LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 29, Number 5 • August 2014

Supreme Court Preserves Fraud-On-the-Market Presumption in Securities Fraud Litigation

By Eric Rieder

The U.S. Supreme Court recently issued its long-awaited decision in *Halliburton v. Erica P. John Fund, Inc.*, and the result was very much in line with the forecasts of those who predicted a kind of split decision: The Court provided securities fraud defendants with a significant weapon to use in opposing class certification, but declined to jettison the fraud-on-the-market theory that has served as the basis for securities class actions for the past 25 years.

Despite the urging of Halliburton and its supporters, the Court did not overturn *Basic Inc. v. Levinson*, 485 U.S. 224 (1988), which conferred on plaintiffs the benefit of a presumption that all purchasers of stock trading in an efficient market relied on any alleged misrepresentation, because public securities markets are presumed to digest and thus reflect all publicly available, material information.

Rebuttable Presumption

However, the Court held that defendants could rebut that presumption at the class certification stage, rather than having to wait until summary judgment motions or trial.

continued on page 9

Supreme Court Opinion Calls into Question Hundreds of NLRB Rulings

By Matthew C. Lonergan and Anne Knox Averitt

On June 26, 2014, the Supreme Court issued its long-awaited *Noel Canning* decision (*NLRB v. Noel Canning*, 572 U.S. ____ (2014)), and invalidated President Obama's January 2012 appointments of three individuals to the National Labor Relations Board (the NLRB or Board): Terence Flynn, Richard Griffin, and Sharon Block. The Court held that while the President can make appointments during a Senate recess under the Constitution's recess appointments clause, the Senate's break in January 2012 was too short to constitute a recess. The Board cannot conduct business without a three-member quorum, so the holding calls into question hundreds of labor decisions issued while those appointees were seated. The NLRB decided 436 cases without a quorum during the 18 months that two of the appointees served on the Board (the third stepped down after only a few months).

The current Board, all of whose members were confirmed by the Senate, must now decide if revisiting each of the 436 rulings will be necessary to preempt additional challenges. Reconsideration of the decisions is unlikely to make a difference in most cases, as both the previous and current Boards have been Democrat-controlled. Companies have challenged over 100 of these NLRB opinions in federal court, and at least one case is pending in each of the 12 federal circuit courts. The courts will likely remand these cases to the Board for reconsideration.

"We are analyzing the impact that the court's decision has on Board cases in which the January 2012 recess appointees participated," said NLRB Chairman Mark Pearce, the only current Board member who served alongside the invalidated appointees. He also remarked that the Board "is committed to resolving any cases affected by [the Supreme Court's] decision as expeditiously as possible."

NLRB Opinions at Issue

While the majority of the 436 decisions are insignificant, several controversial opinions are noteworthy. Among these are *Albertson's, LLC*, 359 N.L.R.B. No.

continued on page 2

In This Issue

Noel Canning

continued from page 1

147, 196 LRRM 1453 (July 2, 2013); *WKYC-TV*, 359 N.L.R.B. No. 30, 194 LRRM 1289 (Dec. 12, 2012); *Banner Estrella Medical Center*, 358 N.L.R.B. No. 93, 193 LRRM 1161 (July 30, 2012); *Costco Wholesale Corp.*, 358 N.L.R.B. No. 106, 193 LRRM 1241 (Sept. 7, 2012); *Hispanics United of Buffalo Inc.*, 359 NLRB No. 37 (Dec. 14, 2012); and *Piedmont Gardens*, 359 NLRB No. 46 (Dec. 15, 2012).

The Board's *Albertson's*, *WKYC-TV*, and *Piedmont Gardens* decisions all are significant because they overturned decades-old precedent. *Albertson's* overruled *Wm. T. Burnett & Co.*, 273 NLRB 1084, 1086, 118 LRRM 1502 (1984), holding that soliciting grievances may be unlawful under the National Labor Relations Act, even if the solicited employee declines to raise a grievance in response. In December 2012, the Board found in its *WKYC-TV* opinion that employers were required to continue deducting union fees from worker paychecks per the arrangement set forth in the governing collective bargaining agreement, even after that collective bargaining agreement had expired. The ruling flew in the face of precedent dating back to 1962, which said that employers could stop deducting union dues after the applicable contract had ended.

The NLRB also handed down its *Piedmont Gardens* decision in December 2012, which overturned a long-established rule insulating companies from being forced to provide unions with witness statements concerning employee discipline. The Board eliminated a "categorical exemption" that protected the confidentiality of witness statements made in the course of an employer's internal investigation. In place of the exemption, the Board adopted a balancing test. Under the test, confidentiality is no longer guaranteed; instead, a statement will remain confidential only when a witness is reluctant to give an open statement due to the risk of intimidation, harassment, or other threatening circumstances.

The Board's July 2012 *Banner Estrella Medical Center* opinion is noteworthy because of its significant consequences for employers. The Board struck down Banner Health System's policy that prohibited employees from discussing ongoing investigations into potential employee misconduct. The Board held that an employer's interest in maintaining an internal investigation's integrity did not outweigh the potential restrictions the policy imposed on an employee's right to concerted action. This decision impacts any private-sector employer, regardless of whether its employees are unionized.

Two additional controversial opinions issued under the invalidated appointees, *Costco Wholesale Corp.* and *Hispanics United of Buffalo Inc.*, concerned social media policies. In September 2012, the Board ruled against Costco Wholesale Corporation's social media policy as overly broad, because it could be construed as a ban on employee criticism of the company or its working conditions. In December 2012, the NLRB issued another social media-related decision, finding against Hispanics United of Buffalo, Inc. for firing five employees who responded on Facebook to a coworker's remarks on their job performance. The NLRB found that the Facebook posts constituted protected concerted action under the National Labor Relations Act, despite the company's assertion that the employees were fired for harassing a coworker.

