LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 29, Number 3 • June 2014

EU Data Protection Reforms Update

European Parliament Progress

By André Bywater

Corporate Counsel would do well to familiarize themselves with the ongoing process of reforms to the EU data protection rules due to their eventual compliance impact and because they constitute more than a simple upgrade to the existing rules. These reforms will affect not only U.S. businesses that currently have EU operations, but also any U.S. businesses without EU operations that are nevertheless active on the EU market and handle personal data. The aspect of the reforms that specifically deal with the rules on data transfers between the EU and the U.S. will also be affected, and have been the focus of particular EU political attention.

The proposed reforms to the EU data protection rules have advanced through the EU legislative pipeline with the March 2014 plenary vote by the European Parliament approving the amendments made at its committee level. Generally speaking, the Parliament has left the constituent elements of the original proposed reforms intact and has instead focused on qualifying a number of aspects and introducing some new elements.

continued on page 8

Upcoming FLSA Changes: What Corporate Counsel Need to Know

By Joseph G. Schmitt

President Barack Obama recently issued a memorandum to the United States Secretary of Labor directing the Department of Labor (DOL) to propose revisions to modernize and streamline existing overtime regulations under the Fair Labor Standards Act (FLSA). Employers and employment law practitioners are now analyzing what changes are likely to be proposed, and evaluating how those changes might impact the workplace and employment litigation. The changes will likely have a significant impact on employers and their overtime obligations.

Salary Threshold

President Obama issued a "Fact Sheet" at the same time that he directed the DOL to propose revisions to the FLSA regulations. The Fact Sheet provides clues as to the ultimate direction the President wishes the DOL to take in revising those regulations. In particular, the Fact Sheet focuses on the minimum salary threshold that employers must pay to employees in order for them to qualify for one or more of the so-called "white collar" FLSA exemptions (the administrative exemption, professional exemption, executive exemption, and related exemptions). The current minimum salary threshold for the white-collar exemptions, $455 per week, was last raised during the Bush administration, in 2004. (Prior to that point, the minimum salary threshold had not been modified since 1975, when it was set at $250 per week.) As noted in the White House Fact Sheet, the current $455 minimum weekly salary is below the 2014 poverty line for workers supporting a family of four. At a time when the Obama administration is pushing an increase in the minimum wage for "non-exempt" hourly employees, this minimum salary threshold for exempt professionals is obviously problematic.

Given these observations, it is abundantly clear that the DOL's proposed revisions to the FLSA regulations will raise the minimum salary threshold for the

continued on page 2

In This Issue

FLSA

continued from page 1

white-collar exemptions. Commentators expect that the new minimum threshold will exceed $600, given that the $455 threshold from 2004 would amount to $561 in 2014 when adjusted for inflation. But given that the salary threshold has been revisited only once a decade (or even longer, such as the 30-year gap between 1975 and 2004), it seems probable that the DOL will propose a new minimum salary threshold that is significantly higher than $600, so as to keep the threshold at a reasonable level for the foreseeable future. It is even possible that the Department will propose some type of indexing of the new dollar figure, so as to ensure that the minimum salary threshold will increase at the rate of inflation in the future.

Regional Problems

One problem that is likely to confront the Department is the fact that the salary threshold is uniform across the country. The White House notes in its Fact Sheet that some states, such as New York and California, have already adopted minimum salary thresholds for exempt status under state overtime laws that are significantly higher than the federal threshold. Although the White House identifies this as a reason to increase the minimum salary threshold across the country, it also illustrates the fact that different regions may require different minimum salary thresholds. The cost of living in New York City is not the same as in Sioux Falls, IA; and the cost of labor is likewise very different in those two cities. If the DOL sets a minimum salary threshold that ensures that a worker will receive sufficient compensation to comfortably support a family of four in Los Angeles, that new minimum salary threshold may create an extraordinary burden for an employer in Peoria, IL. The DOL will need to be cautious in establishing a new minimum salary threshold that works for the entire country, and not merely for the coasts.

Joseph G. Schmitt is a shareholder in the labor and employment group at Nilan Johnson Lewis PA in Minneapolis. He focuses his practice in representing management in counselling and litigation matters. Reach him at jschmitt@nilanjohnson.com or 612-305-7577.

Simplifying the Regulations

President Obama's Directive to the Secretary of Labor also suggests strongly that the proposed revisions to the FLSA regulations will extend beyond raising the minimum salary threshold for the white-collar exemptions. President Obama has specifically directed the DOL to consider "how the regulations could be revised to update existing protections consistent with the intent of the act; address the changing nature of the workplace; and *simplify the regulations to make them easier for both workers and businesses to understand and apply*" (emphasis added). The last of those items, simplifying the regulations and making them easier to apply, does not appear to be related to the salary threshold. The President instead seems to be instructing the DOL to make substantive changes to the regulations.

Simplifying the FLSA regulations, of course, is a laudable goal. President Obama is not the first United States Chief Executive to seek to accomplish this goal. Ten years ago, the Bush administration issued new regulations that were also ostensibly designed to simplify the application of the FLSA. However, the 2004 changes to the FLSA regulations ultimately added additional complexities and requirements to the white-collar exemptions. Most commentators have concluded that the revisions resulted in a regulatory scheme that was more complex and harder to apply than the pre-2004 regulations. It is not at all clear how the DOL will be able to simplify the regulations in the year 2014 and make them easier to apply when prior efforts to do so have had the contrary result.

continued on page 12

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

First-Amendment Defenses Against Whistleblowers

By R. Scott Oswald and David Scher

The First Amendment prohibits restrictions on speech, including compelled speech. However, mandatory disclosures have long been the linchpin of several major regulatory schemes. For example, publically traded companies are required to share information on the financial health of the companies with investors and with the SEC. Likewise, pharmaceutical companies are prohibited from advertising that their drugs provide certain medical benefits when those benefits have not been approved by the SEC.

