AN LRN® THOUGHT LEADERSHIP REPORT

Ethics & Compliance Alliance

Risk Forecast Report 2013

LRN® *Inspiring Principled Performance℠*

Contents

CLICK ARTICLE NAME
TO GO TO ARTICLE

The views and opinions expressed in this Report (a) are for informational purposes only and are intended to represent only educated forecasts, not predictions of future events; and (b) are not presented for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular legal or regulatory issue. In the case of opinions in this Report presented by a named author, those opinions are held by the individual author and do not necessarily reflect the opinions of that author's employer or firm.

Executive Summary

Ethics & Compliance Risk Projections for 2013

According to the recent LRN Ethics & Compliance Leadership survey, leaders say their top five risks for 2013 are Data Privacy, Bribery and Corruption, Conflicts of Interest, Electronic Data Protection, and Gifts and Entertainment.

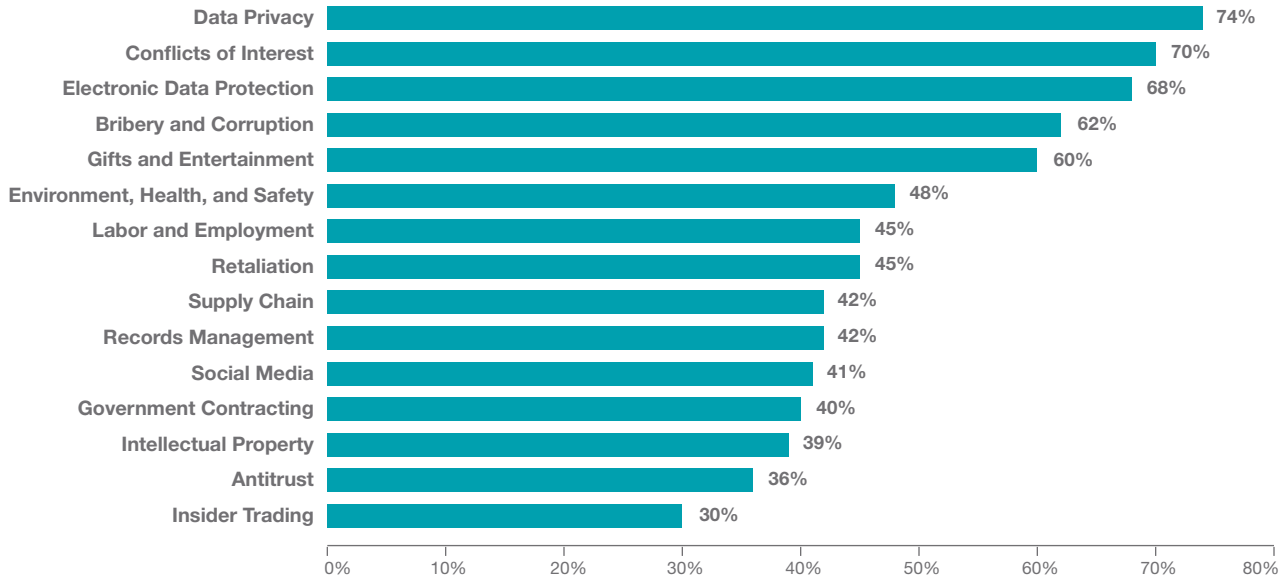
Ethics and compliance risks confronting organizations in 2013 have grown more complex and nuanced than ever before. In the year ahead, executives responsible for managing those risks will need to adapt to a legal and regulatory environment increasingly shaped by an array of economic and political pressures. Keeping pace will require companies to be smart, efficient, and laser-focused on motivating a diverse workforce to do the right thing.

Those are the primary themes that emerge in this 2013 Risk Report from the LRN Ethics & Compliance Alliance (ECA), a proprietary information platform for E&C professionals. In the pages that follow, you'll find top-level analysis and information on 11 different risk areas—from antitrust to social media—that present day-to-day challenges for most any organization. Our authors are experts in their respective fields, highlighting trends and new developments that have impact on E&C program management.

This collection of articles in some ways resembles an ethics and compliance Rorschach test, with each article likely to resonate in different ways within different organizations. The concerns of E&C professionals are diverse: according to the recent LRN Ethics & Compliance Leadership survey (conducted in December, 2012) leaders say their top five risks for 2013 are Data Privacy (74%), Conflicts of Interest (70%), Electronic Data Protection (68%), Bribery and Corruption (62%), and Gifts and Entertainment (60%). Overall, the profile of leading critical risks is generally consistent with what emerged in last year's survey.

Key E&C Risks Identified in Risk Assessment Process

Ranked by Percentage of Respondents N=151



The LRN leadership survey found that in 2013 most E&C leaders appear to be focusing on "defensive" goals, with an emphasis on improving risk management capabilities and third-party oversight. Encouragingly, however, two-thirds (66 percent) of E&C professionals say they are also striving to promote alignment between core company values and day-to-day operations; a similar percentage aim to increase employee comfort with speaking up about misbehavior.

Accomplishing those varied goals will require across-the-board commitments at all levels of a company, which means the job can't be done alone. "Compliance and ethics officers have so much on their plates that they can forget how their roles can overlap with others within the organization," observes Marcia Narine, a labor and employment expert writing in this report. Indeed, building organizational bridges—and ethical cultures—is never easy. But in 2013 it may be an essential strategy for E&C professionals as they plan for success in the year ahead.

Investigations and Prosecutions

Goals will require across-the-board commitments at all levels of a company, which means the job can't be done alone.

Helping employees and managers understand the implications of their actions is critical, even in areas that might not seem to affect the average worker. For example, ECA expert Ted Banks looks into his crystal ball for 2013 *(Antitrust and Competition Law)*, and advises that "given the potentially draconian penalties that can be imposed for a violation…continued antitrust compliance vigilance is essential."

A recent case in point: AU Optronics, a maker of liquid crystal display panels, was convicted in 2012 of price-fixing. Federal prosecutors sought a huge fine ($1 billion) and lengthy prison terms (ten years), but a judge imposed "only" a $500 million fine on the company, and three-year sentences plus $200,000 fines on convicted executives.

Compliance professionals, writes Banks, "must approach compliance from the employee's point of view. This means communicating in an employee's vernacular, not in lawyer-speak. It means explaining how compliance with antitrust laws will benefit the employee and the company. And it also means explaining how violating the antitrust laws will be detected, and an employee's job may be lost, and his or her life irreparably damaged. Employees should learn how to do their jobs properly because it is in their interest."

If misbehavior does occur, and fellow employees have knowledge of it, how should they react? Brad Bondi *(Hot Topics and Trends in SEC Enforcement)* points to a need for education on a new whistleblower program authorized under the Dodd-Frank Wall Street Reform and Consumer Protection Act, which he believes "has the potential to change the landscape of the SEC's enforcement efforts." The program offers whistleblowers who provide original information that leads to an enforcement action from 10 to 30 percent of the SEC's monetary recovery. The SEC reports that 3,001 whistleblower tips, complaints, and referrals were received during fiscal year 2012.

An important element of the program—and one that compliance professionals need to be especially mindful of—is that it specifically allows and incentivizes individuals to utilize internal reporting channels before going to the SEC. Among other provisions, the SEC rules provide that an internal whistleblower

may be eligible for an award where the company reports to the SEC information received from the whistleblower, or the results of an investigation initiated in response to the whistleblower's information.

Politics and a weak economy are factors in the risk profiles of government contractors, according to Eric Feldman *(Government Contracting and Relationships)*. He thinks the polarized U.S. political process has created "a near certainty" that 2013 will result in substantial challenges for government contractors at the federal, state, and municipal levels, requiring "unprecedented dexterity and prudent decision-making" to survive and prosper in a "new world order."

Ethics and compliance programs have become a competitive differentiator on government contracts, as agencies can ill afford to deal with ethics and integrity problems in either the bidding or execution phases of mission-critical projects.

With fewer contracting opportunities, Feldman writes, employees (particularly those in the contract "capture" process) may feel motivated to ignore or marginalize their company ethics and compliance programs and use whatever information is at their disposal—even prohibited government or competitor acquisition data—to give them an edge in the bidding process.

The good news is that strong ethics and compliance programs have become a competitive differentiator on government contracts, as agencies can ill afford to deal with ethics and integrity problems in either the bidding or execution phases of mission-critical projects. Says Feldman: "Proposals that incorporate ethics assessments, training, and education at the project level provide evidence of commitment to controls and accountability important to government agencies in this new environment."

Global Issues and Enforcement

In his analysis of *Anti-Corruption and Bribery*, Michael Fine reports that despite enforcement advances in other countries, the U.S. Foreign Corrupt Practices Act (FCPA) continues to drive risk assessment and mitigation planning at most multinational companies. "Although the U.K. Bribery Act is beginning to make its mark, speculation that it would displace the FCPA model and require wholesale changes to FCPA-oriented programs has not proven out," writes Fine.

The U.S. continues to lead the world in anti-bribery enforcement by a wide margin, according to Fine, with 233 concluded cases and more than 100 open investigations. That number was down slightly in 2012, with the U.S. Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) showing more selectivity on prosecutions and flexibility on settlement terms. Another notable development was the publication in November of a comprehensive "Resource Guide" to the FCPA, developed jointly by the DOJ and SEC.

"For risk managers, the essential message remains the importance of a comprehensive global approach to anti-bribery risk forecasting and compliance," advises Fine. "The challenge ahead will be to build and maintain effective global compliance programs that can capture relevant laws, reconcile differences…and, above all, communicate company standards and expectations to an increasingly diverse workforce."

For U.S. companies whose business is dependent on international sales, Marian Ladner *(Trade Compliance)* reports that the Obama Administration's efforts to reform the U.S. export control system remain the dominant theme in the export trade compliance field.

With the President's reelection, Ladner says, it is expected that the Export Control Reform (ECR) Initiative will now move to the final rule stage, and that export jurisdiction over many items will be transferred from the U.S. State Department to the Commerce Department. For exporters whose products are transferred from State to Commerce jurisdiction, the change will mean much more flexibility in getting those products from the U.S. to their customers abroad. However, the change also shifts a greater compliance burden onto the exporter.

New Media, New Challenges

Executives responsible for ethics and compliance must also address growing complexity brought about by a range of new technologies—especially mobile devices and cloud computing—that help generate enormous quantities of data, according to ECA expert Mike Salvarezza *(Records and Information Management)*.

Executives responsible for ethics and compliance must also address growing complexity brought about a range of new technologies—especially mobile devices and cloud computing—that help generate enormous quantities of data.