While the decisions issued during the tenure of the invalidated

continued on page 12

Matthew C. Lonergan is a partner with Bradley Arant Boult Cummings LLP in Nashville, TN, and practices almost exclusively in the area of labor relations and employment law on behalf of management. He can be reached at mlonergan@babc.com or 615-252-3802. **Anne Knox Averitt** is an associate at the firm, resident in the Birmingham, AL, office. She can be reached at aaveritt@babc.com or 205-521-8621.

The Corporate Counselor® (ISSN 0888-5877) is published by Law Journal Newsletters, a division of ALM.

The Corporate Counselor P0000-233
Periodicals Postage Pending at Philadelphia, PA
POSTMASTER: Send address changes to:
ALM
120 Broadway, New York, NY 10271
Published Monthly by:
Law Journal Newsletters
1617 JFK Boulevard, Suite 1750, Philadelphia, PA 19103
www.ljnonline.com

The EU 'Right to Be Forgotten' Google Judgment

By André Bywater & Jonathan Armstrong

In mid-May, the European Union's highest court, the European Court of Justice, handed down a controversial landmark ruling in a matter commonly referred to as the "right to be forgotten" case, concerning Google. The core of the case concerns the obligations of search engine operators under the EU Data Protection Directive. But at a wider level, the ruling's ramifications go beyond the EU, as it imposes extra-territorial privacy obligations on U.S. businesses. U.S. corporate counsel therefore need to be aware of the legal compliance impact that it may have on U.S. businesses.

Background

The background to the case is straightforward enough. In 2010, a complaint was lodged by a Spanish national, Mario Costeja González, with the Agencia Española de Protección de Datos ("the Spanish Data Protection Agency") against La Vanguardia Ediciones SL ("La Vanguardia"), a Spanish newspaper publisher, and two companies, Google Spain and Google Inc. Mr. Costeja González was unhappy that when Internet users entered his name into the Google search engine, the list of results would display links to two pages of La Vanguardia dated January and March 1998. Those particular two pages contained an announcement for a real-estate auction organized following attachment proceedings for the recovery of social security debts owed by Mr. Costeja González. According to Mr Costeja González, these proceedings had been fully resolved a number of years ago and so reference to them was now consequently entirely irrelevant.

Mr. Costeja González made two requests in his complaint. The first was that La Vanguardia either remove or alter the pages in question, so that personal data relating to him would no longer appear, or to use certain tools made available by search engines in order to protect the data. The second was that that either Google Spain or Google Inc. remove or conceal the personal data relating to him, so that it would no longer appear in the search results and in the links to La Vanguardia.

The Spanish Data Protection Agency rejected the complaint against La Vanguardia, on the basis that the information had been lawfully published by the latter. But, the Agency upheld the complaint against the two Google companies, and accordingly requested the companies to, in effect, remove the data in question and to make future access to the data impossible.

In response, the Google companies brought actions against the Agency's ruling in the Spanish High Court which then referred the matter under the EU's so-called preliminary ruling procedure to the European Court (based in Luxembourg) for interpretation of certain provisions of the EU's 1995 Data Protection Directive in order for the Spanish court to be able to resolve the dispute at hand.

Processing

The European Court ruled that the nature of the activities of a search engine qualify it as "processing" personal data under the EU Data Protection Directive. By searching automatically, constantly and systematically for information published on the Internet, the operator of a search engine is considered under the Directive as collecting data. The operator, within the framework of its indexing programs, retrieves, records and organizes the data in question, which it then stores on its servers, which, where applicable, it discloses and makes available to its users in the form of lists of results. Those operations are to be considered as "processing" under the Directive, regardless of the fact that the operator of the search engine carries them out indistinctively in respect of information other than the personal data, even where the operations exclusively concern material that has already been published as it is in the media.

Controller

According to the European Court, because a search engine operator determines the means and purposes of the above-mentioned "processing," it qualifies as a "controller" of the "processing" under the EU Data Protection Directive.

Extra-Territorial Jurisdiction

The European Court ruled that the EU Data Protection Directive has extra-territorial jurisdiction application where the above-mentioned "processing" is carried out in the context of the activities of an EU-located branch or subsidiary of a business. Google Spain is a subsidiary of Google Inc. on Spanish territory and, therefore, according to the Court, an "establishment" under the Directive. Where data are "processed" for the purposes of a search engine operated by a business which, although it has its seat in a non-EU Member State, has an "establishment" (branch or subsidiary) in a Member State, the "processing" is carried out in the context of the activities of that "establishment," under the Directive: 1) if the "establishment" is intended to promote and sell, in the Member State in question, advertising space offered by the search engine; and 2) orientates its activity toward the inhabitants of that Member State, in order to make the service offered by the engine profitable.

Right to Be Forgotten

According to the European Court, when requested to do so, a search engine operator must remove links

continued on page 4

André Bywater and **Jonathan Armstrong**, a member of this newsletter's Board of Editors, are commercial lawyers with Cordery Compliance in London, where they focus on regulatory compliance, processes and nvestigations. Reach them at Jonathan.Armstrong@CorderyCompliance.com. and Andre.Bywater@CorderyCompliance.com.

EU Google

continued from page 3

to web pages that are published by third parties and contain information relating to a person from the list of results displayed following a search made on the basis of that person's name. This obligation also applies where the name, or information, in question, is not erased beforehand or simultaneously from those web pages, and even when its publication in itself on those pages is lawful. Public interest might override this concerning public figures, depending on the circumstances at hand.

Further, aggrieved individuals may make their requests directly to the search engine operators. But, it must be emphasized, this newly interpreted "right to be forgotten" exists within the context of EU Data Protection Directive criteria, *i.e.*, where the information in question is, in particular, inadequate, irrelevant or outdated. In that case, a request can be made to have a link removed from future search results. The "right to be forgotten" is therefore not absolute, but qualified to these types of circumstances.

Legal Effect of Ruling

European Court preliminary rulings are not appealable. Although technically speaking the ruling only legally binds the (Spanish) court that referred the case, the ruling has in effect the character of precedent on other EU Member State courts, without prejudice to the right of those courts to make requests for preliminary rulings on the interpretation of the Data Protection Directive.