Enter the whistleblower, who comes to believe that his company is not complying with certain provisions of regulatory schemes that would require it to disclose (or refrain from disclosing) information about the company's business, its products, or its services. The whistleblower discloses what he believes to be a violation and, shortly thereafter, is terminated by his company.

Most attorneys are familiar with what comes next. The employee files a lawsuit alleging retaliatory discharge under whatever statutes are available to him. Generally, the employee must demonstrate that his disclosure was impermissibly related to the termination decision. The employer, on the other hand, will seek to demonstrate that the termination had nothing to do with the employee's whistleblowing activity.

R. Scott Oswald is the managing principal and **David Scher** is a principal of The Employment Law Group, P.C., based in Washington, DC. Oswald handles all manner of employment discrimination cases, including those litigated under Title VII and the Fair Labor Standards Act. Scher focuses his trial practice on discrimination, *qui tam*, and whistleblower retaliation cases.

But in a case involving mandatory corporate disclosures, the employer may have another way to head the plaintiff off, even before dealing with causation. The employer may be able to argue that the complained-of activity was nothing more than an exercise of free speech, and that the plaintiff disclosing the corporation's exercise of free speech cannot be deemed protected activity. If the employer can convince the court that the employee's conduct was not protected, its decision to terminate cannot be "retaliation," and the employer will likely make quick work of the employee's claim.

Setting the Stage for a First-Amendment Defense

Cases in which the employer can rely upon First Amendment defenses are, for the most part, limited to those instances involving a corporate disclosure. To illustrate the point, it is actually helpful to first look to a criminal case involving off-label drug promotions.

In November 2009, at the conclusion of a jury trial in the Eastern District of New York, Alfred Caronia, a pharmaceutical sales representative, was found guilty of promoting the drug Xyrem for "off-label use." *United States v. Caronia*, 703 F.3d 149, 152 (2d Cir. 2012). Under the Federal Food, Drug and Cosmetic Act (FDCA), pharmaceutical companies are required to obtain FDA approval in order to distribute and market their drugs. *See* 21 U.S.C. § 355(a). Once approved, the pharmaceutical company may only brand their drugs in accordance with the FDA's approval. In other words, "the FDCA prohibits 'misbranding,'" or '[t]he introduction or delivery for introduction into interstate commerce of any ... drug ... that is ... misbranded.'" *Id*. at 154 (citing 21 U.S.C. § 331(a)). As stated by the Court of Appeals, "The government has repeatedly prosecuted — and obtained convictions against — pharmaceutical companies and their representatives for *misbranding* based on their off-label promotion." *Id*. at 154 (citations omitted) (emphasis added). At trial, the government produced tape recordings in which Caronia pitched to physicians the effectiveness of his company's drugs in treating conditions for which the drugs had not received FDA approval.

Thus, the issue in *Caronia*, according to the Court of Appeals, did not have to do with the company's branding, but rather Caronia's promotion of the drug for off-label uses. Relying on a recent Supreme Court ruling in *Sorrell v. IMS Health, Inc.*, 131 S. Ct. 265 (2011), a divided Court of Appeals found that the government's prosecution of Caronia rested on an understanding that the FDCA restricted speech, that the restriction was both content- and speaker-based, and, ultimately, that prohibiting promotions like those in Caronia was a violation of First-Amendment speech protections insofar as the government "cannot prosecute pharmaceutical manufacturers and their representatives under the FDCA for speech promoting the lawful, off-label use of an FDA-approved drug." *Caronia*, 703 F.3d at 169.

Enter the Whistleblower

Over the last few years, the False Claims Act (FCA), 31 U.S.C. § 3729, has proven to be an effective tool in combating off-label marketing, and its antiretaliation provision, 31 U.S.C. § 3730, has offered would-be whistleblowers with the protections needed to come forward. Though *Caronia* dealt with an individual facing one individual's criminal liability, most employment law, whistleblower, and pharmaceutical attorneys are aware of the risks for companies associated with off-label drug marketing. For example, in July 2012, GlaxoSmithKline agreed to pay $3 billion to settle allegations of, among other things, off-label marketing. *See* Press Release, Department of Justice, GlaxoSmithKline to Plead Guilty and Pay $3 Billion to Resolve Allegations and Failure to Report Safety Data (July 2, 2012) (available at 1.usa.gov/1jpi9lM).

Assume for a moment that *Caronia* involved a claim of retaliation under the False Claims Act. More

continued on page 4

Whistleblowers

continued from page 3

specifically, assume that a whistleblower learned of and disclosed Caronia's off-label promotion activity and that the company terminated him the very next day. Temporal proximity would suggest that the termination was in retaliation for whistleblowing.

But, as suggested above, the company may be able to demonstrate that the would-be whistleblower's disclosures relate to nothing more than the company's exercise in free speech. Indeed, injecting the whistleblower into *Caronia* illustrates just this point. The company can challenge the underlying regulatory regime while simultaneously attacking the whistleblower's protected activity. As noted, if the conduct in which the whistleblower engaged was not protected, his claim of retaliation will ultimately fail.

The Employee's Reasonable Belief

It seems that the employer's First Amendment challenge would, at least in this instance, prove fatal to the whistleblower's claim. Indeed, if the whistleblower complained of nothing more than the employer engaging in free speech, it seems unlikely that his claim of retaliation would prevail. Fortunately for the whistleblower, the courts have made clear that a plaintiff need only to "reasonably believe" that the issue he is investigating or disclosing could lead to false claims being submitted to the government. This same line of thinking pervades other whistleblower statutes, so it is important to understand exactly what it means.

