone number* may expose the employee to fraud, deception, and abuse;<sup>50</sup> and
- *email address* may result in multiple problems for the employee, given the costs of storage, risks of deception, and/or time spent accessing, reviewing, and discarding such email.<sup>51</sup>

---

the information to another for an illegal purpose.” N.M. Stat. § 30-16-24.1(A)-(D) (emphasis added).

<sup>48</sup> Cal. Civ. Code §§ 1798.29(a) and 1798.82(a).

<sup>49</sup> In *Reed v. NLRB*, 927 F.2d 1249 (D.C. Cir. 1991), the court held that the disclosure of private sector employee home addresses “would constitute a clearly unwarranted invasion of personal privacy,” protected from disclosure under Exemption 6 the Freedom of Information Act, 5 U.S.C. § 552(b)(6). Similarly, in *United States Dep’t of Defense v. FLRA*, 510 U.S. 487 (1994), the Court held that the Privacy Act of 1974, 5 U.S.C. § 552a, prohibits a government agency from disclosing the home addresses of public sector employees to the employees’ collective-bargaining representative. The Court emphasized that the “privacy of the home . . . is accorded special consideration in our Constitution, laws, and traditions.” *Id.* at 501.

<sup>50</sup> *See, e.g.*, Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, in which Congress found that telemarketing fraud causes the recipients of such calls to lose an estimated \$40 billion a year. Additionally, the telephone recipients are victimized by other forms of telemarketing deception and abuse. 15 U.S.C. §§ 6101(3)-(4).

<sup>51</sup> *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), 15 U.S.C. §§ 7701-7713, in which Congress found, among other things, that the receipt of unsolicited email may result in costs to recipients who cannot refuse to accept it and who incur costs for storage and/or time spent accessing, reviewing, and discarding such email. *Id.*

The Occupational Safety and Health Administration (OSHA) also recognizes the need to protect the PII of employees that employers collect and report to OSHA. On its frequently-asked questions page (concerning the recent regulations designed to improve tracking of workplace injuries and illnesses), OSHA states:

**How will Personally Identifiable Information (PII) be protected?**

OSHA has effective safeguards in place to prevent the disclosure of personal or confidential information contained in the recordkeeping forms and submitted to OSHA. OSHA will not collect *employee name, employee address*, name of physician or other health care professional, or healthcare facility name and address if treatment was given away from the worksite. All of the case specific narrative information in employer reports will be scrubbed for PII using software that will search for, and de-identify, personally identifiable information before the data are posted.<sup>52</sup>

The Board likewise recognizes the sensitivity of PII by requiring parties to redact such information prior to e-filing a document with the agency:

**E-FILINGS SHOULD NOT CONTAIN “SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION” (SPII) THAT IS NOT ESSENTIAL TO THE MATTER AT ISSUE**

Please redact (remove) any non-essential personally identifiable information before uploading an E- Filing. If you believe you must file documents with the Agency that contain unredacted sensitive personally identifiable information, you must indicate during the E-filing process the type of SPII contained in the document.

SPII is an individual’s name in **combination with** one or more of the following:

- Date of birth
- Social Security number
- Driver’s license number
- Financial account number
- Credit or debit card number<sup>53</sup>

---

at § 7701(a)(3) Additionally, many senders of unsolicited email purposefully disguise their identity and include misleading information. *Id.* at §§ 7701(a)(7)-(8).

<sup>52</sup> [https://www.osha.gov/recordkeeping/finalrule/finalrule\\_faq.html](https://www.osha.gov/recordkeeping/finalrule/finalrule_faq.html)

<sup>53</sup> <https://apps.nlr.gov/eservice/efileterm.aspx>; *see also* NLRB DIVISION OF JUDGES, BENCH BOOK § 12-800 (Jan. 2018) (the Board also requires that SPII not be submitted by a party into the record during a hearing or used in decisions).

In addition to the business and legal justifications for protecting guest, employee, and third party PII in compliance with state and federal laws,<sup>54</sup> the undisputed evidence also illustrates practical justifications. In the competitive hospitality industry, the Information Protection policy prevents employees from sharing PII in Respondent's database with a competitor. The policy also safeguards the PII of Respondent's 30,000 employees by protecting information stored in its database from being provided to unauthorized individuals, such as the perpetrator in a domestic dispute.