Reaction

The ruling has met with criticism and raised a number of issues. The ruling itself does not accord with certain aspects of the earlier official Opinion of the European Court's Advocate General (who makes preliminary recommendations, but which are not binding on the Court) whose approach was more subtle and convincing concerning the key issues of data "controlling and, the right to be forgotten balanced against the freedom of expression and information. Criticism from the U.S. has understandably focused on this latter issue in what is seen as a legal culture clash of the trumping of (EU) privacy over the (U.S.) right to free speech. The technical-logistical challenges of deleting data and the consequent financial costs are inevitable issues. The extent of the role of search engine operators operating as quasi-censors or arbiters in deciding what is in the public interest and who is a public figure has been questioned. Whether the ruling will restrict the efforts of law enforcement investigations also raises concerns.

Next Steps

As can be imagined, immediately following the ruling there has been a deluge of so-called take-down (removal) requests made by individuals, principally to search engine operators but also to data protection regulators.

The most immediate next step was therefore Google's response, which was to put online a form allowing for search engine users to request the removal of, what Google has summarized as the Court's ruling, "results for queries that include their name where those results are inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed." Requests must be supported by valid ID, a URL for each link to be removed, and the appropriate justification for removal.

The evaluation of requests will consider whether results include outdated information or public interest in the information such as with regard to "financial scams, professional malpractice, criminal convictions, or public conduct of government officials." Information will not of course be totally removed online as it will always remain on the website in question — it will just be more difficult to find as it won't come up on search engine results.

Because the form requires proof of identity to be provided this has itself raised privacy concerns with regard to the "processing" of the personal data contained in the identification. It could well be that the form itself is open to challenge by national data protection regulators. The UK's Information Commissioner's Office (ICO) had recently said in the context of subject access requests that the recipient of a request cannot insist on its own form being used to the exclusion of any other valid form of request.

The Hamburg data protection commissioner (Germany has a local not national system for most data protection regulation), Johannes Caspar, has also criticized Google's form and the level of personal information it seeks on the basis that Google must only ask for personal data that is absolutely required for the purpose of verifying the individuals' identity and that other details should be redacted. Mr. Caspar also suggested that Google may cause more privacy issues with its new procedure by not being clear how long it would hold the new data before deleting the information.

Some national data protection regulators in the EU, like the ICO, have also publicly stated that they are giving search engines a period of grace to put in place systems to deal with take-down requests and that following this, their focus will be on cases "linked to clear evidence of damage and distress to individuals."

New EU Data Protection Rules

The European Court's ruling strengthens the hand of those in the EU backing "the right to be forgotten" under new proposed legislation. At the time that the EU Data Protection Directive was first proposed in 1990, the Internet and search engines were at a rudimentary stage of development and popularity. By 1995, when the directive was finalized, it did not really envisage the extent to which the use of the Internet and the activities of search engines would fall under its scope. Bringing data protection up-to-date is therefore one of the aims of proposed new EU data protection rules, in the form of an EU Regulation put forward by the European Commission.

continued on page 10

Collecting Social Security Numbers

By Nicole Pszczolkowski and L. Elise Dieterich

In the first six months of 2014, at least 96 significant data breaches were reported, compromising more than 2.2 million records, according to the Privacy Rights Clearinghouse. Of these breaches, at least 46 involved records that may have contained Social Security Numbers (SSNs). What the affected businesses may not know is that their mere collection of SSNs may have put them in violation of state laws, in addition to the liability they may now face for having failed to protect the SSN information.

Despite their limited original purpose, SSNs have become *de facto* national identifiers, frequently used as an authenticator in both the public and private sectors. In fact, no other form of personal identification plays a more significant role in linking together records that contain an individual's sensitive and confidential information. Ironically, the widespread use of SSNs as both an identifier and an authenticator is precisely what makes collecting and using the numbers so risky.

Not surprisingly, the fact that SSNs serve as the keys to unlock a host of personal, medical, and financial information about individuals makes them highly desirable to criminals, such as identity thieves. And, thanks to never-ending technological advancements, SSNs are increasingly being transmitted and stored electronically, vastly expanding nefarious actors' ability to wrongfully obtain them. Given this climate, numerous state and federal laws have been enacted to limit the collection, use and disclosure of SSNs.

Nicole Pszczolkowski is an associate in Kutak Rock LLP's Washington, D.C., office. L. **Elise Dieterich** is a partner and the leader of Kutak Rock's privacy and data security practice in D.C., and a member of this newsletter's Board of Editors.

As a result, the presence of customer, patient, or employee SSNs in your business records, whether collected intentionally for a specific business purpose or inadvertently as part of an unrelated request, adds yet another layer of potential data-related liability. Although most businesses understand that they should limit the disclosure of SSNs consistent with state and federal laws, they may be unaware of the state laws placing restrictions on businesses' ability to request, collect, or store SSNs in the first place.

This article suggests a framework for ensuring compliance with the majority (albeit not all) of the applicable state laws and avoiding the financial, legal and reputational damage that can occur when SSNs are improperly collected, used or disclosed.

An Overview of SSN Restrictions

While federal laws typically focus on limiting the use and disclosure of SSNs in specific circumstances, such as in connection with medical information (HIPAA), student information (FERPA), or credit information (FCRA), more than 40 states have enacted laws restricting the collection and/or use of SSNs.

Several of these state laws limit to varying degrees the purposes for which SSNs can be collected. Alaska, for example, categorically prohibits businesses from collecting SSNs unless for fraud prevention, medical treatment, or to perform a background check on an individual. The majority of states, however, still allow for the collection of SSNs under a broader set of circumstances, including in connection with an individual's employment and employment benefits, for law enforcement or other government purposes, and for verification of an individual's age or identity.

At least six states require businesses that collect SSNs to have some form of written privacy policy in place. Texas, for example, prohibits requiring an individual to provide an SSN, unless the requesting entity has in place a privacy policy, a copy of which is provided to the individual, that addresses: 1) how personal information is collected; 2) how and when the personal information is used; 3) how the personal information is protected; 4) who has access to the personal information; and 5) the method of disposal of the personal information.