The dramatic surge of information stored on smart phones, tablets and other PDAs has caused some organizations to abandon efforts to "control" which devices are used by employees in favor of a BYOD (Bring Your Own Device) approach, according to Salvarezza. But with that flexibility come numerous risks to the records manager, including an inability to access company records that are housed on mobile devices; rapid sharing and proliferation of records from device to device and from one to many people; and co-mingling of business and personal records.

"Simply put, the ability to 'manage records' may become impossible using traditional methods," writes Salvarezza. "To truly be successful in the long term, records management professionals must begin to challenge the very requirements that they are attempting to comply with. These requirements must be carefully re-examined and be subject to overhaul to remove outdated and impossible to achieve compliance requirements."

And how many readers of this report are not already users of Facebook, LinkedIn, or Twitter? Michael Connor *(Social Media)* reports that more than 1.5 billion people around the globe now have an account at a social network site. According to Connor, "social media are transforming the very nature of the Internet, from a medium dominated by static web sites to one featuring multiple levels of interaction on platforms like Facebook, Twitter, LinkedIn, and YouTube."

Keeping pace with these technologies from a compliance perspective requires attention at all levels of the enterprise. Connor cites a recent survey of senior executives and corporate directors which found that while 90 percent of respondents claim to understand the impact that social media can have on their organization, only 32 percent of their companies monitor social media to detect risks to their business activities.

While social media empower users to become their own publishers, developing effective organizational policies for social media can prove challenging. In the U.S., Connor notes, the National Labor Relations Board has focused considerable energy on social media issues, with a series of rulings that have confounded some compliance professionals.

Robert Bond (*Privacy and Data Security*) considers what global companies should be doing to mitigate privacy risk, with a particular focus on the Asia-Pacific region and the continued challenges of implementing ethical hotlines in the European Union. Also on the horizon: the EU's pending draft Data Protection Regulation, which Bond says will impose "significant compliance obligations" on businesses that use equipment in the EU for processing personal data, or are not in the EU but who process EU data subjects or monitor their behavior. According to Bond, a negligent or reckless breach of the Regulation could lead to fines of up two percent of a company's worldwide revenue.

The poor economy has led to a new category of laws that make employers particularly vulnerable.

The Workplace

"Who's the boss?" Marcia Narine *(Labor and Employment)* reports that in coming months the U.S. Supreme Court will address that question, perhaps providing a "watershed" ruling for employers. In the case of *Vance v. Ball State University*, an African-American kitchen worker alleges that her co-employees actually served in the capacity of her supervisors because they directed her day-to-day activities, and that their actions, including racial epithets and physical threats, created a hostile work environment. Narine cautions that if the Supreme Court relaxes the definition of a supervisor to include co-workers it "could fundamentally change the workplace" and make it easier for employees to bring legal action against an employer.

More broadly, Narine says, the poor economy has led to a new category of laws that make employers particularly vulnerable. For example, a number of states are considering or have passed laws on unemployment discrimination, making it unlawful to refuse to hire someone because they have been out of work for too long. And because of the economy and foreclosure crisis, some states now forbid employers from inquiring about credit during a background check.

Culture and Program Management

While a traditional approach to E&C education and communication may make an organization "compliant," its employees are often not prepared to deal with difficult situations, suggests Charles Ruthford *(Education and Communication Strategies)*. He says new research challenges the assumption "that, armed with knowledge, a decision-making process, and an awareness of consequences," most people would make rational and proper choices when confronted with ethical challenges.

Ruthford argues on behalf of educational programs that are interactive, collaborative, and focused on problem-solving with real-life examples. "This new approach to learning and communication will require commitment by senior leaders, involvement of mid-level managers, and individual measurement systems that are aligned with organizational ones," Ruthford writes. It will also be more expensive, but costs will be outweighed "by the benefits of engaged employees who will respond in an ethical and compliant manner in difficult situations."

For LRN's Michelle Moyer *(E&C Program Management)*, the pressing question is how a company can optimally position itself to operate responsibly in a hyper-connected, hyper-transparent environment over the long term, and not

only survive, but thrive. She points to proprietary LRN research which shows that self-governing organizations in some 18 countries experienced higher levels of innovation, employee loyalty, and customer satisfaction; lower levels of misconduct; and superior overall financial performance.

Proprietary LRN research shows that self-governing organizations in some 18 countries experienced higher levels of innovation, employee loyalty, and customer satisfaction; lower levels of misconduct; and superior overall financial performance.

The answer, according to Moyer, "lies in creating an internal culture that is self-governing; that is, a culture where employees are guided by clearly defined and well-understood principles and values, and are inspired by those values to be leaders and to align around the company's mission, purpose, and business objective because they feel genuinely responsible and accountable for the company's long-term health, welfare, and legacy."

The Year Ahead

Economists these days generally hedge their forecasts pretty carefully. While the business outlook for 2013 seems to be improving, there are huge imponderables that also threaten recovery. Much the same can be said for a risk forecast like this one, especially as it applies to any individual organization. While it is possible to discuss the broad parameters of risk, particular situations often require more detailed examination and discussion.

If you and your organization would like to explore these topic areas in more detail or would like to connect with one of our Ethics & Compliance Alliance experts, please don't hesitate to contact us for more information. In the meantime, we invite you to read and consider the expert perspectives in this report and leverage them in support of your ethics, compliance and risk management programs and related initiatives. We are confident you will find them worthwhile and insightful.

Best Regards,

Greg Triguba

For the LRN Ethics & Compliance Alliance

Greg Triguba

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Michael Fine
ECA Expert Panelist

Michael Fine is a leading expert in the area of anti-corruption and bribery law and provides advisory support on the effective implementation and management of related compliance programs and infrastructures. Michael is Principal of NXG Global Law & Compliance where his practice focuses on anti-corruption programs, public policy advocacy, regulatory counseling, and the implementation of corporate compliance programs. Prior to establishing NXG Global, Michael served as the Director of Private Sector Initiatives for Transparency International and practiced law at the Firm of Powell, Goldstein, Frazer & Murphy.

Anti-Corruption and Bribery

Global Anti-Corruption 2013

The expectation for anti-corruption enforcement in the coming year is more of the same, with continued vigorous enforcement of the Foreign Corrupt Practices Act (FCPA) and still slow but steady advances internationally.

Past Risk Forecasts have highlighted the sharp rise in the number and magnitude of FCPA enforcement actions; our message this year is more nuanced. Raw enforcement numbers are down slightly for a second consecutive year, with the more consequential FCPA developments in the details. The year 2012 saw a continued ramping-up of agency enforcement capacity, more selectivity on prosecutions and flexibility on settlement terms, and publication of a detailed "FCPA Guide" spelling out agency interpretations and priorities. In a word, a maturation of FCPA enforcement—with these trends expected to continue through a second Obama Administration. The global anti-corruption picture remains mixed, with growing caseloads in a few jurisdictions but lagging efforts in many other countries that will continue to invite gap-filling FCPA enforcement.

FCPA Baseline

The FCPA has remained an essential baseline for most companies even as anti-corruption programs take on a more global tone and nomenclature.

We begin this year's forecast once again with the FCPA, which despite advances elsewhere continues to drive risk assessment and mitigation planning at most multinational companies. Although the U.K. Bribery Act is beginning to make its mark, speculation that it would displace the FCPA model and require wholesale changes to FCPA-oriented programs has not proven out. The U.S. continues to lead the world in anti-bribery enforcement by a wide margin, with 233 concluded cases and more than 100 open investigations, as well as corporate penalties that dwarf those elsewhere.[1] As such, the FCPA has remained an essential baseline for most companies even as anti-corruption programs take on a more global tone and nomenclature.

Enforcement highlights

On the surface, 2012 was a year like most others for FCPA enforcement, with a number of high-profile settlements, notable additions to the corporate investigations docket, and an ongoing focus on criminal prosecutions of individuals. Raw numbers were off for a second year for new cases and settlement amounts, but were still robust by historical standards and consistent with trends described in prior reports. The Department of Justice (DOJ) and

1 *Progress Report on Enforcement of the OECD Anti-Bribery Convention, 2012*, Transparency International at 37 (Aug. 2012).

Securities and Exchange Commission (SEC) continued to add enforcement resources (including more FCPA-dedicated prosecutors) and new cases to the investigations pipeline (most notably for Wal-Mart in Mexico), to advance sectoral enforcement initiatives (particularly in health care), and to target violations by non-U.S. companies. Health care actions accounted for roughly 60% of all dispositions through the first three quarters of 2012, and investigations involving non-U.S. companies continued to feature prominently. Substantial resources were again devoted to individual criminal prosecutions, with a number of successes but also failures. The latter included the dismissal, after a two-year prosecution, of charges against 21 of 22 defendants in the Las Vegas "Shot Show" case.

Highlights from the year included a $54 million settlement with the Japanese Trading Company Marubeni Corporation (probably the last in the long-running TSKJ Bonny Island joint venture investigation), a $60 million settlement with Pfizer (resolving multiple investigations, including one inherited through an acquisition), a $29 million settlement with Eli Lilly (resolving SEC civil action, with an apparent pass on DOJ criminal enforcement), and a $26 million settlement with Swiss-based Tyco International. A number of other major cases were thought to be near settlement at year's end, with most speculation focused on French oil giant Total SA (with a $398 million reported reserve) and Avon's long-running global investigation. Record fines are also possible in the widening Wal-Mart Mexico investigation, although not for another year or so.

All in all, an enforcement record not terribly different in its essentials from 2011—or from what we can expect in the coming year.

All in all, an enforcement record not terribly different in its essentials from 2011—or from what we can expect in the coming year. A five-year surge begun in the latter years of the Bush Administration appears to have leveled off, with a normalization of the case load and settlement activity at still high but more stable levels. These raw figures are only one measure of enforcement activity, of course, and could change in response to any number of factors (for example, an upsurge in Dodd-Frank whistleblowing). On the whole, though, they reflect a pattern seen in other enforcement areas following an initial ramp-up period—as well as the heightened C-Suite attention generated by the initial case surge and associated advances in prevention efforts at multinational companies.

But in other respects 2012 was a very different and more consequential year for FCPA enforcement. We saw the first serious effort in decades to roll back key elements of the FCPA, notable refinements to DOJ and SEC enforcement and settlement practices, publication of a comprehensive FCPA resource guide, and finally a presidential election that secured the current FCPA path for at least another four years.