Unfortunately, the ALJ disregarded all of Respondent's proffered justifications and instead found that Respondent could accomplish its justifications "with a more narrowly tailored rule that does not interfere with employee protected activity."<sup>55</sup> However, the Board in *Boeing* refused to adopt the requirement that employer rules be "narrowly tailored" because "it is impossible to craft reasonable workplace rules to [such] exacting standards."<sup>56</sup> Indeed, the requirement imposed by the ALJ is an "(unattainable) requirement of linguistic perfection" that has been rejected by the Board.<sup>57</sup>

---

<sup>54</sup> The General Counsel gives weight to legitimate business justifications, like those Respondent asserts:

Employers have an obvious need to protect confidential and proprietary information, as well as customer information. Customer information may include records of past purchases, which may affect an employer's decisions concerning inventory and marketing, among other things. Customers also routinely provide businesses with their personal information, such as credit card numbers, with the reasonable expectation that the business will protect that information. Employers have a compelling interest in prohibiting the disclosure of such information to protect their business reputation and avoid significant legal liability.

General Counsel Memorandum 18-04, at 11 (Jun. 6, 2018).

<sup>55</sup> ALJD 21:20-22.

<sup>56</sup> See *Boeing*, 365 NLRB No. 154, slip op. at 21, n.90.

<sup>57</sup> *Id.* slip op. at 10, n.42.

Accordingly, contrary to the findings of the ALJ, any potential adverse impact on protected rights is outweighed by Respondent's need to protect the PII and other confidential information of its employees, customers, and third parties that is contained in Respondent's databases.

**B. *The Government Investigations Policy Does Not Interfere with or Prohibit Employees from Participating in Government Investigations, Including Those of the NLRB***

**1. *The Government Investigations Policy, When Reasonably Construed, Is Lawful***

The ALJ erroneously concluded that Respondent's Government Investigation policy "impacts the Section 7 right of employees to provide evidence to the Board, or to cooperate in Board investigations."<sup>58</sup> However, the policy provides guidance on Respondent's cooperation with government investigations, not employees' personal cooperation, and ensures that Respondent provides an appropriate response to requests from law enforcement and government agencies. The plain language of the policy makes obvious that the subject of the policy is the Respondent, not employees. For example, the policy begins with "[w]e promote cooperation with law enforcement and government agencies," and goes on to explain that "*the Company* requires an official written request or a subpoena" prior to the Respondent providing information.<sup>59</sup> Thus, Respondent's Government Investigation policy controls the employer-response to law enforcement agencies and government agencies, not the employee-response.<sup>60</sup>

---

<sup>58</sup> ALJD 18:18-19.

<sup>59</sup> GX 3, p. 6.

<sup>60</sup> The distinction between employer-response and employee-response is important. For example, in *Macy's, Inc.*, the administrative law judge, applying *Lutheran Heritage*, found the following policy would interfere with an employee's right to give a statement to a Board agent, or other governmental agency: "If *we are asked to provide information*- verbal or written- for a government investigation, or if a government representative appears at our workplace, we must promptly notify our Human Resources representative or the Law Department and obtain approval for the release of any information. We must not obstruct, influence, mislead or impede the

Respondent's Government Investigations policy does not prohibit employees from speaking to law enforcement or government agencies or prohibit release of non-official information without approval as the ALJ assumes. The "critical inquiry into employer rules" of this nature is "whether the rule prohibits employees from communicating" about protected matters or "merely states that employees cannot speak on behalf of the [Employer]" concerning such matters.<sup>61</sup> Unlike those rules found to be unlawful because they broadly applied to "all inquiries," the Government Investigations policy, by its plain language, is limited to "official written requests" and "subpoenas" from a government or law enforcement agency. As Johnson testified, Respondent is merely seeking to prevent employees from providing an *official response on behalf of Respondent*. Any finding made by the ALJ otherwise directly contradicts the undisputed evidence.