Massachusetts requires businesses that collect SSNs (as well as other personally identifiable information) of any Massachusetts resident (regardless of where the business is located) to have in place a comprehensive written information security program (WISP) that satisfies stringent and detailed administrative, technical and physical data security requirements. For example, the Massachusetts law and accompanying regulations require WISPs for organizations that electronically store or transmit personal information to establish a computer security system that at a minimum includes: 1) encryption of all sensitive information; 2) secure user authentication and access control measures; 3) unauthorized use monitoring; 4) up-to-date firewall and malware protection; and 5) operating system security patches.

Additionally, all businesses' WISPs must include: 1) assessment on an ongoing basis of reasonably foreseeable internal and external risks to records containing personal information, and adoption of steps to mitigate those risks; 2) designation of one or more employees to maintain and monitor the WISP; 3) development of security policies for employees and the imposition of disciplinary measures for violations; 4) documentation of responsive actions taken in connection with breaches; and 5) a requirement that third-party service provider contracts mandate implementation and maintenance of the security measures set forth in the business's security plan.

Once SSNs are collected, both federal and state laws impose restrictions on companies' ability to use SSNs. The majority of state laws are similar to California's (California is often considered to be a bellwether state in the privacy arena), which

continued on page 6

SSNs and Privacy

continued from page 5

permits collection of SSNs, but prohibits: 1) public posting or public display of SSNs; 2) printing or electronically embedding an individual's SSN on a card required to access products or services; 3) requiring an individual to transmit an SSN over the Internet, unless encrypted or over a secure connection; or 4) printing an SSN on materials mailed to an individual.

Should Your Business Collect SSNs?

In view of these state and federal restrictions on the collection, storage, and use of SSNs, and the risk a business incurs when it has SSNs in its possession, it is strongly recommended that businesses collect and use SSNs only on an as-needed basis (*i.e.*, only when required to do so by federal or state law, or when no other form of identification will suffice). At a minimum, businesses should audit their data collection practices to determine in what context, and for what purposes, SSNs are being collected.

In many instances, SSNs are inadvertently collected when customers, patients, or employees are asked to submit necessary information, such as educational, medical, or veterans' records, that happens also to include the individual's SSN. If this is occurring, the business should make a conscious determination about whether the collection of the SSN is necessary, or whether that data element could be redacted from the form on which it appears.

If SSNs are being collected to provide a unique personal identifier for the customer, patient, or employee, businesses should consider developing their own internal identifier as a substitute for the SSN. Ideally, if your business has no compelling reason to have SSNs, there shouldn't be any SSNs in your electronic or paper files. Data you do not have cannot be breached!

If SSNs Are Necessary, How Should They Be Handled?

If the collection of SSNs is essential to your business, we recommend (and, in many cases, the law requires) the following "best practices" for handling such information:

Eliminate Public Display and Unencrypted Transmission of SSNs

- Never publicly post or display an individual's SSN.
- Never print an individual's SSN on any personal identification card or badge.
- Never print an individual's SSN on any piece of mail that is being sent to the individual.
- Never require an individual's SSN to be transmitted or used over the Internet unless the connection is secure and the SSN is encrypted.
- When possible, redact an individual's SSN when keeping a document on file or encrypt the SSN when storing electronically.
- Never require an individual's SSN to be used as a login or password on any Internet site.
- Note that even the last four digits of an SSN can be enough to enable identity theft — omit any reference to SSNs whenever possible.

Control Access to SSNs

- Limit access to records containing SSNs to only those who need to see the numbers for the performance of their duties.
- Never store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
- Avoid sharing SSNs with other companies or organizations, and use written agreements to protect confidentiality if sharing is necessary.

Protect SSNs with Security Safeguards

- Develop — and enforce — a written security plan for record systems that contain SSNs.
- Encrypt SSNs in electronic records and store hard-copy records and removable media (such as disks, tapes, or USB drives) in locked cabinets.
- Provide for secure destruction of all documents and electronic files containing SSNs when no longer needed.

Ensure Accountability for Protecting Safeguards

- Provide employees with training and written materials addressing their responsibilities in handling SSNs.
- Conduct risk assessments and regular audits of record systems containing SSNs.
- Designate someone at your company to be responsible for ensuring compliance with policies and procedures for protecting SSNs.
- Implement specific privacy policies to protect SSNs and make such policies available to your customers, patients, or employees whose SSNs you collect.

Additionally, it is recommended that you inform individuals from whom you collect SSNs of the purpose of the collection, the intended use, whether the law requires the SSN to be provided or not, and the consequences of not providing the number.

While following these guidelines will enable compliance with the majority of the current federal and state laws addressing the collection, use, and disclosure of SSNs, such actions may not ensure compliance with every applicable law, particularly in those states, such as Alaska, Texas, and Massachusetts, with the most stringent requirements. Moreover, each new high-profile data breach prompts legislators to reexamine businesses' data collection practices, and new privacy laws are enacted each year. To the extent your business has a need to collect SSN numbers, or is at risk for inadvertently collecting such information, consultation with privacy counsel and assessment of the specific laws applicable to the jurisdictions in which you operate should be undertaken on a regular basis.

Other Risky Data Elements

SSNs are not the only data element that can cause unexpected risks for businesses — others include ZIP codes, driver's license numbers, and cell phone numbers. For example, in 2011, the California Supreme Court in *Pineda v. Williams-Sonoma Stores, Inc.*, 51

continued on page 9

Immigration Compliance

Can You Afford to Do Without?

By Irina B. Plumlee

Many of us are guilty of complaining about our outdated immigration laws and burdensome processes of applying for immigration benefits for foreign workers and complying with a set of regulations that turn employers into makeshift cops responsible for creating barriers to illegal employment. With the dire and obvious need for immigration reform and the equally obvious slow move toward adopting a comprehensive (or, at this point, even a non-comprehensive) solution, some companies fatigued by the debate and hopeful for the slow enforcement choose to put immigration compliance on the back burner.