Legislative challenge

The year began with growing momentum for a package of legislative reforms that would have significantly altered key aspects of the FCPA. As we reported in last year's Forecast, this initiative had its origin in a 2010 study commissioned by the U.S. Chamber of Commerce that called for, among other things, an affirmative compliance defense to FCPA liability (similar to the U.K. Bribery Act), a new "willfulness" requirement, and narrowing of coverage for foreign state-

owned enterprises. Other provisions would have limited successor liability for pre-acquisition violations (based on a knowledge standard) and parent liability for subsidiary actions.[2]

Reaction to the proposed amendments was along predictable lines, with strong opposition from the Obama Administration and little prospect of meaningful action in the last Congress. Still, proponents had been optimistic that a new Republican administration might be more sympathetic and had begun laying legislative groundwork for that prospect. The Chamber launched what one close observer described as an "intense" lobbying campaign that produced, among other early fruits, a supportive congressional hearing on the reforms and letters to the DOJ from several prominent Democrats. By the late spring, the initiative appeared poised for more gains, only to be sidetracked by the Wal-Mart scandal,[3] and then in November the President's reelection.

While the immediate chance for legislative action has passed, probably for another four years, the broader campaign to narrow FCPA enforcement that sparked it has not. Public advocacy efforts will continue into the new year, together with a companion initiative to reshape enforcement through the courts. Illustrative of the latter has been a closely-watched challenge to the government's application of FCPA "foreign official" status to state-owned companies. (Several district courts have ruled for the government, but the matter is on appeal.) Past efforts to circumscribe FCPA enforcement through the courts have not been successful and prospects for this and similar challenges are probably low, but for the first time the DOJ and SEC are being required to defend their interpretations, a step many consider salutary and overdue. Setting particulars to the side, a larger message from these developments is the fraying of a bipartisan consensus and business support so crucial historically to the FCPA's advance—and by extension global efforts in this area.

Past efforts to circumscribe FCPA enforcement through the courts have not been successful and prospects for this and similar challenges are probably low, but for the first time the DOJ and SEC are being required to defend their interpretations, a step many consider salutary and overdue.

Refinements to enforcement practice

Coincident with the Chamber campaign—which has been the most far-reaching, public and politically successful in the FCPA's 35-year history—the past year has seen notable refinements to FCPA enforcement practice. The DOJ and SEC have been more public about "declinations" (decisions not to prosecute after initiating an FCPA investigation) and the reasons; they have awarded more (or at least clearer) credit to companies for cooperation and quality compliance efforts; and there has been an easing of some settlement conditions (in particular, mandated independent monitors). The DOJ and SEC also have been clearer about not prosecuting de minimis violations, have taken steps to encourage internal reporting by Dodd-Frank whistleblowers, and have been more expansive in advisory guidance.

2 The 2010 study drew on similar restrictive provisions found in the contemporaneous U.K. Bribery Act. For a detailed comparative analysis of the U.K. Bribery Act and FCPA, see *Coordinating U.K. Bribery Act & FCPA Compliance* on the ECA: https://eca.lrn.com/focus-area-resources/coordinating-U.K.-bribery-and-fcpacompliance. See also *"UK Bribery Act: Mixed OECD Review Portends Change"* on the ECA, summarizing concerns about certain of these provisions identified in a March 2012 OECD anti-bribery working group review of U.K. convention efforts.

3 For a discussion of the Wal-Mart Mexico case, see M. Fine, *"A Teachable Moment: FCPA Lessons from the Wal-Mart Experience,"* SCCE Compliance & Ethics Professional at 49 (Sept/Oct 2012).

Speaking at a recent national conference on the FCPA, Assistant Attorney General Lanny Breuer reaffirmed the U.S. commitment to "combating corruption around the world," describing FCPA enforcement as one of the DOJ's "signature achievements" and part of a record that has put the U.S. "on the right side of history."[4] At the same time, there was a recognition that the DOJ and SEC needed "to strike an appropriate balance between vigorous and responsible enforcement." As an illustration, Breuer cited the DOJ's decision last April not to charge Morgan Stanley directly for an employee's bribery because the violation had been self-disclosed, and because the firm had cooperated with the investigation and could point to a rigorous compliance program. In another case, involving potential successor liability, a similar judgment not to prosecute was made based on the pre-acquisition due diligence conducted. In both instances, declinations were publicized to encourage similar proactive efforts by others.

Opinions vary on the significance of these cases—whether reflective of systemic change or only a few "good apples," so to speak—but at the least they suggest a more nuanced approach to enforcement in the future. For example, while there may be little appetite for a formal "compliance program defense," the practical effect from a more robust and public crediting of corporate investments in quality programs may not be very different, especially given the uncertainty and practical challenges associated with a formal Bribery Act-like defense.[5] In some cases, this may manifest through declinations that completely shield a company from enforcement action (as for Morgan Stanley); in others, through a substantial penalty deduction (pegged at 30% in one recent settlement) or avoidance of mandated independent monitors (multiple cases in 2012). Likewise, although we are unlikely to see significant changes to the expansive application of FCPA authority that has developed, the more nuanced enforcement posture may shield companies with exemplary prevention efforts as in the "successor liability" declination mentioned earlier.

The year's other notable development was the publication in November of a comprehensive "Resource Guide" to the FCPA, developed jointly by the DOJ and SEC.

New FCPA guidance

The year's other notable development was the publication in November of a comprehensive "Resource Guide" to the FCPA, developed jointly by the DOJ and SEC. Over a year in the drafting, the 120-page document contains a useful historical overview of the FCPA and Organization for Economic Cooperation and Development (OECD) expansion together with these agencies' reading of the law and enforcement priorities. Much of this information had already been available, but not in one place or with the same clarity and detail. Topics addressed range from the definition of a "bribe" and "foreign official" to gifts and entertainment, FCPA jurisdiction and the hallmarks of an effective anti-corruption program. There are also helpful commentaries and illustrations to make the guidance more concrete.

4 L. Breuer, Speech at 28th National Conference on the FCPA, 16 Nov. 2012 (http://www.justice.gov/criminal/pr/speeches/2012/crm-speech-1211161.html).

5 U.S. authorities have been reluctant to adopt a formal compliance program defense like the one for "adequate procedures" in the U.K. Bribery Act in part because of the practical difficulty of judging adequacy in a particular context. Most FCPA prosecutions have involved large or systemic patterns of bribery, often with high-level involvement or knowledge, and how these might be squared with an "effective" program standard is not immediately obvious. In a U.K. context, the challenge is further compounded by a relative lack of historical experience with compliance practices both in government and the private sector (compared to several decades of trial-and-error advances in the U.S. under the Federal Sentencing Guidelines framework) and uncertainty about how and when judgments about the defense will be made.

Although the FCPA remains central to risk assessment and mitigation planning for most international companies, counterpart laws in other jurisdictions merit heightened attention. Chief among these is the U.K. Bribery Act, but other countries (notably Germany) also stand out.

The Guide was developed with several objectives in mind. The initial catalyst was a recommendation from the OECD working group on bribery that the U.S. spell out more clearly its enforcement policies and priorities, with an eye toward a similar push in the future with other OECD countries. As importantly, the year-long process and resulting document have provided a rebuttal of sorts to the U.S. Chamber reform initiative, elaborating in greater detail the DOJ and SEC position on contested issues, and at the same time countering the criticism that enforcement standards have been too opaque or uncertain. Finally, and most significant from a compliance vantage, the Guide has provided the DOJ and SEC with an opportunity to spell out in greater detail for the business community factors that they consider in deciding whether and how to pursue an enforcement action, evaluating a compliance program, deciding whether to impose a monitor, and choosing among alternative forms of resolution.

In the month following release of the Guide, numerous reviews have been published and there is much in these and the document itself worthy of careful review. Some highlights:

- The Guide provides a detailed listing of elements the DOJ and SEC will consider when evaluating a company's anti-bribery program, acknowledging that "no compliance program can ever prevent all criminal activity by a corporation's employees," and that meaningful credit will be given for a comprehensive risk-based program implemented in good faith.
- Commentaries and illustrative examples clarify the standards for determining whether a bribe meets the "business purpose" test, and when a particular state-owned entity will be considered governmental.
- There is also helpful (if not new) advice on gifts and entertainment, reaffirming the requirement of corrupt intent for an FCPA violation, and that payments of nominal value (such as a cup of coffee or taxi fare) are not an enforcement priority.
- There is also some comfort on successor liability (short of a safe harbor) for acquiring companies that have checked diligently for problems in advance, and taken preventive measures after acquisition, plus a reaffirmation that pre-acquisition bribery must have been in violation of the FCPA at the time it occurred.
- The Guide emphasizes the broad nature of FCPA jurisdiction over non-U.S. companies, reaffirming expansive theories that have been used to reach companies with only nominal territorial contacts (as under "correspondent bank jurisdiction") or none at all (on a "conspiracy" basis).

Additional Global Considerations

Although the FCPA remains central to risk assessment and mitigation planning for most international companies, counterpart laws in other jurisdictions merit heightened attention. Chief among these is the U.K. Bribery Act, but other countries (notably Germany) also stand out.

Global enforcement efforts continue to lag behind the U.S., with only modest gains over the past year. By one measure, there are still only seven OECD countries with "active enforcement," and another dozen rated as "moderate."[6]

6 *Progress Report on Enforcement of the OECD Anti-Bribery Convention, 2012*, Transparency International at 4 (Aug. 2012).

Modest as this figure is, it still overstates the actual progress, with countries needing only one active major case and investigation to qualify for "moderate" enforcement status. On the other hand, formal cases take time to develop and a somewhat more robust picture emerges if one looks instead at investigative activity. A number of lower-ranked countries report relatively high levels of current investigative activity, while others considered "active" rate less well. Using an investigations measure, those currently most active include, in addition to the U.S. (at 113 active investigations), Germany (43), the U.K. (29), Italy (15), Canada (34), Austria (10), and Australia (8). According to the OECD working group on bribery, at year end 2011 there were approximately 300 ongoing investigations in the 26 signatory states to the anti-bribery convention.[7]

For risk managers, the essential message remains the importance of a comprehensive global approach to anti-bribery risk forecasting and compliance.