The ALJ failed to apply the proper *Boeing* standard, which requires analyzing whether the challenged policies, when reasonably interpreted,<sup>62</sup> would prohibit or interfere with Section 7 rights. Under *Boeing*, "[t]he Board will no longer find unlawful the mere maintenance of facially

---

investigation." *Macy's, Inc.*, 365 NLRB No. 116, slip op. at 13-14 (emphasis added). The employer did not file any exceptions to this finding. *Id.*, slip op. at 1 n.1.

In making this finding, the administrative law judge incorrectly compared the policy to a one found to be unlawful in *DirectTV*, which stated: "If law enforcement wants to interview or obtain information regarding a DIRECTV employee . . . *the employee* should contact the security department. . . who will handle contact with law enforcement agencies . . ." 359 NLRB 545, 546, n.4 (2013) (emphasis added).

The policy in *Macy's* is wholly unlike the policy in *DirectTV* because the *Macy's* policy (like Respondent's here) referred to the employer-response requirements, whereas the *DirectTV* policy referred to the employee-response requirements. For these reasons, including that the administrative law judge relied upon the now defunct *Lutheran Heritage* standard, *Macy's* should not be controlling here.

<sup>61</sup> *Blue Man Las Vegas LLC*, Case 28-CA-21126, 2008 NLRB Lexis 225, \*60 (NLRB Div. of Judges, July 18, 2008).

<sup>62</sup> *Boeing*, 365 NLRB No. 154, slip op. at 4 n.16 ("this is an objective standard, and the reasonable interpretation of the rule is conducted from the perspective of a reasonable employee").

neutral employment policies, work rules and handbook provisions based on a single inquiry, which made legality turn on whether an employee ‘would reasonably construe’ a rule to prohibit some type of potential Section 7 activity that might (or might not) occur in the future.”<sup>63</sup> Indeed, one of the problems with the *Lutheran Heritage* standard was the inconsistent application as to whether a “reasonable employee would read the rule to apply to [a protected] activity simply because the rule *could* be interpreted that way.”<sup>64</sup>

Here, the ALJ erroneously concluded “it is reasonable to conclude they [employees] *would* believe that its [the policy’s] provisions generally govern their interaction with government agencies, including Board investigators”<sup>65</sup> and that the policy “puts employees at risk of intimidation, and *could* make them ‘reluctant to give statements to NLRB investigators at all.’”<sup>66</sup> These conclusions are impermissibly based on activity that may or may not happen in the future, in direct contradiction to the requirements of *Boeing*.<sup>67</sup>

---

<sup>63</sup> *Id.*, slip op. at 7.

<sup>64</sup> *Id.*, slip op. at 13, n.68 (citing *Lutheran Heritage Village-Levonía*, 343 NLRB 646, 647 (2004) (“to take a different analytical approach would require the Board to find a violation whenever the rule could conceivably be read to cover Section 7 activity, even though that reading is unreasonable”)).

<sup>65</sup> ALJD 18:12-14 (emphasis added).

<sup>66</sup> ALJD 18:34-35 (emphasis added).

<sup>67</sup> The following case law cited by the ALJ in support of his conclusion should be disregarded because it does not provide guidance or support for how to reasonably interpret employer policies, such as Respondent’s Government Investigation policy: *Laidlaw Transit, Inc.*, 315 NLRB 79 (1994) (employer failed to clarify an overly broad no-solicitation/no-distribution rule); *Nash v. Florida Industrial Commission*, 389 U.S. 235 (1967) (reversing a Florida unemployment compensation decision because employees must be free from coercion when reporting unfair labor practices to the Board); *Robbins Tire & Rubber Co.*, 437 U.S. 214 (1978) (the Board was entitled to withhold witness’ statements, regardless of a Freedom of Information Act request, due to the risk that witness intimidation would dissuade potential witnesses from testifying).

A reasonable interpretation of the Government Investigation policy is that it does not prohibit or interfere with Section 7 rights. When the language the ALJ found unlawful is read in context with the surrounding paragraph, the inescapable conclusion is that the “*requests* from the police, Internal Revenue Service and other regulatory authorities” that must be referred to Respondent’s legal department are only requests for Respondent’s official position.