ICE Audits

As we are nearing the 30th anniversary of the 1986 law mandating Form I-9 Employment Eligibility Verification, there still is a sizeable segment of U.S. businesses that have not taken even the most basic steps to protect themselves in case of an Immigration and Customs Enforcement (ICE) audit. While this approach provides short-term savings of time and money, it has a proven track record of being highly detrimental to the business's future in the long- and even medium-term.

Irina B. Plumlee is a shareholder in the Dallas, TX, office of Munsch Hardt Kopf & Harr, P.C. Her practice focuses on business and family immigration, including international executive and managerial personnel transfers, investment-based (EB-5) immigration proceedings and U.S. work visas for professional workers, and employment and family-based permanent immigration proceedings, as well as on employers' I-9 compliance, and fairness in employment practices. She can be reached at iplumlee@munsch.com.

In the age of the increasingly aggressive I-9 compliance audits and "generous" fines imposed by ICE to settle immigration violations uncovered during its investigations, immigration matters are shifting from traditional handling by human resources professionals to in-house legal departments. With the increasing frequency of ICE's audits and severity of fines levied against violators, to say nothing about significant disruption to company operations due to auditors' visits, it is advisable to use legal expertise to audit the business's current practices and set legally sound policies and procedures before charging HR or administrative professionals with their implementation.

Since most of us did not devote law school years to an in-depth study of the Immigration and Nationality Act and, years after the United States Citizenship and Immigration Services (USCIS) replaced its predecessor, still refer to this government agency as INS, let us refresh a few key compliance rules and best practices.

Key Points

Every U.S. employer, regardless of size and whether it employs foreign workers or not, must complete employment eligibility verification and maintain Form I-9 for each employee hired after Nov. 6, 1986. While it is permissible to keep I-9 files in either hard copy or electronic format, these files should be kept separate and apart from individual personnel files. Additionally, it is advisable to keep I-9 records for current workers separate from those of former employees. In case of an audit, you do not want to inadvertently turn in records that are not subpoenaed.

The following rules should help put an efficient company-wide compliance system in place, regardless of business industry or company size:

- Establish clear employment eligibility verification procedures, assign HR or legal department personnel to be in charge, and assure training and follow-up training.
- Decide if the company will use E-Verify or another government system (*e.g.*, IMAGE) for the I-9 process.
- If the government system is not selected, determine whether I-9 compliance will remain manual/hard copy-based or electronic.
- Determine whether or not documentation presented for I-9 verification is to be copied, and clearly formulate any related policies or policy changes.
- Perform an in-house audit of I-9 files for conformity with the I-9 best practices, and plan and implement corrective measures. Assure that HR personnel is trained on appropriate I-9 correction practices and follows them consistently.
- Set a company-wide system for a twice a year I-9 self-audit and a reminder on your due diligence list to review I-9 files at the time of any corporate changes (*e.g.*, mergers, acquisitions, layoffs, and seasonal hiring surges)
- Schedule refresher training for HR and administrative professionals charged with I-9 responsibilities on a regular basis, using outside expertise as necessary, and keep records of all such training

As every U.S. employer is obligated to review documentation presented by every employee hired after Nov. 6, 1986, and to fully complete the latest edition of Form I-9 in effect at the time of hire, the strongest employment eligibility compliance policies are centered on a few basic points with related procedures set to support and implement them:

Three-Day Rule

Section 1 of Form I-9 should be fully completed for each worker on their first day of hire, and the I-9 process (*i.e.*, documents review and Section 2 execution by the company's representative) should be finished within three days of hire.

Accept Valid Documents Selected by Employee

During Section 1 completion, the worker should be given an opportunity to select one document from List A on the back of Form I-9, or

continued on page 8

Immigration Audits

continued from page 7

one document from List B and one document from List C. An employee chooses documents to present for verification, and the employer is legally obligated to accept facially valid documents. Importantly, offer letters and employment agreements should not list specific documents a new hire is to bring at the start of employment or any time thereafter. If the employer has a legitimate need to review documents that can also be used for I-9 verification (*e.g.*, a company-wide rule for Social Security Cards presented for payroll purposes or driver's license for certain positions), do not mix these otherwise legitimate requirements with the I-9 process, and clearly state the non–I-9 related reasons for these documents.

Maintenance and Upkeep

I-9 files, which contain fully completed and executed Forms I-9 and copies of documents evidencing employment eligibility (if the company copies documentation presented as part of the employment eligibility verification), should be kept separately from personnel records and other employer-maintained documentation. This includes I-9 files for current and former employees. Businesses with multiple offices may choose to keep the I-9 files in a centralized location or at individual offices. In case of an audit, the company should be given reasonable time to transport the I-9 files to the ICE preferred location.

Reverification

All documents presented for I-9 purposes should be unexpired at the time of verification. Identity confirming documents (*e.g.*, driver's license) do not need to be re-checked upon expiration. However, temporary employment-authorizing documents (*e.g.*, Employment Authorization Document or EAD) should be calendared for re-verification by the their expiration time. When performing reverification, an employer should not request or require that a renewed document be presented. Instead, the worker should be allowed to decide which documentation from List A or from Lists B and C to present. The employer's representative should complete Section 3 of Form I-9 at the time of reverification.

Store

Each worker's I-9 file should be retained throughout their tenure at the company. Upon the employee's departure, the I-9 file should be kept for one year from the date of employment termination or three years from the date of hire, whichever comes later.

Purge, When Allowed

Purge I-9 files upon the mandatory record maintenance period completion as per the above, but even outdated records should not be destroyed upon an audit subpoena issuance.

Perform Self-Checks

An in-house audit is the best way to ensure your records are in order and to avoid last-minute efforts to comply when auditors are at the door. It is advisable to perform in-house audits every six months and immediately after any significant business changes, such as hiring surges or layoffs. Provide annual training and refresher training to I-9-responsible personnel.