The U.K. Bribery Act has remained center stage for many global companies, but with a mixed record to this point. A year and a half on, there have been relatively few prosecutions, and these mostly of individuals rather than companies and under pre-Bribery Act statutes. Still, there has been a notable rise in the overall level of activity, with 14 individual convictions through the first three quarters of 2012 and another 11 active foreign bribery cases, and 18 others said to be under consideration. In addition to the first individual conviction under the Bribery Act—of a domestic court clerk for traffic court bribery—the past year saw civil resolutions in several corporate cases (Oxford Publishing, Abbot Corp.) and the launch of a high-profile defense sector investigation (EADS). Set against this has been a record turnover in the lead enforcement agency, the Serious Fraud Office (SFO), together with ongoing concerns about its authority and resource levels. A March, 2012 OECD working group assessment also gave the U.K. a decidedly mixed review on its anti-bribery enforcement efforts. Although it credited SFO outreach to the business community, citing its detailed guidance on the "adequate procedures" defense and the design of effective compliance programs, the report identified a number of gaps in the legal framework that may require further legislation. Chief among these are lingering concerns about the government's ability to hold companies accountable for bribery by an employee or affiliate.[8] The law courts have also cast a cloud over SFO authority to settle matters through Deferred Prosecution Agreement (DPA) and other alternative means, although a measure has been introduced in the Parliament to remedy this.

Still, the pace of action internationally clearly is picking up and, in the wake of this year's FCPA reform debate, there will be even more pressure for OECD partners to step up their own enforcement, and on non-U.S. companies through gap-filling FCPA actions. For risk managers, the essential message remains the importance of a comprehensive global approach to anti-bribery risk forecasting and compliance. Although enforcement in most countries is still spotty—and well below U.S. levels even in the most active countries—there are now important exceptions. And even for the laggards, multinational companies (especially from the U.S.) will remain an appealing early target. The challenge ahead will be to build and maintain effective global compliance programs that can capture relevant laws, reconcile differences (for example, on facilitation payments), and, above all, communicate company standards and expectations to an increasingly diverse workforce.

7 *OECD Working Group on Bribery, 2011 Annual Report at 10*. These annual reports are summary, and have been criticized for overstating progress, but the more detailed assessments conducted for individual countries can be a valuable resource for risk assessment. The OECD "Phase 3" review conducted for the U.K. last April is illustrative, highlights from which are described in an alert on the ECA website (*"UK Bribery Act: Mixed Review Portends Change"*).

8 See *"UK Bribery Act: Mixed Review Portends Change,"* available on the ECA.

CLICK HERE TO RETURN TO TABLE OF CONTENTS

Ted Banks
ECA Expert Panelist

Ted Banks is a recognized and leading expert in areas of global antitrust and competition law. Ted is a seasoned attorney and partner in the Law Firm of Scharf Banks Marmor LLC in Chicago, IL, and is President of Compliance & Competition Consultants, LLC.

In his practice, Ted concentrates on general corporate and antitrust matters and serves his company clients in development of effective ethics and compliance programs, antitrust and competition compliance initiatives, and records management programs. Formerly, Ted served as Chief Counsel & Senior Director, Global Compliance Policy at Kraft Foods.

Antitrust and Competition Law

Where is it going in 2013?

Antitrust/competition law compliance programs are commonplace. Nearly every code of conduct has a general antitrust compliance statement. But while the basics of antitrust are unchanged (collusion and abuse of dominance), the specifics of antitrust violations have evolved, as have the techniques available to ensure an effective compliance program. Spending a few minutes thinking about where the law might be going in 2013 can be useful in making sure that your compliance program really is addressing today's risks.

The Second Obama Administration and Antitrust

2013 is beginning with a newly confirmed FTC Commissioner[1] and a newly confirmed head of the Antitrust Division.[2] One can reasonably expect that the policies established in the first administration will be continued. The government will be more aggressive in its enforcement efforts than was the Bush Administration in areas like mergers. Cartel enforcement, which was aggressive in the past, will continue. The Antitrust Division will utilize its amnesty program as a key enforcement tool, so it will behoove any attorney or compliance officer who detects the possibility of collusion to consider going to the government as quickly as possible.

The Antitrust Division will utilize its amnesty program as a key enforcement tool, so it will behoove any attorney or compliance officer who detects the possibility of collusion to consider going to the government as quickly as possible.

As is discussed below, the position of the Antitrust Division on compliance programs has been one of disdain. Several years ago, it apparently secured an exception from the Federal Sentencing Guidelines (FSG), so that the presence of an "effective" compliance program will not entitle a company to any sort of reduction of sentence. However, it did require the appointment of a compliance monitor in the *AU Optronics* case (discussed below), so there may be a recognition that compliance programs have a value after all.

Antitrust and Banks

While there is still talk of antitrust concern about "too big to fail," it seems that public enforcement against financial institutions will focus on conduct, not size. Private litigation may be the major risk, as shown by the LIBOR cases.[3]

1 Professor Joshua Wright, who does not have an expansive view of the scope of § 5 of the FTC Act, was nominated for the "Republican" seat previously held by Thomas Rosch. FTC Chairman Jon Leibowitz may also resign soon in 2013, and it would be expected that someone with similar pro-enforcement leanings would be nominated to replace that seat on the Commission.

2 William Baer, former head of the Bureau of Competition at the FTC, was confirmed on December 31,2012, while most of the country's attention was focused on fiscal cliff negotiations.

3 UBS may be fined more than $1 billion by U.S. and U.K. regulators. Barclays Bank agreed to pay $467 million to settle Libor manipulation allegations.

If a case can be made that collusion by financial institutions is the cause of consumer pain, then one should expect aggressive pursuit by private parties. Combined with increasing willingness by many courts (particularly state courts) to allow consumers to recover in antitrust cases, the imperative for banks to strongly police their antitrust compliance programs is ever more important.

On the public enforcement side, one might expect a mixed bag. The regulators in the United States continue to shut down insolvent financial institutions, and the government needs to find homes for the assets of those banks quickly. In addition, the Federal Reserve has signaled that it wants to continue an "easy money" policy to provide economic stimulus, so anything that might disrupt the flow of cash into the economy would face internal Administration opposition, regardless of what the antitrust enforcers would want to do.

If, however, a credible case can be made that the policies of the largest banks have been working in opposition to the Administration's stimulus policy, that might provide the impetus to attach a large financial institution based on size. The case, however would not be an easy one to bring, and would involve a new approach where financial institutions, by virtue of their size, could behave in a way that was injurious to the economy, if not to competition. If there was a thought to challenge a bank based on its size, it might well be easier to do so in a financial regulatory context, rather than rely on antitrust.

The War against Conspiracies Continues

Public enforcement against cartels continues, with lengthy prison terms and large fines sought. The Department of Justice (DOJ) will proceed against conspiracies that occur outside the United States, when they have a domestic impact. *The AU Optronics*[4] case showed several interesting developments, however. The government sought a huge fine ($1 billion) and lengthy prison terms (ten years), but the judge imposed "only" $500 million, and three-year sentences of $200,000 fines on the convicted executives. She ruled that the fines sought by the DOJ would cripple the company, and hurt the public by reducing competition. The judge was sensitive to arguments that the individuals had "relatively little personal motivation" and "thought they were doing the right thing vis-à-vis their company." Part of the sentence of the case did require the appointment of a compliance monitor, which may indicate increased attention by the Antitrust Division to the value of compliance programs. Other defendants in the investigation of price-fixing of LCD displays chose to settle with the government and not go to trial, and they received fines ranging from $30 million to $400 million, under the Guidelines range, based on cooperation with the government. The moral of the story: going to trial is always a risky proposition.

The Department of Justice (DOJ) will proceed against conspiracies that occur outside the United States, when they have a domestic impact.

The question of whether there was personal motivation was also raised in the prosecution involving bid-rigging of municipal bonds. The sentencing memorandum from the DOJ urged ten-year sentences based on losses that ranged from $5 million to $10 million for each defendant. The memorandum rejected the idea that employees were just trying to help their companies, and that there was no personal motivation. The memorandum noted that there was a great motivation on the part of the employees to keep high-paying jobs.

4 United States v. AU Optronics Corp., No. 09-cr-0110 (N.D. Cal. June 11, 2012).

Economics and Behavior

Antitrust jurisprudence, particularly in the United States, evolved over the last 40 years by reflecting concepts of economics. A debate raged over whether the Chicago-school of economics (reflecting, at least in theory, an analysis of pure market forces) or the Harvard-school (reflecting a more values-based analysis) should guide antitrust enforcement. Meanwhile, some economists started looking at the other factors that influence how people behave. It may not be because they are always trying to maximize their profits, or trying to increase social welfare through behavior that might otherwise be thought of as inefficient. In fact, the realization dawned that disciplines such as psychology could be viewed in conjunction with economics to offer new insights as to how people behave and why, including why they might violate the law.

It behooves all compliance officers to make certain that they understand the forces that drive their company. In the antitrust area, financial incentives for sales may encourage employees to "bend" the rules in order to collect a bonus.

Effective compliance programs do not just establish rules and give orders. They must approach compliance from the employee's point of view. This means communicating in an employee's vernacular, not in lawyer-speak. It means explaining how compliance with antitrust laws will benefit the employee and the company. And it also means explaining how violating the antitrust laws will be detected, and an employee's job may be lost, and his or her life irreparably damaged. Employees should learn how to do their jobs properly because it is in their interest. And they should learn what not to do, and the consequences of violating these laws.

So, it behooves all compliance officers to make certain that they understand the forces that drive their company. In the antitrust area, financial incentives for sales may encourage employees to "bend" the rules in order to collect a bonus. Employees should be educated about what they cannot do (such as colluding with competitors), and motivated to use their creativity to figure out how to get the job done within the parameters of the law. Companies should recognize outstanding performance not just with money, but with an acknowledgement that each person is important no matter what his or her job, and that all play a part in the success (or failure) of the company.

Employment

Antitrust compliance programs often fail to cover the antitrust risks that might be presented by the activities of human resources departments. While there may be antitrust exemptions for collective bargaining, it is a mistake to assume that anything done with regard to hiring employees is free from antitrust concerns. Actions have been brought by the federal government and the states to challenge "non-poaching" agreements among companies that might be drawing on the same pool of employees, even if they were not direct competitors.[5] The increased aggressiveness of the Department of Labor, combined with the reduced reluctance to attack employment activities under the antitrust laws, signals that the risks of government enforcement here are increasing. Private parties have also brought actions challenging agreements among competitors that allegedly limited their job opportunities or salaries.

5 Cases were brought in 2010 against Google, Apple, Intel, Intuit, Pixar, and Lucasfilm. More recently, United States v. eBay, Inc., No. 12-cv-5859 (N.D. Cal. Nov. 16, 2012), challenged a "handshake" agreement between eBay and Intuit not to solicit each other's employees.