In *Graham Cnty. Soil & Water Conservation Dist. v. U.S. ex rel. Wilson*, the Supreme Court stated that the FCA's anti-retaliation provision "protects an employee's conduct even if the target of an investigation or action to be filed was innocent." 545 U.S. 409 (2005). Various Courts of Appeals have interpreted this to require only that the employee had a "reasonable belief" that the complained-of conduct could lead to a viable claim under the False Claims Act. *See, e.g., Hoyte v. Am. Nat. Red Cross*, 518 F.3d 61, 71 (D.C. Cir. 2008).

In the context of the hypothetical described above and with the limited facts provided, it seems clear that the whistleblowing employee's disclosure could meet this "reasonable belief" standard. It is unlikely that the average employee would be able to distinguish between off-label promotion and off-label branding. Indeed, Caronia's conviction was only overturned by the Court of Appeals. It is unlikely that a court would find a whistleblower's belief that he was engaged in wrongful conduct "unreasonable."

Though this hypothetical involved only a pharmaceutical company, the same discussion can be applied in a variety of industries and regulatory regimes. Many corporations, regardless of the industry in which they practice and the statutes governing their conduct, are required to make mandatory disclosures to the federal government. An opportunistic employee who believes he or she is on the cusp of being terminated could rely upon these mandatory disclosure regulatory regimes to make a frivolous report and seek to insulate himself from termination.

For example, the SEC requires that a company disclose in its 10-k reports any ongoing litigation, but the rules allow for a carve-out for routine litigation incidental to the business. An employee could review the most recent 10-k report, note that the company has failed to disclose some minor legal claim against it, and disclose the existence of a missing legal proceeding to his or her managers. When the employee is terminated, he may have a claim of retaliatory discharge under the Sarbanes Oxley or Dodd-Frank Act.

Practical Considerations For Management Attorneys

So how does a company meet its obligation to investigate and remediate potential legal violations that its employees bring to its attention while preserving its right to defend employment claims that may result from its action in the wake of such employee disclosures? We believe that the answer lies in employee training. Continuing the above example, assume that only a couple of weeks before the opportunistic employee made his disclosures, he attended a company-sponsored training course that dealt with the SEC's mandatory reporting requirements. Likewise, imagine that the employer in the Caronia hypothetical scenario had circulated a memo distinguishing between off-label promotion and off-label branding. These might, at least arguably, be pieces of evidence to call into question whether the employee's belief was, in fact, reasonable.

With the Supreme Court's decision in *Lawson v. FMR LLC*, the number of companies embraced by whistleblower protection and securities laws is at an all-time high. 134 S. Ct. 1158 (2014) (finding Sarbanes Oxley's anti-retaliation provisions applicable to employees of contractors to publically traded companies). In short, we think that the answer to these cases involving an intersection between the First Amendment, mandatory corporate disclosures and whistleblowers lies less in challenging the regulatory regime and more in educating and cross-training employees.

On the other hand, such a defense will certainly not protect an employer that engages in false speech or misrepresentation, as such conduct will certainly fall within the embrace of the law. Robust training programs and internal compliance offices are key to ensuring that the company is in compliance with the laws, rules and regulations governing its industry, and that, when an employee comes forward with a frivolous retaliation claim, the employer is in the best position possible to defend itself during litigation.

—❖—

Predictive Coding and Keyword Search

Complements or Competitors?

By Adam Beschloss and James K. Jones

Litigation, investigation, and regulatory requests require in-house counsel to manage multivariate issues (legal and business) to effectively mitigate risk involving threats to reputation, finance, and even survivability. This must all be done within the confines of expedience and cost.

Well into the era of electronic discovery, few would argue against the value of technology to assist in this regard. Predictive coding, also referred to as "technology assisted review" or TAR, is the latest attempt at taming the electronic data behemoth that presents itself as millions of pages for review (and represents approximately 70% of discovery costs). Clearly, one cannot apply the same methods or technologies that were established when a matter involved boxes of paper to electronic data volumes that are now counted in terabytes. (This article only considers the review of language-based, unstructured data and not structured data, such as financial information or documents such as schematics.)

In-house counsel are often presented with a multitude of options by both outside counsel and eDiscovery vendors, and it can be difficult to digest this information and choose the best approach for a given matter, especially when faced with the strong opinions of a trusted law firm that has successfully used a technology or process before. While outside counsel will be tasked with actually implementing the process going forward, in house counsel can play a more involved role in the decision making process if they have a grasp of the right questions to consider. Is the use of traditional keyword searching to effectively cull and search a corpus now defunct? Is predictive coding inherently superior? What does predictive coding do differently than keyword searching and how can counsel design the most effective process around predictive coding?

Much of the discussion has forced attorneys and other laypersons (from the perspective of the science involved) to come to terms with concepts such as recall and precision, richness, confidence levels, confidence intervals, acceptable error rates, false positives and negatives, statistical sampling, algorithms, and other rather involved topics. "Acceptable error rate" is a particularly jarring concept for the practice of law, where attorneys strive for nothing less than perfection outside the realm of eDiscovery. This concept, however, is not the sole purview of machines. Human review is subject to these rules as well, as are keyword searching methods.

The advent of TAR with the express purpose of not reviewing certain documents, however, has pushed this topic to the forefront. "Technology-assisted review highlights, and renders eminently calculable (at least from a statistical perspective) … the fact that some number of relevant documents knowingly will not be produced" (Schieneman, Karl, and Thomas C. Gricks III, The Implications of Rule 26(g) on the Use of Technology-Assisted Review. *The Federal Courts Law Review*. no. 1 (2013): 243). It is worth stepping back from the trees of statistics, linguistics, and algorithms to see the forest, particularly as in-house counsel consider how money can best be spent to uncover salient issues and meet production obligations.