Exercise Due Diligence

Include I-9 review in your due diligence list when preparing for a merger or acquisition of another company or its employees. The law allows an acquiring entity to "inherit" the purchased business's I-9 records, but remember that this also means inheriting all related liabilities.

Act in Good Faith

Properly maintained I-9 compliance procedures and records protect businesses, but only if your company acts in good faith. If the government proves that the employer has actual knowledge or reason to believe its employees lack legal status and are unauthorized to work, perfect documentary compliance will not help — and worse — may be viewed as evidence of concerted efforts to defraud. Supervisors' knowledge of an employee's illegal status would be imputed upon the company under the actual knowledge concept. Under constructive knowledge (*i.e.*, "the employer should have known"), credible information regarding unauthorized employment from trustworthy sources and/or I-9 files documentation with obvious deficiencies will be viewed as evidence against the employer.

Use Immigration Expertise

Have an immigration specialist on call in case of a tricky I-9 documents verification or if you are facing auditors. With short audit preparation timelines upon ICE's subpoena receipt (*i.e.*, three days), having counsel on standby will help you hit the ground running.

The Anatomy of an Audit

The hallmark of the day is that, irrespective of the industry or size of business, an employer may become a target of a random or not-so-random audit (*e.g.*, through a former or current worker's complaint or even a competitor's claim of unauthorized hiring). The current ICE audit approach is centered on an efficient and economically sound model, with the auditors serving a subpoena providing a three-day notice to produce the original I-9 files for the business and outlining documentation for provision, and issuing Notice of Fine upon the audit conclusion.

More often than not, a subpoena is not limited to the I-9 files, but also includes corporate documents including articles of incorporation, employee roster, and wage and hour records. A three-day notice is mandatory and standard, but, depending on the specific circumstances (such as a multi-office situation with I-9 files kept at headquarters), the notice period may be extended based on the subjective business needs. Importantly, extension of the notice period should not be taken for granted and needs to be negotiated with the auditors as quickly as possible.

Even the diligent employer that follows the recommended best practices of I-9 compliance should never waive the notice period and simply

continued on page 12

Halliburton

continued from page 1

While it will take some time to see how lower courts apply the decision, it seems likely to intensify defendants' focus on trying to defeat class certification through evidence, particularly experts' event studies, that rebuts claims that alleged misrepresentations affected the price of a company's securities. It was generally understood that defendants could take on this fight at trial or summary judgment. Having the chance to challenge price impact on a class certification motion, as *Halliburton* now permits, should be of real value to defendants.

The significance of the *Halliburton* decision arises from *Basic*. That case eased the burden that plaintiffs' lawyers had to meet in order to obtain class certification in a securities fraud action under Section 10(b) of the Securities Exchange Act of 1934, and Rule 10b-5. Instead of requiring each investor in the class to prove that he or she had relied on the alleged misstatements, *Basic* created a presumption of reliance — not on any particular statement by a company in its financial statements or SEC filings, but rather, reliance on the fact that all available public information was reflected in the company's stock price.

Eric Rieder is a partner in the New York office of Bryan Cave LLP. A member of this newsletter's Board of Editors, Rieder has broad experience as a litigator in securities and other commercial cases and as an adviser on the duties of directors and officers of both public and private companies. He can be reached at ERieder@bryancave.com.

The Majority Opinion

In declining to overturn *Basic*, the majority opinion, written by Chief Justice Roberts, invoked *stare decisis*, the principle against overruling precedents absent "special circumstances." It also rejected what it said were mischaracterizations of *Basic* by the defense side advocates: "Halliburton's criticisms fail to take *Basic* on its own terms." The Court was also unmoved by defense arguments that the *Basic* presumption encourages the filing of meritless claims that impose significant costs on businesses and consume judicial resources, stating that those concerns would be better addressed by Congress. The majority also emphasized that the *Basic* presumption was a rebuttable one from the start, and that *Basic* only concluded that most, not all, investors, rely on market efficiency.

In addition to failing to overturn *Basic*, the defendants also lost in their effort to have the burden placed on plaintiffs seeking class certification to prove that the defendants' misrepresentations actually affected the stock price, or caused price impact.

Where the defense bar succeeded was in its quest for a rule that permitted defendants to "rebut the presumption of reliance with evidence of a lack of price impact, not only at the merits stage — which all agree defendants may already do — but also before class certification."

That evidence would come in the form of "event studies," which are regression analyses concerning how the market price of issuers' stock responds to various publicly reported events. Both plaintiffs and defendants in securities cases that get past the motion-to-dismiss stage already use these studies. Plaintiffs, the Court noted, use them to demonstrate how the market for a company's stock considers material public information. Defendants counter with their own studies. While the *Halliburton* plaintiffs' lawyers did not dispute that defendants could use event studies on a class certification motion to address general market efficiency, they argued that such studies should not be considered with respect to actual price impact until a merits determination on summary judgment or trial.

In its key holding, the Court rejected this argument and held that defendants may use event studies to refute price impact at the class certification stage.

Conclusion

Considering how vigorously *Halliburton* was contested and the large number of business and investors' advocates who weighed in, it was striking that the Court issued an opinion with no dissents. But that did not evidence unanimity. Justice Thomas, joined by Justices Scalia and Alito, issued a concurrence that made clear those three thought the Court should have gone further and overruled the fraud-on-the-market theory adopted in *Basic*. Justice Ginsburg, joined by Justices Breyer and Sotomayor, issued a one-paragraph concurrence saying she joined the majority on the basis that defendants still bore a key burden in opposing class certification. Justices Kennedy and Kagan simply joined in the Chief Justice's majority opinion.

—❖—

SSNs and Privacy

continued from page 6

Cal. 4th 524 (2011), held that ZIP codes are "personal identification information" subject to protection under the state's Song-Beverly Credit Card Act of 1971. Similarly, two years later, the Massachusetts high court deemed ZIP codes "personal identifying information" in *Tyler v. Michaels Stores, Inc.*, 464 Mass. 492 (2013).