Compliance officers need to work closely with labor and antitrust lawyers, and with human resources departments, to make sure that none of their practices violate antitrust laws. Common activities, such as salary surveys among companies in the same city or the same industry, should not be undertaken without guidance.

Global Enforcement

The Federal Trade Commission (FTC) and Antitrust Division will continue to cooperate with foreign enforcement agencies and international organizations. Regulation of competition is now a common part of the legal infrastructure of most countries, and while enforcement policy and competence may vary widely outside of the United States, antitrust must be a part of compliance programs wherever a company does business. As in the *AU Optronics* case, U.S. government enforcement against cartels will take place if there is an impact in the U.S., and private follow-on litigation should be expected. The concept of private antitrust actions is gaining support outside of the United States. Compliance officers of multinational companies must continue to firmly resist the entreaties of overseas managers to allow them to participate in local cartels based on local custom.

Although the new merger guidelines purport to give less weight to the need to define a market, in practice, market definition will continue to be the key determinant of how the government analyzes the competitive impact of a transaction.

Mergers

The Administration is likely to continue its course of challenging mergers that appear to be anticompetitive from a consumer point of view, and will probably continue to give less weight to arguments of efficiency than might have been persuasive in the Bush era. Although the new merger guidelines purport to give less weight to the need to define a market, in practice, market definition will continue to be the key determinant of how the government analyzes the competitive impact of a transaction.

Expect to see a willingness to challenge mergers that have already been consummated.[6] Political or consumer complaints may also result in the scrutiny of transactions that fall below the reporting threshold, particularly at the FTC. As implementation of the Affordable Care Act rolls out, expect to see continued antitrust enforcement in health care, particularly where prices rise after hospitals or other health care providers merge.

What does this mean for compliance officers? Insist on a seat at the table as acquisitions are being considered. When a horizontal competitor is the acquisition target, insist that there be a good explanation as to why the transaction should be allowed to be consummated, in language that you—not only an economist—can understand. Of course, make sure that the due diligence of the target includes a review of their compliance programs, and any shortcomings in that area should be flagged in time to put a hold on the transaction progress until all of the risks can be evaluated. The government has shown increased willingness to impose conduct-based remedies in merger transactions, which may require the involvement of the compliance officer to ensure that terms of any settlement are followed.[7]

6 Polypore International, Inc. v. FTC, 686 F.3d 1208 (11th Cir. 2012).

7 Conduct remedies include firewalls that may limit sharing of certain confidential information or the requirement to license technology to competitors on a fair, reasonable and non-discriminatory ("FRAND") basis.

Monopolies

The withdrawal of the prior administration's policy statement on Section Two signaled that the Obama administration's approach to monopoly enforcement would be more expansive. Not much has happened in this area recently from the Department of Justice, although the FTC has continued its enforcement against monopolies based on its authority under Section 5 of the FTC Act. In recent years, the FTC's cases that might have been characterized as monopolization cases focused on things like exclusive dealing agreements, and its more recent investigation of Google looked at director interlocks between Google and Apple that might violate Section 8 of the Clayton Act.

Prosecutions against monopolistic behavior, whether under Section 2 of the Sherman Act or Section 5 of the FTC Act, often come as a surprise to compliance officers because there is no black-and-white line that can be defined in a code of conduct or antitrust policy. Practices that may have gone on for years, and would never have been the subject of a compliance training program, suddenly become violations. So what does this mean for a compliance officer?

Compliance officers (and their antitrust law experts) should look with special scrutiny at products or services where there is a market share in excess of 50 percent. These are the areas that may be most likely to attract enforcement attention from government enforcers (in the United States and other countries) and from private plaintiffs. The risk assessment should specifically examine whether any changes in law or the political environment might signal a need to review business practices. Changes in the structure of the market, such as the failure of a competitor or complaints from customers or suppliers, might also be significant in evaluating the risk in this area.

Patents

The increasing antitrust litigation involving patents may be a sign of the evolution of our economy (and society) to a more technology-based world. But even without trying to make any profound interpretations of this trend, it is important to note the presence of antitrust intruding into the world of patent "monopolies."

The increasing antitrust litigation involving patents may be a sign of the evolution of our economy (and society) to a more technology-based world.

In cases where there seems to be abuse of patent rights where a patent is part of an industry standard ("standard essential patent"), the government is willing to seek an order compelling the licensing of the patent on fair, reasonable, and non-discriminatory ("FRAND") terms Although it does depart from the traditional rule that a patent owner can license a valid patent when, where and how it wishes, it should not come as a huge surprise. If an industry standard has been established, and certain patents are essential to complying with the standard, the standard setting organizations usually require that those patent owners agree to FRAND licensing in the first place. The FTC has required FRAND licensing of patents as a condition to allowing a merger to proceed.[8] It also has stated that a patent owner that agrees to FRAND terms and then seeks an injunction for alleged infringement against companies willing to take licenses is violating Section 5 of the FTC Act without a showing that the patent owner acted in bad faith. The European Union, in furtherance of its

8 In re Robert Bosch GmbH, FTC File No. 121-0081, Consent Agreement (Nov. 26, 2012).

mission of promoting European integration and the free movement of goods, has stated that it will attack attempts to foreclose access to markets through the use of intellectual property rights. Economists from the DOJ, FTC, and EU Directorate General for Competition have issued suggestions for standard setting organizations (SSOs) that should be noted. They have suggested that 1) FRAND commitments should be binding on subsequent purchasers of the patent; 2) the SSO should have procedures in place to resolve disputes about FRAND licensing; 3) licensees should have the option of licensing a patent on a cash basis instead of only on a cross-licensing basis; and 4) as noted above, limitations should be placed on a FRAND patent holder that seeks to use an injunction to exclude a licensee from the market.

What is left unclear, however, is exactly what constitutes FRAND terms. A patent owner whose technology has been incorporated into an industry standard, and who has committed to license the technology on FRAND terms, should be cautioned, at a minimum, not to be greedy.

Another area of continued patent concern is the use—and possibly the abuse—of patent rights in the pharmaceutical industry. The FTC continues to challenge the settlement of patent lawsuits by generic drug manufacturers which result in the payment to the generic manufacturer in exchange for delay in introduction of generic competing products. The results here have been inconsistent,[9] and making predictions about liability in this area difficult. The Supreme Court will review these decisions, and, in addition to monitoring court decisions, companies involved in this area need to carefully monitor the relevant political activities, since various legislative proposals are pending to clarify the legal status of these activities.

Another area of continued patent concern is the use—and possibly the abuse—of patent rights in the pharmaceutical industry.

A patent that was obtained by fraud on the Patent & Trademark Office does not get antitrust protection.[10] Until recently, challenges against the validity of patents based on fraud were brought by companies facing the threat of patent infringement actions. In *Ritz Camera & Image, LLC v. Sandisk Corp.*,[11] the Federal Circuit ruled that a purchaser of a product, who would not be facing a threat of an infringement action, could bring a claim under the *Walker Process* fraud approach. There was no requirement that a challenger had to have standing under the patent law to bring a declaratory judgment action for patent invalidity. From a compliance standpoint, the burden falls on patent attorneys to ensure that there is full disclosure of prior art and no misrepresentation to the PTO, but that is hardly anything new. There may be increased litigation from disgruntled purchasers unhappy with high prices of patented goods; so the risk control may be a consideration if, assuming the patent is valid, the pricing for patented goods might be considered excessive by purchasers. Further court cases may flesh-out the parameters of claims made on purchasers, but for now the risk of increased patent-antitrust litigation looms.

Pricing: Maintaining and Discriminating

The Supreme Court has whittled away the antitrust rules against resale price maintenance, and now both minimum resale price maintenance (attempts to limit discounting by resellers) and maximum resale price maintenance (attempts

10 Walker Process Equipment v. Food Machinery & Chemical Corp., 382 U.S. 172 (1965).

11 No. 2012-1183 (C.A.F.C. Nov. 20, 2012).

to limit price gouging by resellers) are judged under the rule of reason in federal court. Federal enforcement in this area is unlikely, unless the price maintenance allegations come as part of a monopolization or merger case. Private parties may raise these allegations, but it will be difficult to show damages or even get beyond early motion practice. Nevertheless, if a price maintenance policy is adopted, there should be a rationale for the price restraints prepared in advance of any litigation that demonstrates the reasonable, pro-competitive impact of the restraint.

State and federal price discrimination laws are still on the books, but the legal risk they pose has been significantly diminished by court decisions that make it increasingly difficult for plaintiffs to win their cases. But particularly where companies sell a branded product to competing wholesalers or retailers, management of pricing differences is important both for limitations of legal risk and for maintaining good relations with—and trust by—all customers. Antitrust litigation often results from a feeling of being mistreated, even if the facts prove otherwise.

Unlike other compliance programs that meet the effectiveness criteria of the Federal Sentencing Guidelines, you will not get any credit from the Department of Justice in sentencing recommendations based on your antitrust compliance program.

Can you count on your antitrust compliance programs?

Yes—and no. Unlike other compliance programs that meet the effectiveness criteria of the Federal Sentencing Guidelines, you will not get any credit from the Department of Justice in sentencing recommendations based on your program. But the goal of compliance programs is to do the right thing in the first place. We may see the passage of whistleblower legislation specifically related to antitrust in 2013, as suggested by the Criminal Antitrust Anti-Retaliation Act, introduced by Senators Leahy and Grassley in July 2012.[12] The credit for "trying hard" is an added bonus. So, notwithstanding the anomalous position of the Antitrust Division, effective antitrust programs are still a must.

Conclusion

While there may be political differences on other areas of regulatory enforcement, in the United States, antitrust enforcement, at least against price fixing, is vigorous, whether there is a Republican or Democrat in the White House. Differences in enforcement philosophy show up primarily in merger policy, and then perhaps in other peripheral areas such as Section 2 or joint venture enforcement. Given the potentially draconian penalties that can be imposed for a violation (e.g. huge fines, lengthy jail terms, large treble damage lawsuits), with little or no ability to use FSG criteria as an offset, continued antitrust compliance vigilance is essential.

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

12 The bill would create a process to seek instatement, back pay, and damages if an employee were discharged for being a whistleblower with regard to horizontal conspiracy violations. Unlike the False Claims Act, there is no financial reward for antitrust whistleblowers.