Predictive Coding

At a high level, predictive coding works as follows: A set of features is identified that is used to distinguish between relevant (R) and non-relevant (NR) documents. These features often include the frequency of occurrence of individual words, phrases, and sets of words that co-occur in documents. The reader may recognize similarity between what predictive coding is attempting and what a well-constructed keyword query ideally does. A key difference is that predictive coding automates this process. Of course, this automation does not happen by magic. The system must be trained.

As the system is trained, it determines which features best discriminate between R and NR documents. There are a variety of ways this is accomplished, but the primary methods include: 1) calculating the probability that a particular feature is associated with R or NR documents; 2) using the features to determine which documents are most similar to each other; 3) deriving rules from the features to make R/NR classifications; and 4) trying to draw a line that would best separate the R documents from the NR documents if you were to graph them according to their features. (The graph would actually be multi-dimensional and the "line" a hyperplane. We can add hyperplane separation theorem and Euclidean Geometry to the list of concepts that most lay people shouldn't need to talk about.)

Training

All of this is made possible through the training. This training is usually accomplished with "training" and "seed" sets. These sets are composed of documents known to be R or NR, and are used to train the system in identifying other documents like them (based on the features described above). You can't simply point the predictive coding engine at a document collection and say "do math and hyperplane separation and find me only (and all) the relevant documents."

We must instead turn to the oft-maligned entity, the human mind. The training regimen requires trainer(s) to code documents R and NR to train the system. Multiple trainers may be required due

continued on page 6

Adam Beschloss is director, business development in the New York office of QuisLex, where he designs and implements eDiscovery workflows for litigation matters and investigations. **James K. Jones** heads QuisLex's Legal Technology Group. The authors would like to thank **Phil Algieri**, associate vice president of Legal Services, for his contributions to this article.

Predictive Coding

continued from page 5

to time constraints and the number of training documents required, but this raises concerns about consistency. (This now adds repeatability, reproducibility, and measurement system analysis to our lexicon of concepts that lay people shouldn't have to talk about.) All of this can present a bit of a conundrum: If one knew where to find R documents to begin with, we wouldn't have to understand the arcane concepts of statistics and linguistics.

Creating a Model

Basically, the system needs a fundamental model of what R and NR documents look like to function. With this model, the system returns documents identified as matching the set of features found in the exemplar documents. The trainer(s) then agrees or disagrees with the identification and returns the results to the system. This continues until the system has the best fit for the model. Again, how do we find those initial "training" documents?

Finding the 'Training' Documents

One approach is to randomly sample documents from the unculled document population, and then have the trainer(s) code them as R or NR. This continues until the system has enough identified R documents that it can form the necessary model. The drawback is that the document population can be extremely large, while the "yield" or "richness" (*i.e.*, the percentage of R documents in the unculled pool) is typically very low. This necessitates a significant amount of manual review before the predictive coding system can perform well. Further, such an approach may not identify enough exemplar documents for the system to fully develop a model. The number of NR documents identified through random sampling is likely to be much higher than the number of R documents delivered to the trainer(s), prolonging the exercise.

Keyword Searches

Another approach involves using keyword searches to increase the likelihood of identifying R documents and consequently provide a richer set of data for initial training. While certain proponents of predictive coding may doubt the efficacy of this process, search terms can perform very well if properly constructed. The key is to not simply create a list of terms via guesswork, but to engage in a process involving custodial interviews, sampling and statistical validation, iterative refinement, intelligent application of Boolean search concepts in collaboration with search experts. In fact, many predictive coding systems allow the trainer to proactively identify particularly relevant documents with which it can supplement the model. Through the intelligent use of search as described above we can specifically target these documents. It may be that the "old" method is what provides efficacy to the "new."

An argument against the use of keywords to kick-start predictive coding is the fear of bias. Specifically targeting documents relating to known issues to form the training set may bias the system to recognize as relevant only these known issues while failing to identify important issues you may not have known to search for, but would be uncovered with a large random sample. The fear is that the system may code documents pertaining to the important but unknown issues as NR having never encountered documents of this type.

On the other hand, as responsive or relevant topics are often interrelated, it may be more likely for the trainer(s) to come across these unknown issues as they review the targeted set as opposed to happening upon them in a random sample. In short, even within a predictive coding regimen, a properly constructed keyword search may have real value, particularly when it comes to increasing the degree of relevant material in the initial training and seed sets and in effect, making better use of dollars invested.

Search terms can be used later in the process as well when further investigating the document population that has been "predictively" coded. If you are are only concerned with fulfilling your basic discovery obligations, it may be possible to engage in a review designed to simply validate the system's R/NR decisions. However, the "most relevant" documents as determined by the review technology may be routine, uninteresting documents that need to be produced, but aren't meaningful or case altering (aka, hot). Customized search strings (which can then be further refined by date, time, custodian, file type, etc.), however, can be very effective at examining specific issues. In this sense, keyword search again serves as a powerful tool.

Conclusion

Ultimately, there is nothing inherently best about any particular methodology. A technology or process is only valuable in terms of the ability to solve a particular problem. As effective as technology may be, no single tool (excepting human intellect) is appropriate in all circumstances. Understanding what tools to use, and when, is critical from both a legal and business perspective. Moreover, the ability to comprehend their efficacy relative to the nuances of a particular matter determines whether potential benefits are fully realized.

Technology, such as predictive coding, requires the involvement of highly trained attorneys, statisticians, linguists, and technologists. Effective keyword searching requires no less skill. It is only the practical application of technology (and knowledge) that will provide counsel with the confidence that they have done what is necessary from a strategic vantage point and met their 26(g) obligation. Whether this is affected by a review employing predictive coding, keyword search, or some combination of the two, is a decision that shouldn't be based on the general acceptance that only the newest technology is best, but on the specifics of the matter.

—❖—

The Rest of the Profit and Loss Statement

By Michael Goldman

This article is the ninth installment in an ongoing series focusing on accounting and financial matters for corporate counsel.