The ALJ also concluded that “in practice,” the policy “would require employees to identify themselves to Interstate as having been contacted by a Board agent—or other government/law enforcement agency—and receive clearance before providing evidence; this puts employees at risk of intimidation and coercion.”<sup>68</sup> This conclusion is not based on the evidence. What the evidence *does* show is that employees are advised by all legally required government postings that they have protected rights and employees are also provided contact information for the various government agencies. Obviously, “in practice,” Respondent’s Government Investigations policy did not deter former employee Ramirez-Orozco from filing her charge and two amendments thereto. Nor did it deter her from filing an EEOC charge, a workers’ compensation claim, or a wage claim.<sup>69</sup> Similarly, the policy did not interfere with Brandt, Orona, and Ramirez participating in Region 28’s investigation, providing affidavits, and testifying at the hearing in this matter.<sup>70</sup>

In sum, the Government Investigations policy describes the procedure Respondent follows when a government or law enforcement agency requests cooperation from Respondent. A reasonable interpretation of the policy would not cause an employee to believe that it interferes with his/her right to speak about or report workplace complaints to government agencies, such as

---

<sup>68</sup> ALJD 18:21-24.

<sup>69</sup> T 113-15.

<sup>70</sup> T 47, 98, 129.

the Board or law enforcement. The policy simply addresses Respondent's need to have legal counsel manage the procedure and manner in which *official information* is provided to law enforcement and government agencies to ensure that the rights of others are not violated. It also reinforces Respondent's position that "[w]e *promote cooperation with* law enforcement agencies and government agencies."<sup>71</sup>

**2. *The ALJ Incorrectly Disregarded Respondent's Legitimate Business Justifications for its Government Investigations Policy and Improperly Advocated for a More "Narrowly Tailored" Policy***

Assuming *arguendo* that the Government Investigations policy could somehow be interpreted to have an adverse impact on protected rights, any adverse impact of the policy is outweighed by the justification for Respondent's appropriate response to government investigations. Respondent must be able to control the methods by which it releases official information to government and administrative agencies, such as the Internal Revenue Service, Equal Employment Opportunity Commission, the Federal Bureau of Investigation, etc.<sup>72</sup>

A recent Supreme Court case illustrates the need for this type of policy. In *City of Los Angeles v. Patel*, the Court found as unconstitutional a Los Angeles ordinance that required hotel operators to make all of their guest records available to the police on demand.<sup>73</sup> The recordkeeping

---

<sup>71</sup> GX 3, p. 6.

<sup>72</sup> See *The Kroger Co of Michigan*, Case 07-CA-098566, 2014 NLRB Lexis 279, \*21 (NLRB Div. of Judges, Apr. 22, 2014) ("an employer has a legitimate interest in stopping unauthorized employees from speaking on behalf of the company, and indeed, from being perceived to have spoken on behalf of the company"); *Blue Man Las Vegas LLC*, Case 28-CA-21126, 2008 NLRB Lexis 225, \*59-60.

<sup>73</sup> *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015). The Court assumed that such police searches would "ensure compliance with the recordkeeping requirement, which in turn deters criminals from operating on the hotels' premises." *Id.* at 2452. The Court held that "a hotel owner must be afforded an opportunity to have a neutral decisionmaker review an officer's demand to search the registry before he or she faces penalties for failing to comply." *Id.* at 2453.

requirements of the ordinance, which were not at issue before the Court,<sup>74</sup> mandate that hotels record various information about all guests, including: each guest's name and address; the number of people in each guest's party; the make, model, and license plate number of any guest's vehicle parked on hotel property; the guest's date and time of arrival; the room number assigned; the guest's scheduled departure date; the rate charged and amount collected; and the method of payment.<sup>75</sup> Guests without reservations, those who pay for their rooms with cash, and any guests who rent a room for less than 12 hours must present photographic identification at the time of check-in, and hotel operators are required to record the number and expiration date of that document.<sup>76</sup> For guests checking in via an electronic kiosk, the hotel's records must also contain the guest's credit card information.<sup>77</sup> This information must be "kept on the hotel premises in the guest reception or guest check-in area or in an office adjacent" thereto for a period of 90 days.<sup>78</sup> Prior to the Court's decision, a hotel operator's failure to make such guest records available for police inspection was a misdemeanor punishable by up to six months in jail and a \$1,000 fine.<sup>79</sup>

Obviously, without a review by Respondent's legal department of a police request for such records at one of Respondent's Los Angeles hotels, an employee might be intimidated by the police into improperly disclosing private and confidential information.