Michelle Moyer
LRN Knowledge Leader

Michelle Moyer is an LRN Knowledge Leader and seasoned attorney with deep experience in areas of ethics and compliance programs, education solutions, legal research and analysis and inspirational leadership. Among other key roles, Michelle provides oversight of the LRN Ethics & Compliance Alliance (ECA) and provides invaluable support and subject-matter expertise across a number of the LRN ethics and compliance education solutions.

Michelle has served as Legal Counsel for LRN and has been responsible for designing and developing legal and compliance frameworks for a number of the LRN on-line education courses and experiential learning programs that ensure legal concepts are presented in an effective and meaningful manner. Michelle also serves and provides support in a leadership role as a member of the LRN Living How Council.

E&C Program Management for 2013 and Beyond

The Value of a Self-Governing Culture to Business Success, Sustainability and Significance

As the world around us becomes more transparent and interconnected, leaders of organizations have begun to understand that *how* they do business is as important as the goods they manufacture and the services they provide. Technology now offers every customer, shareholder, employee, business partner, regulatory agency, and public interest group an intimate view into the methods companies use to conduct business; *how* those methods impact individuals, communities, and the world at large; and what those impacts mean for our future and the future of generations to come.

In this environment, if a company is doing the right thing – for example, if it is making concrete and impactful efforts to ensure that neither it nor any entity in its supply chain is paying bribes, employing child labor, or dumping harmful chemicals into nearby rivers and streams – it is far more likely to be more successful and sustainable than a company that is not so actively and effectively taking steps to operate in legally, socially and environmentally responsible ways.

The question then becomes: how can a company optimally position itself to operate responsibly in this hyper-connected, hyper-transparent environment over the long-term, and not only survive, but thrive? The answer for E&C professionals lies in creating programs which foster an organizational culture that is self-governing; that is, a culture in which employees are guided by clearly defined and well-understood principles and values, and are inspired by those principles and values to be leaders and to align around the company's mission, purpose and business objectives because they feel genuinely responsible and accountable for the company's long-term health, welfare and legacy.

How can a company optimally position itself to operate responsibly in this hyper-connected, hyper-transparent environment over the long-term, and not only survive, but thrive?

Developing, implementing and leading programs that exemplify a self-governing mindset will catalyze others within the organization to think, feel and behave similarly. Why? Because inspiration is contagious. With a higher-purpose mission, long-range goals, and core values and principles in place to guide behavior and decision-making, the next step that you, as an E&C professional, will need to take is to work with other leaders in the organization to intentionally, rigorously and relentlessly drive the self-governing mindset and associated behaviors into all ethics and compliance efforts, and into the business in general.

This process involves (among many other things) developing codes of conduct, policies, procedures, education opportunities and communication strategies that emphasize and incorporate not only legal requirements and other rules that bind the company and its employees, but the values, ethics and broader individual, community and societal considerations that underlie those rules and the company's dedicated and unyielding observance of them.

As an example, when developing a policy to communicate the company's stance on bribery and corruption, explain not only that bribery violates laws worldwide, but also that it is arguably the single greatest obstacle to economic and social development in the world because it distorts markets, stifles economic growth, debases democracy, and therefore undermines the very purpose of those laws.

Similarly, when developing a policy to address harassment, relate not only that harassing behavior can result in legal action against the company, but also that it is morally wrong and creates work environments characterized by lack of professional courtesy and respect, which, if allowed to fester, can lead to wider-spread, equally serious illegal and unethical actions that have the ability to threaten the company's very viability.

By emphasizing and communicating the company's commitment to behaving with integrity, employees come to know not only "the rules," but the soul and spirit that underlie those rules and the broader consequences of their actions.

By emphasizing and communicating the company's commitment to behaving with integrity, employees come to know not only "the rules," but the soul and spirit that underlie those rules and the broader consequences of their actions. Put another way, they begin to more conscientiously consider not only what they're doing, but *how* they're doing it. The importance of conducting business by inspiring employees to lead and behave in a self-governing way, and driving self-governance into the company's ethics and compliance efforts and the business in general to reduce risk and increase opportunity, cannot be overstated. The alternative - instituting and commanding support for short-sighted goals and rigid rules through the use of carrots and sticks - is neither stimulating nor engaging nor empowering and is therefore doomed to fail.

So, what does a self-governing culture look like? At its core, self-governing organizations exhibit the following characteristics:

- They aim to positively impact the world rather than pursue only short-term, narrowly-defined, self-interested goals and objectives;
- They engage in decision-making and goal-setting, utilizing long-term vision;
- They encourage and facilitate effective coordination and collaboration among different segments of the organization;
- They ensure that information is shared throughout the organization authentically and transparently;
- They extend trust; rather than waiting for trust to be "earned";
- They embrace and celebrate employees who voice their concerns and who report behavior they believe to be illegal, unethical, or otherwise contrary to the company's values and principles;
- They use values and principles, rather than rules, to govern and guide behaviors and decision-making;
- They engage and impassion employees by inspiring them rather than motivating or coercing them;
- They enable productive, timely and aligned decision-making through a deliberate system of governance, culture and leadership;

- They respond effectively and resiliently to unexpected and even sudden and dramatic shifts in competitive dynamics, economic conditions and societal forces.

These characteristics of a self-governing culture have the power to engage and ignite employees to such a tremendous extent that the company's ability to succeed and sustain itself, and to achieve its definition of significance, dramatically increases. The bottom line is this: intentionally, systematically and purposefully nurturing the culture of an organization unlocks its potential to experience and enjoy significant competitive advantage in the marketplace. And, the news gets better: these priceless business benefits can and have been tangibly demonstrated.

Self-governing organizations experience higher levels of innovation, employee loyalty and customer satisfaction; lower levels of misconduct; and superior overall financial performance.

In 2010 and 2011, LRN conducted groundbreaking research by way of its Governance, Culture and Leadership Assessment. The Assessment is a diagnostic tool that consists of over sixty questions designed to help a company discover and quantify whether and to what extent the characteristics of a self-governing culture are present among employees, and the impact that the presence or absence of those characteristics has on business performance.

The research LRN conducted using this tool is known as the Global Governance, Culture and Leadership Assessment, and involved surveying over 36,000 employees from eighteen countries around the world, including Australia, Brazil, China, France, Germany, India, Israel, Japan, Mexico, Russia, Saudi Arabia, Scandinavia, South Africa, Turkey, the United Kingdom and the United States.

The findings of this research, which have been captured and summarized in *The How Report* (see LRN's *The How Report* at LRN.com), reveal a great deal about the impact that self-governing cultures have on business performance.

Among other things, *The How Report* evidences the following:

- Self-governance in organizations across the globe is rare. A mere 3% of the 36,280 employees surveyed in the Global Governance, Culture and Leadership Assessment observed high degrees of self-governing behavior among their colleagues. Of note, this remarkably low level of self-governance was consistent across every demographic category, including country, industry, economic environment, language and ethnic culture.
- Self-governing organizations in all eighteen countries involved in the Global Governance, Culture and Leadership Assessment experience higher levels of innovation, employee loyalty and customer satisfaction; lower levels of misconduct; and superior overall financial performance.
- There is a serious disconnect between the C-suite and the employees they lead. The C-suite, on average, is three times – and in some countries even eight times – more likely to view their organizations as self-governing, more inspiring and less coercive than the employee population at large.
- Trust, shared values and a deep understanding of and commitment to a purpose-driven mission are the three most important drivers of self-governing behaviors that produce competitive advantage and enhanced business performance.

Armed with these and other findings from *The How Report*, company leaders everywhere have a unique opportunity to unlock the full potential of their employees' hearts and minds, and to thereby position the companies they

are entrusted to run to enjoy a level of success and significance far beyond that which their less evolved, less self-governing competitors can achieve. And ultimately, over time and through leading by example and manifesting the fruits of self-governance, these organizations will pave the way for others to embark on a similar journey.

The wave of self-governance is unstoppable, and ultimately what is best for our future. Our world is threatened by problems that seem more serious, complex and insurmountable than ever before. Hunger, poverty, war, environmental devastation and lack of access to education and basic healthcare continue to threaten the survival of our species and leave us worrying about the state of the world our children will inherit. These problems, and a whole host of others, require levels of creativity, innovation and cooperation among companies and their employees previously unseen; and as evidenced in *The How Report*, those qualities surface, ignite and catalyze geometrically in self-governing organizations.

That said, self-governing organizations and the business benefits they reap don't spontaneously come into being. Creating and maintaining them requires a strategy. So as a company leader, where should you start? Here's what we at LRN recommend:

Self-governing organizations and the business benefits they reap don't spontaneously come into being. Creating and maintaining them requires a strategy.

- Challenge your assumptions about governance, culture and leadership. Remember that these are drivers of business performance and that their impact is measurable. Pursue culture as a strategy by measuring it, and then take advantage of its strengths and address opportunities for growth.
- Extend trust throughout your organization and commit to leadership that inspires. Doing this ignites potential because power is not held and wielded from the top down. Rather, it is shared and used to achieve the mission and purpose of the organization through behaviors guided by universally accepted core values and principles.
- Embrace transparency. Understand that in today's world, very little remains hidden so it is more important now than ever to have nothing to hide. Help your company protect and maintain its good reputation by taking action to ensure that values and behaviors are aligned with purpose and business strategy.
- Stay committed, no matter what. The journey to self-governance is not easy. It requires letting go of control and proceeding into the unknown. This can be uncomfortable, especially in times of tumult and change. Keep going. Be deliberate and relentless in your focus on governance, culture and leadership; and continuously develop and implement strategies designed to shift behavior and thereby improve company performance.

At the end of the day, a company filled with inspired, empowered, self-governing employees who rally around shared principles and values to serve a higher-purpose mission – and who have at their fingertips tools and other methods of support by way of their company's ethics and compliance program and other business processes to help them behave legally, responsibly and ethically under any and all circumstances – will enjoy a position of markedly greater strength in the marketplace, and will be able to sustain and differentiate itself and to pursue significance far more easily, organically and effectively than its competition. Given that these results are real and have been proven, shouldn't you embark on the journey?

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Charles Ruthford
ECA Expert Panelist

Charles Ruthford is nationally recognized in the ethics profession as a leader in measuring organizational culture, ethics education and ethics program development.

With over 22 years of management and 14 years of front-line leadership experience, Charles served as ethics and compliance officer with The Boeing Company where, among other leadership roles, he chaired the Defense Industry Initiative on Business Conduct and Ethics (DII) Survey Team. His deep experience at Boeing included managing executive and senior-level leadership development programs at the Boeing Leadership Center where he was responsible for leadership, business, finance and strategy curricula. Charles retired from Boeing in March 2010.