The first thing I do as I start writing each of these installments is pull out my old 1,300-page graduate school Intermediate Accounting textbook and refresh myself on the basics that should be taught about the topic I am discussing. I was totally shocked to find, however, that there are no chapters at all in the book for Expenses and most of the other elements of net income.

Based on the textbook, one would think that the only thing that mattered on the Income Statement was Revenues, which have been enshrouded in non-stop accounting controversy for over 30 years. Financial Accounting literature seems to marginalize the expenses of running a business, covering them broad-brush with the Matching Principal (account for the costs of generating revenue when the revenue is recognized) and the Consistency Principal (however you choose to account for Expenses, account for them consistently from one period to the next).

GAAP's failure to focus on Expenses flies totally in the face of my 30-years' experience as a practitioner — whether working as management, an outside accountant, an insolvency adviser, a business valuator, or a fraud examiner, expenses have always been a key area of focus and concern. Expenses are the tools that companies use to generate revenue. They are the most controllable thing for management, and hence where management can have the most short-term impact. Analyzing how a company spends its money tells you almost everything you need to know about its management and a lot of what you need to know about its future prospects.

Michael Goldman, MBA, CPA, CVA, CFE, CFF, is principal of Michael Goldman and Associates, LLC in Deerfield, IL. He may be reached at michaelgoldman@mindspring.com.

Financial Statement Presentation

Expenses tend to be clumped into broad categories on the Income Statement. The first category is called Cost of Goods Sold or Cost of Services, and represents the direct costs associated with providing the goods or services that generated the company's revenue. The definition of "direct" can vary from company to company. Plant management, freight costs, warehousing costs, design and purchasing costs, and engineering costs are all examples of costs that could legitimately be considered as either "direct" or "indirect."

Cost of Goods or Services Sold consist of labor, materials, and overhead directly allocable to what was provided to the customer. It is driven by input prices paid by the company, the level (volume) of activity, and the efficiency of the organization.

Gross Margin is the difference between what was sold and the direct cost of those sales. Other than revenue and net income, it is usually the number on the income statement that is most focused on.

Two companies that conduct every aspect of their business identically the same except for their accounting can report very different gross margins based on how they classify expenses. An analyst comparing gross margins across different companies would need to drill further into the Cost of Sales numbers to determine what is and is not included in them.

Selling, General, and Administrative expenses (SG&A) are all of the other ordinary costs of running the business that are not included in Cost of Sales or Cost of Services. These typically include salaries and benefits, occupancy costs, advertising, supplies, professional fees, and "corporate" expenses. Presentation on the financial statements can vary from one company to another based on management's interpretation of what is important to show.

Some companies clump so many different expenses into broad categories that it is very difficult to glean any useful information out of the totals presented. Others report in such minute detail that it is easy to lose the forest for the trees. A good medium is to report on key expenses (those that are really important to the business), separately and then lump the others together in broader categories.

There are a few different ways to categorize operating expenses, and again the only standards are reasonableness and consistency. Some of the different reporting formats used include:

- Functional (*i.e.*, Selling, Administrative, etc.);
- By type of expense (*i.e.*, payroll, benefits, occupancy costs, etc.); and
- By categorization of expense (*i.e.*, variable or fixed).

After operating expenses on the Income Statement, but before net-income, are non-operating items (interest, gain or loss on disposals of assets, etc.), non-recurring costs such as restructuring costs or casualty losses, and income taxes. These are all shown separately to help the analyst evaluate the performance of on-going operations.

Reality

Don't feel impotent if you can't learn much from a single Income Statement — top-level financial statements are usually very limited in how much information they provide. To gain a good understanding of how a company spends its money, it is usually necessary to get into deeper levels of detail. Knowing that a company's occupancy costs are high, for example, is not a very actionable piece of information. Being able to pinpoint which elements of occupancy costs — rent, property tax, utilities, maintenance, repairs, security, etc., is critical to evaluating and possibly correcting those high costs. The difference between having this information in a useful

continued on page 8

Accounting

continued from page 7

format or not usually depends on the quality of the company's Controller or chief accountant. If the financial reports aren't giving you the information you need, blame the Controller, not yourself.

Expenses can be good or bad, depending on whether they are really helping to generate income. If the CEO has a luxury car, for example, the costs related to the car are expenses. If the CEO is constantly visiting or transporting customers with that car and the customers are impressed enough to buy more because of it, then the money was well spent. On the other hand, if that car isn't generating income somehow, then it is still a business expense from an accounting standpoint, but a questionable one from a business perspective. Expenses need to be evaluated in the context of the overall business operations and environment.

There is an entirely separate (from financial accounting) branch of accounting, called Managerial Accounting, which focuses directly on the costs and expenses of running the business. Managerial Accounting is concerned with providing useful and actionable information to management, whereas Financial Accounting focuses on reporting to shareholders, creditors, and other outsiders. Managerial Accounting helps managers actually operate the business, while Financial Accounting reports on past performance. It will be covered in future installments of this series.

—❖—

EU Compliance

continued from page 1

Background

Just over two years ago, the European Commission initiated the process with the aim of comprehensively reforming the 1995 EU data protection rules. It is no exaggeration to state that the 1995 rules have been one of the EU's most widely impacting pieces of legislation, entailing significant compliance requirements for businesses both inside and outside the EU.

Although the 1995 rules are being replaced entirely, the core elements concerning privacy remain, the main EU motive for the reforms being to "strengthen individual rights and tackle the challenges of globalization and new technologies." The extent to which these issues are finally addressed remains to be seen, notably as regards new technologies.