Another key judicial decision involving the collection and use of ZIP codes is expected soon in a case that was pending in the U.S. District Court in Massachusetts at press time. In *Alberts v. Payless Shoesource, Inc.* (D. Mass. Case No. 1:13-cv-12262, filed Sept. 12, 2013), Payless Shoesource, Inc. moved to dismiss a putative class action on the basis that its customers voluntarily provided their ZIP codes when asked at checkout, and the ZIP code information is stored in a database separate and distinct from the credit card transaction forms — thus, Payless argues, Massachusetts'

continued on page 11

EU Google

continued from page 4

As reported by one of these authors in the June 2014 edition of this newsletter (article available at http:// bit.ly/UktAl8), the EU is currently at an important stage in the process of overhauling the EU data protection rules, although final implementation might not be until 2016. In particular, the proposed Regulation contains a specifically set-out (qualified but not absolute) "right-to-be-forgotten" provision. Under this, a person will have the right to have his or her data erased when there are no legitimate grounds for the data to be retained, as long as this does not encroach on the freedom of expression and information.

In addition, not only will the proposed new Regulation apply where either a data-controller or processor, or, "data subject" (an identified or identifiable person to whom specific personal data relates) are based in the EU, but, in addition, the rules will also apply to businesses based outside the EU where they process data of EU residents who are offered goods or services — this extra-territorial reach has been very specifically spelled out. This all has to be put into the context of another aspect of the proposed new Regulation, which empowers data protection authorities to fine businesses that infringe the data protection rules (specifically including the "right to be forgotten") up to Euro 1 million or up to 2% of the global annual turnover of a business, whichever is the greater. These figures may be higher in the final version of the new rules.

The European Commission is of the view that the recent European Court ruling has vindicated the Commission's inclusion of the "right to be forgotten" in the new proposed Regulation, and has gone so far as to issue its own fact sheet on the ruling, concluding that the ruling makes the adoption of new EU data protection rules "more, not less, urgent." This said, not everyone has been comfortable with "the right to be forgotten," including persons at high political levels in some EU Member States. Therefore, its legislative introduction is not necessarily a foregone conclusion. Ironically the judge-led introduction of the "right to be forgotten" comes at a time when the Commission's proposed statutory "right to be forgotten" seemed to be losing some of its momentum.

Compliance Considerations

Corporate counsel will rightly be asking themselves at this stage how this ruling affects their business, especially as there is no equivalent "right to be forgotten" in the U.S., and the new EU law has yet to be finalized.

The outcome of the ruling is that individuals based in the EU have a stronger right and ability to control the dissemination of public information about them, which they can now in effect exercise extra-territorially and over a wider category of organization controlling data.

If your business is a search engine (with an EU connection) it will therefore clearly be directly affected and the most immediate practical consideration will be to develop solutions to removing links. The ruling has already, however, had a much wider impact than search engine businesses. For other businesses, maybe at a different point in the supply chain, there may be an issue as to whether for certain of their activities they could now be considered as data controllers who are processing data on people in the EU. They could also now be subject to EU data protection laws including the new "right to be forgotten."

From another perspective, if your company is making a search, for example, in the context of due diligence (with an EU aspect), there is now a distinct possibility that the search results may not be as complete as would be expected. In other words, if links have been deleted following the granting of take-down requests (which may be extensive if a search engine decides to play things as cautiously as possible) all the information expected to be captured in a due diligence exercise might not be there.

One area of particular concern here given the higher profile now given to corruption and bribery issues, is whether it will be more difficult to trace all the relevant information in this high-risk area. Legislation in Europe like the UK Bribery Act 2010 has seen an increased focus on due diligence in a commercial setting and some sectors like financial services have seen increased regulatory activity in this area of their business. One solution would be to undertake more in-depth due diligence where appropriate in order to ensure compliance, but this will likely be more resource-intensive and costly.

Another speculative issue is whether at a later stage, the ruling could be extended (through a further preliminary ruling process) to going beyond removing a link to the information, and widened to include the information itself. The current ruling has ruled this possibility out, but this does not mean that in certain particular circumstances (as yet unforeseen) removing the information might have to be undertaken. In the meantime, certain individuals might try this now anyway, as Mr. Costeja González did in the case itself.

By way of general legal risk reduction, this ruling is also a timely reminder of the need for any business to refresh its official data retention and destruction policies and check on what information the business retains and what it should delete where no longer needed.

And as a final ironic reflection, if you don't want to be forgotten, type into Google the surnames Costeja González.

—❖—

SEC Narrowly Adopts Money Market Fund Reforms

Years of debate between regulators and the securities industry dating back to the financial crisis came to an end on July 23 when the Securities and Exchange Commission (SEC) narrowly approved rules aimed at lessening the risk of investor runs on money market funds, Reuters reported.

The Commission approved the new rules in a 3-2 vote. Commissioners Michael Piwowar, a Republican, and Kara Stein, a Democrat, cast the two no votes.

The new rules require prime institutional funds to do away with their fixed $1 share price and float in value. All money funds will also be permitted to impose fees for investors to redeem their shares and temporarily block investors from withdrawing cash at times of market stress, *The Wall Street Journal* reported.

"Today's reforms fundamentally change the way that money market funds operate. They will reduce the risk of runs in money market funds and provide important new tools that will help further protect investors and the financial system," SEC Chair Mary Jo White said in a statement. "Together, this strong reform package will make our markets more resilient and enhance transparency and fairness of these products for America's investors."

Prime funds invest in short-term corporate debt. The new rules — with which companies will have two years to comply — will only apply to prime funds that cater to large, institutional investors. Those sold to individual investors will be able to keep the stable $1 share price. Money funds that purchase short-term Treasurys and debt issued by government agencies will also remain unaffected by the floating share price requirement, *The Wall Street Journal* reported.

"Today's adoption of final money market fund reforms represents a significant additional step to address a key area of systemic risk identified during the financial crisis," Norm Champ, director of the SEC's Division of Investment Management, said in a statement. "These reforms are important both to investors who use money market funds as a cash management vehicle and to the corporations, financial institutions, municipalities and others that use them as a source of short-term funding."