Education and Communication Strategies for 2013

Effective Approaches to Mitigating Risk

The risks associated with ethics and compliance education and communication may seem minor when compared to the risks of FCPA (Foreign Corrupt Practices Act), ITAR (International Traffic in Arms Regulations), lobbying, or insider trading violation. The reality is that ineffective and outdated education and communication methodologies coupled with complacency from knowing that all employees have received their annual refresher training actually increases the risk of misconduct and violations of law.

Recent research in the areas of ethics and culture is shedding new light on how people view themselves in an ethical and compliance context and how they act in actual situations. By looking at how people use decision criteria and tools to help them choose to "do the right thing," the research calls into question many of the assumptions we've made in the past about how to influence ethical and compliant behavior.

Our traditional approach to ethics and compliance education and communication may have us "compliant," yet our employees are not prepared to deal with difficult situations. A reasoning- and rules-based educational focus does not necessarily guarantee proper behavior in such situations. However, when components of emotion and efficacy are added to the reasoning and values focus, employees do, in fact, demonstrate increased ethical and compliance behavior.

When components of emotion and efficacy are added to the reasoning and values focus, employees do, in fact, demonstrate increased ethical and compliance behavior.

Your current education and communication approaches are no doubt in alignment with common industry practices. You are not alone in your past assumptions about how to influence employee behavior through training. This report provides a clearer picture about how employees react in stressful situations. The findings may surprise you, and cause you to question your past approaches to ethics and compliance education and communication. The report suggests proven methods and tools that you can use to respond to these new findings and make your education and communication experiences compelling; more importantly, they can lead to behavior change and real compliance within your organization.

As an ethics and compliance practitioner, you strive to design and deploy educational experiences and communication events that will influence employee behavior and affect the ethical climate in your organization. One of your responsibilities is to identify and reduce risk. Employees must be prepared to "do the right thing" when they encounter a difficult situation. For

organizations to move from a myopic "rules-based" focus to a more expansive "values-based leadership" view, there is a need for new approaches and models.

This report is designed to help point you in the right direction and mitigate risk in your organization. Compelling education and communication experiences lead to more engaged employees, a greater sense of collaboration, a reduction in organizational risk, and improved business performance. More resources may be required to build and deploy such compelling experiences. This report also helps make the business case with senior leaders for expending additional resources to create and deploy these enhanced and effective experiences.

The Past and Present: Why Are We at Risk?

We had previously assumed that collective moral reasoning or the ethical climate in organizations leads to ethical behavior. While current and past research shows a positive correlation between collective moral reasoning (inputs) and ethical or compliant behavior (outcomes), the correlation isn't all that strong. In the 1980s and 1990s, ethics and compliance practitioners took a cognitive or knowledge-based approach to educating employees. Our assumption was that armed with knowledge, a decision-making process, and an awareness of consequences, people would make rational and proper choices.

The online format does a good job of conveying information to employees. However this format doesn't necessarily help influence or change behaviors.

Our classroom training focused on the rules and expected behaviors. Participants heard a clear explanation of the consequences of misconduct. Case studies and problem solving were used as examples to highlight rules and ethical principles. Employees were directed to their managers or an "ethics line" if they needed assistance or had an issue to report. Finally the classes provided a five- or six-step ethics decision-making process. These were high-quality classes. They were designed and built by experienced instructional systems design professionals and delivered, in person, by qualified instructors.

We heard two common messages from employees about these classes. First they were not shy about telling us they "got" the ethical principles after the first class, and they asked whether their brains been cleared on the 366th day, requiring them to be "refreshed" each year. Secondly we heard sarcastic comments about how the individual employees were being punished for the misdeeds of senior management by having to participate in the annual refresher training.

As computer and networking technology improved, the classes were transformed into an online format to take advantage of the scalability and efficiency features of the Internet and company intranets. The online format does a good job of conveying information to employees. However this format doesn't necessarily help influence or change behaviors.

The Latest Research: Preparing to Meet the Risks

In their 2011 book *Blind Spots*, professors Max Bazerman (Harvard Business School) and Ann Tenbrunsel (University of Notre Dame) write about how people act against their own ethical values, and how they aren't as ethical as they may think they are. The situations the authors describe are more common than you

might realize. Their research data clearly show how people, when asked about a difficult or confrontational situation, say they will act ethically. This is what they "should" do. In the *real* situation, they choose the non-confrontational or easy path, and act unethically. This is what they "want" to do. When asked to recall how they acted, they engage in a form of revisionist history and describe what they did as ethical. After all, in seeing themselves as ethical people, they couldn't have engaged in unethical behavior. You can imagine how this line of reasoning could move people onto the "slippery slope" of seeing unethical behavior as actually being ethical.

The authors also presented data showing how over 50% of respondents said they would act a certain way when facing a situation, and yet when they actually encountered the situation, none of the respondents acted the way they predicted. It's clear that people *intend* rather than *demonstrate* ethical behavior.

In the recommendations sections of their book, the authors state that ethics and compliance education and communication, in order to be effective, need to move away from knowledge-based and rational thinking, and toward a behavioral and psychological focus.

To be effective, ethics and compliance education and communications need to focus on intuition and emotion, in addition to facts and consequences.

The second piece of research is from Nobel Prize Laureate Professor Daniel Kahneman. In his 2011 book *Thinking Fast and Slow*, Professor Kahneman describes two systems in the brain. One system works quickly, using intuition and emotion to guide decisions. The other system works slowly, evaluating situations from a more thoughtful and rational perspective. When it comes to ethical or compliance dilemmas, in which people have a stake in the outcome, they will make their decision in a split second and be guided by their intuition and emotion. They won't even consider using the six-step ethical decision-making model.

While Professor Kahneman doesn't give specific recommendations for education and training, it's easy to see how his research agrees with that of Professors Bazerman and Tenbrunsel. To be effective, ethics and compliance education and communications need to focus on intuition and emotion, in addition to facts and consequences.

The third piece of research comes from Professors Anke Arnaud (Embry-Riddle Aeronautical University) and Marshall Schminke (University of Central Florida). In their paper "The Ethical Climate and Context of Organizations: A Comprehensive Model," *Organizational Science, November/December 2012*, the authors describe how adding emotion and efficacy to moral reasoning greatly enhances ethical behavior. In the past, emotion was thought to hinder rational business decision-making. Our earlier management and leadership training and measurement systems stressed the deleterious nature of emotion. The latest research, however, shows how emotion actually *enhances* rational business decision-making.

Professors' Anke and Schminke results highlight and confirm previous research concerning ethical efficacy. Ethical efficacy occurs when people believe that the action they are about to take, or the questions they need to raise, will have an effect on ethical behavior, be meaningful, or make a difference within the organization. Their findings go on to say that when collective moral reasoning, collective moral emotion, and collective ethical efficacy are all synchronized, the effects on ethical behavior jump dramatically.

An Effective Approach to Ethics and Compliance Education

The steps below will help create the compelling educational and communication experiences that will influence people and cultures at emotional and intuitive levels.

1. **Interaction.** Experiences need to be interactive in nature. When participants are able to view a situation or case study, and experiment with a number of different solutions to see which one works best, they are able to recognize the best approach. They can incorporate that best solution into their daily activities, and are more likely to react properly when a difficult situation occurs.
2. **Collaboration.** Compelling education and communication activities need to support collaboration between several participants. People learn best when they have an opportunity to tell stories, listen to others, and consider different or diverse ideas about a situation. By our nature, we humans learn best together.
3. **Problem Solving.** Research shows that participants rate education and communication activities more effective and satisfying when they employ real-life case studies, solve ethical dilemmas, and engage them in role-playing.
4. **Transformation.** The activities also need to be transformative. There needs to be time in the activity to discuss concrete examples of how the ethical principles and desired behaviors apply directly to the participant and his or her organization. How will people need to change?
5. **Reflection.** The transformation process starts to take hold when there is time allocated for reflection. During reflection, participants talk about and possibly write about the individual and organizational changes that are necessary to incorporate the ethical principles and desired behaviors into daily activities. At this point, participants are making choices on how they will act in the future.
6. **Learner-Directed Outcomes.** Adult learning principles assert that participants report greater satisfaction with the learning activity, and find it more effective, when they can customize the experience to suit their specific needs. One size does not fit all. To be meaningful, the learner needs to be able translate and apply the ethical principles and desired behaviors into his or her context. This is not to be confused with "situational ethics," where people modify the ethical principles and desired behaviors to justify unethical acts.
7. **Front-Line Management Involvement.** Education and communication experiences are most effective and satisfactory when front-line managers lead and have a significant involvement in the activity. Research published by Larkin and Larkin in their 1994 book Communicating Change, Winning Employee Support For New Business Goals, shows that the front-line manager is the person in the organization most trusted by employees. Management's involvement and leadership further solidifies the alignment with values, strategies, and tactics.

Participants report greater satisfaction with the learning activity, and find it more effective, when they can customize the experience to suit their specific needs.

Attributes and Results of Education and Communication Approaches

Assumption	Assumption
Ethics and compliance decision-making is a split-second process. People unconsciously use emotion and intuition to guide choices	Ethics and compliance decision-making is a rational, reasoned-through process
In both cases, it is assumed that the person making the decision will be personally and significantly affected by the outcome.	
New Approach to Education	**Past Approach to Education**
• Interactive exercises and activities provide opportunity to experiment. • Collaboration brings in different ideas and approaches. • Problem-solving with real-life examples engages participants. • Transformative activities launch change processes that affect emotion and intuition. • Reflection promotes "how am I going to do this differently in the future" thinking. • Learner-directed outcomes encourage the learner's increasing engagement. • Front-line management involvement increases trust and engagement.	• Lessons provide knowledge and information about expectations and rules. • Examples make consequences for misconduct clear. • Exercises promote practicing the concepts. • Supplemental materials provide decision-making tools and support mechanisms.
Results	**Results**
• Education and communication experiences are more engaging and compelling, resulting in greater acceptance and retention. • Education and communication experiences influence emotion and intuition. • Employees are better prepared to deal with difficult situations, because they naturally engage emotion and intuition in decision-making. • Risks are reduced.	• Education and communication experiences provide knowledge and do not affect emotion and intuition. • When dealing with difficult situations, employees will still decide based on emotion and intuition, and will not apply the "rational" decision-making process. • The initial assumption of "rational" decision-making is false. • Employees are unprepared for difficult situations and may choose to do the "wrong thing" based on what they want to do, rather than on what they should do.