André Bywater is a commercial lawyer with Cordery Compliance in London, where he focuses on regulatory compliance, processes and investigations. Prior to working in London he was Brussels-based for many years focusing on a multitude of EU issues across Europe and beyond, including working on EU-funded projects building the expertise and capacity of government ministries and agencies. Reach him at Andre.Bywater@CorderyCompliance.com.

One objective of the reforms is to introduce what the European Commission hopes will be a less administratively burdensome and costly regime for businesses, and, according to Commissioner Viviane Reding, who holds the EU Justice portfolio and is driving the reforms, "Following the U.S. data spying scandals, data protection is more than ever a competitive advantage." Some businesses might share this view but others may disagree. Whatever the final outcome, there will be a high level of compliance obligations to maintain along with financial and administrative costs for businesses.

The reform package consists of a Regulation that sets out a general EU framework for data protection, and, a Directive specifically concerned with protecting personal data processed in a law enforcement context. Both sets of proposals are long and complex, and the European Parliament has itself put forward an enormous amount of amendments, many of which may not be finally taken up.

The Regulation

The Regulation is the main focus of importance for businesses, and, by way of brief reminder, the key reforms set out in it along with the Parliament's proposals are as follows.

One-Stop-Shop

Using the format of a Regulation (as opposed to a Directive, as undertaken under the 1995 rules, which is subject to individual EU Member State implementation), there will be one set of EU-wide rules. Businesses established and operating in several EU Member States will only have to deal with a single national data protection supervisory authority (*i.e.*, the data protection regulator) in the country where they have their base; complainants will also only have to deal with the supervisory authority in their Member State.

The Parliament amendment goes further. Namely, it wants: 1) a lead supervisory authority responsible for the supervision of data processing activities of the "data controller" (the person or entity determining the purposes and means of the processing of personal data); or 2) the "data processor" (the person or entity processing personal data on behalf of the controller), in all EU Member States where the "processing of personal data" (any operation or set of operations which is performed upon personal data) takes place in the context of the activities of an establishment of a controller or a processor in the EU and the controller or processor is established in more than one Member State; or 3) where personal data of the residents of several Member States are processed.

Level Playing-Field

In what must be stressed as a very significant new element, the EU data protection rules will apply equally to EU-based and non-EU based businesses, *i.e.*, not only will the rules apply where either a data-controller or processor or "data subject" (an

continued on page 10

Court Orders Identity of 'Company Doe' Revealed

By Mike Scarcella

The sealing of the identity of a company that fought to block public access to a consumer safety report was improper, the Fourth Circuit Court of Appeals has held, ordering the disclosure of its name and publication of case documents.

Background

"Company Doe" [later self-identified as Ergobaby, a leading manufacturer of baby carriers], represented by Gibson, Dunn & Crutcher, sued in Maryland federal district court to prevent the Consumer Product Safety Commission (CPSC) from posting an incident report on a government-run online database of product complaints. The report, which is under seal, attributes the death of an infant to one of the company's products.

The company's lawyers argued that publication of its name would cause reputational and economic harm. The Gibson team also disputed the accuracy of the product incident report, which the safety commission intended to include online with tens of thousands of incident reports that involve other companies and products. A trial judge agreed to allow the company to litigate under a pseudonym.

Update

A three-judge panel of the U.S. Court of Appeals for the Fourth Circuit rejected the secrecy of the litigation.

"We hold that the district court's sealing order violates the public's right of access under the First Amendment and that the district court abused its discretion in allowing Company Doe to litigate pseudonymously," Judge Henry Floyd wrote for the panel.

Litigation conducted under a pseudonym, the court said, "undermines the public's right of access to judicial proceedings." Company Doe, the appeals court said, "failed to identify any exceptional circumstances to justify the use of a pseudonym."

A lawyer for Company Doe, Gibson litigation partner Baruch Fellner, said in a statement on behalf of the company that "we agree with both the district and circuit courts' statements that the CPSC report in question was false and misleading. Importantly, too, as has been noted by the courts, the product in question was not related to the death of an infant, and the CPSC is not pursuing any claims against Company Doe."

Fellner said that "if the name of Company Doe is revealed, both media and the public will readily understand that these false and misleading reports harm a company that has a perfect record of product safety."

What Happens Now?

The company could decide to ask the full appeals court to review the panel decision, or take the dispute to the U.S. Supreme Court. "We will review the court's decision to determine further action," Company Doe's statement said.

The records were not expected to be unsealed as of this writing. The Fourth Circuit did not immediately issue a mandate instructing the district judge to open up the court files.

Many of the documents in the case — including the nature of the product — are secret. Summary judgment motions and accompanying materials, the appeals court said, had been sealed "wholesale." The trial judge, Alexander Williams Jr., issued a public opinion "with redactions to virtually all of the facts, the court's analysis and the evidence supporting its decision," Floyd wrote.

The public, the Fourth Circuit panel said, has an interest in learning about case evidence in addition to the legal ground supporting a judge's ruling.

"Without access to judicial opinions, public oversight of the courts, including the processes and the outcomes they produce, would be impossible," Floyd wrote.

A corporation, Floyd said, "very well may desire that the allegations lodged against it in the course of litigation be kept from public view to protect its corporate image, but the First Amendment right of access does not yield to such an interest."

Scott Michelman of the consumer advocacy group Public Citizen, which challenged the sealing of the court records, called the Fourth Circuit decision a "strong vindication of the First Amendment."

The consumer groups argued, among other things, that Company Doe's decision to use the federal courts to challenge the public disclosure of the consumer safety report exposed it to the transparency of the judiciary.

"We want our courts to be open and accountable," Michelman said in an interview. "This ruling is very good for consumers. It makes it difficult to drag out in secret a challenge to a report of harm in the consumer product safety database."

Writing separately, Senior Judge Clyde Hamilton, who agreed with the disposition of the case, sympathized with Company Doe.