However, there are those who believe the new rules make money funds no longer appealing. The U.S. Chamber of Commerce has argued that the changes have made money funds more complex to use, because a floating share price requires corporate investors to pay taxes on gains and losses. Corporations are now also at risk of losing principal if a fund's share price declines, *Investment News* reported.

Commissioner Stein expressed concern that the prospect of fees or losing access to their money during times of market stress could cause investors to flee preemptively.

"If investors are not able to redeem before the gate comes down, they will be harmed as they are deprived of access to their capital," Ms. Stein said, according to *Investment News*. "Ultimately, this contagion could freeze the wholesale funding markets in much the same way as occurred during the recent financial crisis."

The Financial Stability Oversight Council — a panel of regulators created by the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act — urged the SEC to move forward with money market fund reforms, but has also expressed concern about the restrictions on investor redemptions. The panel has said it will examine the SEC's new rules..

According to the SEC statement, the rules will become effective 60 days after their publication in the Federal Register, and the reproposal will have a 60-day public comment period after its publication in the Federal Register. **— Isobel Markham**, Law.com

—❖—

SSNs and Privacy

continued from page 9

prohibition on requiring customers to provide their ZIP codes in order to complete a credit card transaction does not apply.

Additionally, the use of cell phone numbers collected from customers for "robocalls" has generated class action litigation — and major settlements — in a number of recent cases. Companies settling in the past year include giants such as Bank of America, JP Morgan Chase, and Papa Johns Pizza.

Also of particular interest to merchants are laws such as the one enacted in Texas, which imposes collection, use and disclosure limitations, as well as destruction requirements, on businesses that collect and use driver's license numbers. Continue to check back with *The Corporate Counselor* for future articles providing guidance on businesses's collection and use of these and other data elements.

Conclusion

Bottom line? In this era of hackers, big data, and ever more restrictive state and federal privacy laws, no data element that is connected to an individual is entirely benign. Data collection, while essential, has become inherently risky for businesses, and SSNs are just one example of why now, more than ever, businesses should be educating themselves about the privacy laws, and assessing their data collection, storage, and use practices.

—❖—

Noel Canning

continued from page 2

appointees' service are easily identifiable, the NLRB's trouble may not be limited to that window. The Board may additionally face challenges of opinions issued after the invalidated appointees had resigned. To the extent that NLRB decisions issued after August 2013 relied on the "precedent" of the opinions handed down by a quorum-less Board, these new decisions may now be subject to collateral challenge even though they were issued under a quorum of rightfully appointed Board members.

Déjà Vu

The Board has faced a similar predicament before. In 2010, the Supreme Court handed down its *New Process Steel* opinion that the NLRB could not conduct official business without a quorum of three validly appointed members. *New Process Steel, L.P. v. NLRB*, 130 S. Ct. 2635 (2010). Following that ruling, the Board had to reconsider approximately 600 decisions. In that scenario, the Board simply invited litigants to file motions for reconsideration based on any factual developments since the issuance of the original decision. The Board is likely to follow a similar procedure in light of *Noel Canning*.

Considerations for Employers

The National Labor Relations Act imposes no statute of limitations for appealing a Board order, so an employer may still challenge an adverse determination issued during the invalidated Board appointees' tenure. Before moving forward, however, employers should consult with counsel to fully understand which NLRB rules are invalidated by *Noel Canning*. If the NLRB can show that the rule articulated in a decision was in existence prior to January 2012, *Noel Canning* is unlikely to affect the validity of the rule.

Conclusion

When deciding whether to challenge an NLRB decision, an employer must weigh the costs that such a challenge will carry with it. An employer should consider, for example, the expenses of litigating the matter against the NLRB, the potential disruption to the workplace, and the costs of rewriting and distributing employment policies. While *Noel Canning* may provide legal footing for an employer to challenge a ruling, it does nothing to mitigate the costs and potential complications of bringing that challenge to bear.

—❖—

Immigration Audits

continued from page 8

turn over the subpoenaed records to the auditors. Rather, the subpoena should be reviewed with in-house attorneys and immigration counsel. The way you use the three-day notice period could make a substantial difference to the audit outcome.

First, assess the current state of I-9 compliance. With the limited amount of time at your disposal and depending on the number of workers at your company, the best approach is to initially review a representative sampling of I-9 forms and accompanying records. If the review indicates deficiencies, the three-day notice period can be used to correct certain mistakes and even to belatedly complete I-9 forms when they are missing in their entirety. Importantly, all corrections must be initialed and dated with the current date, so the auditors are not misled regarding their timing, and the company is not accused of acting in bad faith. Even the belated efforts, if performed correctly, should provide the company with some credit for its efforts to self-correct. Additionally, it is important to determine whether or not all subpoenaed non-I-9-file-related documents are requested legitimately, and whether an argument can and should be made regarding their production.

Upon presenting the I-9 files to auditors, you may have to await the audit outcome for a few weeks or even months. This waiting time is best spent performing a post-audit self-assessment, establishment and implementation of comprehensive immigration compliance practices as per the discussion above, and, importantly, making strategic decisions if audit documentation preparation has indicated a problem with unauthorized workforce.

Often, as the I-9s are turned in to the auditors, the company has already benefited from immigration counsel's expertise and determined that a segment of the workforce is unauthorized. In case of the latter, it is easy to predict that one of the audit outcomes would be the loss of the illegal workers. This is where strategic planning for the remedial measures and future business operations, as well as prior employment policies and procedures, become critical. Importantly, the way you approach this important junction may help or hurt the company when the auditors return with the Notice of Fines. The proper post-audit measures and diligent compliance efforts may affect the outcome of settlement negotiations with the government.

Conclusion

A comprehensive immigration reform will, hopefully, arrive, but in the meantime, taking a back seat to the immigration compliance is a costly and misguided decision for any business to make. When an I-9 compliance program is broken down into clear, gradual steps, the time invested in this effort pays off generously when ICE is at your door.

—❖—