Respondent is also aware that its employees and managers are not legal experts and may not personally know the laws surrounding subpoenas, search warrants, or the interaction between

---

<sup>74</sup> *Id.* at 2448 and 2454.

<sup>75</sup> Los Angeles Municipal Code § 41.49(2).

<sup>76</sup> *Id.* § 41.49(4).

<sup>77</sup> *Id.* § 41.49(2)(b).

<sup>78</sup> *Id.* § 41.49(3)(a).

<sup>79</sup> *Id.* § 11.00(m) (general provision applicable to entire Code).

state and federal laws. The Government Investigations policy gives these employees a procedure to follow in the event they are faced with a law enforcement officer, FBI Agent, or ICE Agent who is requesting information about a guest or employee. Similarly, when a government agency investigates or audits one of Respondent's properties, it is important to use the procedure in the Government Investigations policy to ensure the most accurate and appropriate information is communicated to the agency.<sup>80</sup>

Similarly, many states have laws that conflict with federal law and employees and managers cannot be expected to become conflict of law experts. For example, California Government Code Sections 7285.1 and 7285.2 prohibit employers from voluntarily permitting federal "ICE" agents from entering places of private employment or to obtain certain employee records without a subpoena or warrant. California Labor Code Section 90.2 requires employers to give employees and their representatives 72 hours' prior written notice of a government audit of employee work authorization records. These laws directly conflict with ICE raids that may occur at an employer's place of business, which are becoming more frequent. Given this and other potential conflicts of law, Respondent has a legitimate interest in providing a procedure for its employees to contact its legal department when presented with requests from government agencies and law enforcement.

However, these legitimate business justifications were disregarded by the ALJ, as illustrated by his conclusion that "if, as Respondent asserts," the policy is "'merely seeking to prevent employees from providing an official response on behalf of Respondent,' there would be no need to prohibit all employees from answering requests from Board investigators, or other

---

<sup>80</sup> Johnson testified that Respondent was fined during a DOL audit because a local manager did not provide payroll reports in the proper format to the auditor. Had the manager followed proper procedures, Respondent would have provided the correct report and avoided the fine.

regulatory/law enforcement authorities, without obtaining pre-clearance from the legal department.”<sup>81</sup> The flaw in the ALJ’s reasoning is that he impermissibly read the last sentence of the Government Investigation policy out of context. The ALJ also stated that a “more narrowly tailored rule that does not interfere with protected employee activity would be sufficient to accomplish the Company’s presumed interest.”<sup>82</sup> This conclusion is another example of an “(unattainable) requirement of linguistic perfection” that has been rejected by the Board.<sup>83</sup> Employers are not required under *Boeing* to craft the most narrowly tailored workplace rule to such “exacting standards.”<sup>84</sup>

Accordingly, any potential adverse impact on protected rights that would potentially result from a reasonable reading of the Government Investigation policy is outweighed by Respondent’s need to control the method and procedure through which it provides its official response to government investigations.

---

<sup>81</sup> ALJD 19:22-27.

<sup>82</sup> ALJD 19:27-28.

<sup>83</sup> *Boeing*, 365 NLRB No. 154, slip op. at 10, n.42.

<sup>84</sup> *Id.*, at slip op. at 21, n.90.

**V. CONCLUSION**

For all the reasons set forth above, Respondent respectfully requests that the ALJ's decision be reversed in part, and the complaint dismissed.

Dated: October 9, 2018

Respectfully submitted,

BALLARD, ROSENBERG, GOLPER & SAVITT, LLP  
Matthew T. Wakefield  
Nicole K. Haynes

By: \_\_\_\_\_

NICOLE K. HAYNES  
6135 Park South Drive, Suite 510  
Charlotte, NC 28210-0100  
Telephone: 704-945-7163  
nhaynes@brgslaw.com

Attorneys for Respondent  
INTERSTATE MANAGEMENT COMPANY, L.L.C. as  
agent for BRE NEWTON HOTELS PROPERTY  
OWNER, LLC d/b/a RESIDENCE INN BY MARRIOTT  
SANTA FE ALL-SUITES HOTEL