"Common sense tells us that some harm will befall Company Doe by the publication of the false and misleading reports at issue in this case," Hamilton said. "In the electronically viral world that we live in today, one can easily imagine how such publications could be catastrophic to Company Doe's fiscal health, allowing it never to recover."

But, Hamilton added, "First Amendment jurisprudence requires more than a common sense feeling about what harm may befall Company Doe."

—❖—

Mike Scarcella writes for *The National Law Journal*, an ALM sister publication of this newsletter.

EU Compliance

continued from page 8

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. The Parliament supports this and has left it relatively untouched. How this extra-territorial reach will work in practice though remains to be seen

'Privacy by Design' and 'Privacy By Default'

These will become essential compliance principles, meaning that data controllers will be legally obliged to ensure that data protection safeguards are built into products and services from the earliest stage of development, and that privacy-friendly default settings are the norm. The Parliament supports this and elaborates further by requiring that privacy by design address the entire lifecycle management of personal data, from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data.

Explicit Consent

Where consent is required for data to be processed, it will have to be explicitly given, *i.e.*, it is not assumed. Therefore, saying nothing will not amount to consent. The Parliament supports this and goes further in its amendments, for example, by providing that provisions on the data subject's consent that are partly in violation of the Regulation will be completely void.

The Right to be Forgotten, and Erasure

A data subject 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. The Parliament amendment goes further by allowing EU citizens to obtain from third parties (to whom the data have been passed) the erasure of any links to, or copy or replication of, that data. It also wants EU citizens to have the right to erasure where a court or regulatory authority based in the EU has ruled as final and absolute that the data concerned must be erased.

The Right to Avoid Profiling

Data subjects will have the right not to be subject to data processing intended to evaluate certain personal aspects relating to them, or to analyze or predict in particular their performance at work, their economic situation, location, health, personal preferences, reliability or behavior — subject to certain exceptions. The Parliament supports this, but with some modifications, including the basic way this right is expressed, stating that every natural person shall have the right to object to profiling and the data subject has to be informed about the right to object to profiling in a highly visible manner.

Data Portability

Data subjects will have easier access to their data and be able to transfer data from one service provider to another more easily. The Parliament has left this untouched.

Data Protection Officer

Data controllers and processors will have to appoint an internal data protection officer to oversee compliance where: 1) either data processing is carried out by a public authority or body; or 2) the processing is carried out by an enterprise employing 250 persons or more; or 3) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects. While supporting the appointment of a data protection officer, the Parliament prefers that a data protection officer will be appointed when the processing is carried out by a legal person and relates to more than 5,000 data subjects in any consecutive 12-month period.

Data Breaches

"Personal data breaches" are defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. Under the reforms, where there is a personal data breach, the controller must without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority will have to be accompanied by a reasoned justification in cases where it is not made within 24 hours. The Parliament supports the notification requirement but in a more limited way.

Sanctions

The reforms will empower supervisory authorities to fine businesses that infringe the data protection rules up to Euro 1 million or up to 2% of the global annual turnover of a business, whichever is the greater. The Parliament amendment goes further, raising the level of the fine to up to Euro 100 million or 5% of global annual turnover, whichever is the greater.

Impact Assessment and Risk Analysis

Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf will have to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

An example of such a situation is personal data in large-scale filing systems on children, genetic data, or, biometric data. The Parliament, however, favors more of a risk analysis of the potential impact of the intended data processing on the rights and freedoms of data subjects to determine whether the processing is likely to present specific risks. Those risks are, for example, where the processing of personal data relates to more than 5,000 data subjects during any consecutive 12-month period.

continued on page 11

EU Compliance

continued from page 10

Data Transfers to Third Countries

The core principles concerning the transfer of data from the EU to third countries (including the U.S.) will remain, most notably the requirement that such data flows can only occur where third countries ensure an adequate level of protection. What the reforms introduce is an extension of the existing principles. For example, the criteria against which protection adequacy are considered by the European Commission on its own are more explicitly detailed. In the absence of a Commission protection adequacy decision, data transfers may be made where other safeguards are in place.

Arguably the most notable of these are "Binding Corporate Rules," which essentially allow for intra-group compliance rules as approved by a supervisory authority, which are now explicitly provided for and also extended to data processors as well as data controllers. The criteria against which a supervisory authority approves "Binding Corporate Rules" are also more explicitly detailed. The other main form of safeguards are through the use of Commission-approved "Model Clauses," which are also now explicitly provided for. In the absence of such safeguards, data transfers may still be made according to certain conditions, which have also been revised and extended.

The Parliament broadly supports the changes adding some of its own extending amendments, and, in addition, it has proposed new elements concerning the situation where the courts or regulatory authorities in third countries require or request the disclosure of data from a data processor or controller. Although the reforms bring some clarity, implementing and complying with the various principles of data transfers to third countries may still present challenges to businesses.

These elements raise a number of issues, and, there is also much other detail in the Regulation that will need to be addressed in order for businesses to meet their compliance obligations.

The Politics

As the earlier quote from Commissioner Viviane Reding indicates, the reforms have taken a political slant due to the mass surveillance revelations made by whistleblower Edward Snowden. In November 2013, the European Commission officially voiced its concerns about the implementation of the "Safe Harbor" regime, the 2000 EU-U.S. policy agreement that regulates the way that U.S. companies export and handle personal data of EU citizens. The Commission highlighted various perceived U.S. shortcomings, including from the security perspective.

More politically radical, in March 2014, the European Parliament itself passed an official Resolution calling for the immediate suspension of the "Safe Harbor" regime until the U.S. better respects EU fundamental rights, although technically speaking, this competence rests only with the European Commission. However, in a more upbeat mode, EU and U.S. political leaders have reaffirmed a commitment to "Safe Harbor," which comes in the wake of the announcement by the Federal Trade Commission (FTC) about settlements with a dozen U.S. companies where it had been alleged that the companies had falsely claimed compliance with "Safe Harbor." Despite this more positive recent move, this EU political undercurrent of concern should not be viewed as a simple hiccup and is more likely to persist in one form or another in EU privacy policy developments.

In terms of next steps, the European Parliament's proposed amendments will be considered by the (EU) Council of Ministers. It is expected that the Council will start this month. Once the 28 EU Member States have agreed a position within the Council, the latter will then engage with the Parliament (which will be of a different composition after the May 2014 elections) and both bodies have to come to an accord in order for the reforms to become law; the European Commission (whose Commissioner composition will also change later in 2014) will continue to play a role as a kind of honest broker.

Once adopted, the Regulation would be applicable within a month, completely repealing the 1995 EU data protection rules in the process. Entry into force of the Regulation is a question for speculation right now, but, despite enthusiasm in certain EU quarters for this happening as soon as feasibly possible, it is not anticipated to occur until sometime in 2016.

Although finalization of the reforms may seem to be some time ahead, some compliance issues for corporate counsel and businesses to nevertheless consider are as follows:

- Forward-planning the implementation of comprehensive changes into their business and IT practices — for example, outsourcing arrangements entered into now are likely to be still in place once the new regime comes into place;
- Planning to put in place a privacy by design/default lifecycle policy into all products and services — this could be a selling-point for customers although it may be a two-edged sword as the administrative burden may also be high; and
- Concerning policies, procedures and documentation: 1) prepare to update everything, also bearing in mind that supervisory authorities have powers to request certain information; 2) review all key practical aspects such as data retention, destruction, etc., through all means of collecting data used by the business; 3) ensure that new aspects such as explicit consent, the right to be forgotten and erasure, and, the right to not be subject to profiling are all included; 4) put in place a data breach notification procedure, including detection and response capabilities; 5) where applicable, appoint a data protection officer; 6) where applicable, put in place an impact assessment and/or risk

continued on page 12

FLSA

continued from page 2

The Percentage Test

Nonetheless, if the DOL is looking to simplify the regulations, it is possible that it will do so by following the lead of several states, including California, which have adopted a percentage requirement for the white-collar exemptions. The current white-collar exemptions merely require that an employee's "primary" duty must be the performance of exempt tasks (*e.g.*, administrative duties involving the exercise of discretion and independent judgment, executive duties involving the management of subordinates, etc.).

The current FLSA regulations do not specify how much time the employee must spend performing such tasks in order to qualify for a white-collar exemption. Although employers obviously have an easier time defending exempt status if the employee spends the majority of his or her time performing exempt duties, various employers have successfully defended the classification of employees as exempt on the grounds that their *primary* duty was exempt, even though they spent less than 50% of their work time performing that duty. The percentage test would modify that standard and require that an employee must spend more than half of his or her work time performing exempt duties in order to qualify for an exemption. California is one of several states to have adopted a percentage requirement for the white-collar exemptions. Many commentators believe that the DOL will propose revisions to the FLSA regulations to adopt a similar percentage requirement for the white collar exemptions on a national basis.

Certainly the percentage requirement has an appealing appearance of simplicity. Proponents of the test argue that it is easier to measure how much time an individual spends on each of his or her tasks on a daily basis than to determine what duty is "primary." But if the DOL follows that line of reasoning and suggests a percentage test, employers and their counsel will face significant changes to the FLSA landscape. Employers will need to prove that exempt professionals spend more than 50% of their time performing exempt duties. Many employers will wish to begin documenting employees' time so as to prove that the employees are spending more than half of their time performing exempt duties. Employers may also elect to perform "time and motion" studies for key positions to obtain as much objective documentation as possible supporting the exempt nature of the employees' work. Such studies can be an effective defense to FLSA litigation, but they can also be costly, time consuming, and administratively burdensome.

Of course, the percentage test would not modify or remove the issues that typically are presented in any piece of wage an hour litigation. Employees typically argue that they are not given sufficient discretion to qualify for the administrative exemption, or do not have the authority to make executive decision so as to qualify for the executive exemption. Employees will still be able to make those arguments if a percentage test is adopted. Moreover, the imposition of a percentage requirement may actually make those issues more complicated and difficult to resolve.

Any time and motion study defense must consider not only how an employee spends his or her time, but also whether each duty qualifies as exempt work. Only after the employer establishes that a particular function qualifies as exempt work (*e.g.*, involves the exercise of discretion and independent judgment) can the employer then show that the employee spends most than 50% of his or her time performing functions that qualify as exempt work.

Ultimately, a percentage test would impose significant administrative burdens on employers who wish to classify employees as exempt under one of the white collar exemptions. It seems probable that a number of employers will conclude that the costs and administrative burden of meeting these new requirements are too great to justify classifying employees as exempt, and that those employers would therefore reclassify the employees as nonexempt and pay them overtime. It is also likely that the change will result in a significant increase in wage and hour lawsuits, an area of litigation that is already expanding quickly.

Conclusion

Given the prospect of these changes, employers and their counsel should carefully watch the DOL and assess the proposed revisions when they are ultimately published. Employers should strongly consider offering their opinions regarding those regulations as part of the notice and comment process. In 2004, the regulations ultimately adopted by the DOL differed from the initial proposal, likely as a result of the strong opinions expressed in a number of employer comments regarding the regulations. The DOL may be similarly responsive to feedback in 2014. Finally, of course, employers should be prepared to adapt to any revised regulations when they are ultimately adopted.

—❖—

EU Compliance

continued from page 11

analysis policy; 7) create compliance statements for annual business reports; and 8) train staff on all of the above.

Finally, it must be stressed again that non-EU based businesses that are active on the EU market and handling EU personal data will be affected and so they too will need to ensure that they are compliant.

—❖—