Ethics and compliance decision-making is a split-second process. People unconsciously use emotion and intuition to guide choices.

Tying It All Together

To create and deploy compelling ethics and compliance education and communication experiences, one must obtain support within the organization. These educational experiences will cost more than the traditional methods of the past. The good news is that investment in education and communications activities, along with a focus on values-based leadership, collaboration, engagement, and culture, all produce a positive return on investment. Cultural change does take commitment, persistence, and patience. Once started, positive cultural changes can snowball, and organization members will be more engaged, satisfied, and productive. People will demonstrate ethical behavior, while business performance will improve. Professors John Kotter and James Haskett, in their 1992 book *Corporate Culture and Performance*, describe tremendous performance improvement in organizations with collaborative environments.

To support the educational thrust, additional initiatives to improve *commitment*, *alignment*, and *involvement* are required. While this report focuses on the education and communication initiatives, the other initiatives are briefly described below, with references to other writings and toolkits where practitioners and leaders can learn more.

Values and desired ethical behaviors need to be evaluated in manager and employee performance appraisal processes… The old adage "what gets measured gets done" is still true.

Initiative 1: Setting the Tone. Senior leaders must set the tone in the organization—that values-based leadership and ethical behavior are the expected norm. They do this through modeling desired ethical behaviors, requiring accountability, and linking decisions to organizational values. More information, tools, and examples describing and supporting leadership action on this first initiative can be found on the LRN Inspirational Leadership Alliance website.

Initiative 2: Tone in the Middle. Initiative 1 makes a clear case for guidance, commitment, and action from senior leaders. There is an equally important role to be filled by mid-level leaders and managers. As exemplars of ethical and compliant behavior, team members in the middle are responsible for passing along the values of the culture. More information, tools, and examples can be found in the "Tone in the Middle" toolkit on the LRN Ethics & Compliance Alliance website.

Initiative 3: Establish Measurement Systems. These systems need to measure corporate culture, and offer rewards when the desired values and behaviors are demonstrated. This is a two-pronged initiative. First, a set of metrics and organizational performance measures are required. Aligned with values-based leadership and ethical behavior, these measures need to go beyond financial performance and the "sacred" net income, free cash flow, and P/E ratio metrics.

Second, values and desired ethical behaviors need to be evaluated in manager and employee performance appraisal processes. Are the values and behaviors required to support an ethical culture talked about and used to rate employee and management performance? Are rewards given based on those ratings? The old adage "what gets measured gets done" is still true.

Initiative 4: Building Compelling Ethics and Compliance Education and Communication Experiences. Now that senior and mid-level managers are setting the proper tone, and individual and organizational performance measuring systems are in place, it is possible to create education and communication experiences that truly are compelling and engaging. The efforts made in creating the educational experiences will stimulate an organization in a positive way. It's also a matter of alignment. When the same messages flow in multiple channels, members of the organization pay more attention and incorporate the messages into their personal models of how the organization is run. The result—cultural change starts to occur.

This new approach to learning and communication will require commitment by senior leaders, involvement of mid-level managers, and individual measurement systems that are aligned with organizational ones.

Summary

Compelling education and communication experiences that can influence people at emotional and intuitive levels can reduce ethics and compliance risk. These experiences will likely cost more to develop, and require more employee time to complete. This new approach to learning and communication will require commitment by senior leaders, involvement of mid-level managers, and individual measurement systems that are aligned with organizational ones. These costs are greatly outweighed, however, by the benefits of engaged employees who will respond in an ethical and compliant manner in difficult situations. They will do so in a collaborative environment, thus significantly reducing organizational risk, while at the same time improving business performance.

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Eric Feldman
ECA Expert Panelist

Eric Feldman is recognized for his deep knowledge and expertise in areas of government contracts and relationships. Eric retired from the Central Intelligence Agency (CIA) in 2011 with over 32 years of experience in Inspector General oversight and federal auditing in both the Executive and Legislative branches of government. Eric served in executive positions with the Offices of Inspector General at the Department of Defense, Defense Intelligence Agency, and CIA, and was the longest serving Inspector General of the National Reconnaissance Office (NRO) from 2003 – 2009.

Government Contracting and Relationships

Survival Strategies Beyond the Fiscal Cliff

The Impact of Federal Budget Cuts Looms Large for Contractors

In the 2012 LRN ECA Risk Forecast, I noted that government contracting requires a sharp calculation of risks versus rewards. Typically, that calculation has come out in favor of companies expending the necessary time and effort to maneuver a minefield of often complex and frustrating regulations in order to reap the financial benefits and stability associated with government contracting.

I also predicted that 2011 would be the beginning of a multi-year calibration of the role of government at all levels, and that this process could destabilize the once-predictable environment for government contractors for years to come. Unfortunately, this forecast turned out to be an understatement. Instead of the 2012 "sequestration" process inspiring cooler heads to prevail, the polarized political process has created a near certainty that 2013 will result in substantial challenges for government contractors at the federal, state, and municipal levels requiring unprecedented dexterity and prudent decision-making to survive and prosper in this "new world order."

Is the "Fiscal Cliff" as Dire as Advertised?

The FY 2012 budget included close to $1 trillion in cuts over 10 years, with $21 billion taking effect last year. The Budget Control Act (BCA) of 2011 requires the federal government to reduce spending by more than an additional $1 trillion by 2021. This amounts to cutting about $109 billion from the budget each year. To accomplish this, the BCA created the Joint Select Committee on Deficit Reduction (the "Super Committee").[1]

"Sequestration" was the name given to the mandatory, across-the-board spending cuts (totaling about $1.2 trillion) that would occur automatically should the committee fail to compromise. As we know, there was no grand compromise. Through sequestration, budget cuts would be split equally between defense discretionary spending and non-defense mandatory (entitlement) and discretionary (non-entitlement) spending, without an increase in tax revenue. This represents about $55 billion in cuts from both the defense and non-defense budgets every year. [2]

The polarized political process has created a near certainty that 2013 will result in substantial challenges for government contractors at the federal, state, and municipal levels requiring unprecedented dexterity and prudent decision-making to survive and prosper in this "new world order."

1 Conference Report on H.R. 2112, Consolidated and Further Continuing Appropriations Act, 2012, Congressional Record, November 14, 2011

2 Ousley, Jeff. Sequestration Could Have Serious Consequences for Military Members, Veteran's United, August 7, 2012 (www.veteransunited.org)

Defense spending cuts will be spread across all branches. While some programs may be spared, other sections of the military could see 7-10 percent of their budgets eliminated.[3]

Non-defense spending cuts are typically program-specific and categorized as either mandatory or discretionary. Most mandatory programs such as Social Security, Medicaid, food stamps, and retirement benefits are currently exempt from reductions. Medicare is the exception, though cuts are capped at 2 percent per year ($11 billion in 2013) and limited to providers and insurers, not beneficiaries. The Government Accountability Office issued a decision on May 21, 2012 that Department of Veterans Affairs spending is exempt from sequestration (with the exception of limited administrative expenses).

Non-defense spending cuts will be accomplished through broad reductions in funding for discretionary programs.

Non-defense spending cuts will be accomplished through broad reductions in funding for discretionary programs. If sequestration occurs, $1.2 trillion in budget cuts will begin on January 2, 2013, and continue through FY 2021.[4]

The BCA of 2011 also provides a way to avoid sequestration if Congress successfully acts to achieve equivalent deficit reduction savings. If Congress attains less deficit reduction savings than required, sequestration cuts will be reduced by the amount in savings actually realized. For example, if Congress creates $80 billion in alternative deficit reductions, and the plan becomes law, the $1.2 trillion sequestration will be reduced by $80 billion.[5]

On January 1, 2012, the House passed a series of tax changes and revenue enhancements that avoided the “fiscal cliff” of across-the-board tax increases (the Senate passed the same bill late into the night of New Year’s Eve). This bill also delayed sequestration required by the BCA of 2011 by two months, literally “kicking the can” down the road for the new Congress to deal with in the first quarter of 2013.

Although discussions of sequestration tend to be alarming, it may turn out to be the most politically and practically expedient way to avoid a true fiscal crisis. And, of course, Congress retains options to mitigate the effects of across-the-board cuts by:

- Reprogramming funds after the sequester;
- Changing the definition of “programs, projects and activities” (the budget level at which the cuts are implemented);
- Taking advantage of flexibility within operations and maintenance funds. Because the Office of Management and Budget has declared that war spending is eligible for sequestration, total cuts to operations and maintenance may be spread across a bigger pot of money.

It is important to note that sequestration does not affect funds already obligated and it is not intended to affect *existing* contracts. So if sequestration happens, the world as we know it will not end. Congress, OMB, and the Pentagon will, in fact, have more flexibility than they have been willing to admit.

But how will all of this impact government contractors?

3 Ousley, Jeff.

4 Venable.com

5 Martin, Willard. “Preparing for Government Sequestration and Budget Cuts,” Government Contracts Update, Winter 2012.

The Impact of Sequestration on Government Contracting

If sequestration occurs, the Congressional Budget Office estimates defense programs will be cut by 10 percent and non-defense programs will be cut by 8.5 percent in FY 2013. Consequently, contractors should prepare to navigate in an environment of increased competition.

Last fall, OMB began issuing agency apportionments for FY 2013. An apportionment is a legally binding order and it forbids an agency from spending more appropriated funds than OMB has allocated. In response, agencies are in the process of evaluating and prioritizing their budgets. Typically, agencies attempt to reduce personnel through attrition to meet budget cuts, but this is not a typical budget cut. Agencies will need to scale back the number and size of new contracts for programs deemed non-critical. Even critical programs will likely be impacted as agencies look for the most efficient ways to utilize reduced funding.

Agencies will need to scale back the number and size of new contracts for programs deemed non-critical. Even critical programs will likely be impacted as agencies look for the most efficient ways to utilize reduced funding.

Regardless of mitigating tactics, it is a certainty that sequestration, or even the threat of it, will impact government spending. Government contractors should therefore consider several possible impacts of budget reductions on the government procurement process:

- **Existing Contracts:** Limited funds could cause agencies to reduce the scope and quantity of products or services purchased on existing contracts. Agencies may choose to "de-scope" the quantity, capability, or breadth of contract performance through change orders, as well as partial, or even complete, contract terminations for convenience. However, outright terminations for convenience require the government to pay recoveries to terminated contractors; these may therefore be used sparingly. Contractors should expect agencies to propose restructuring existing contracts to defer costs to the future. Such restructuring may result in more term contracts, extensions of contract schedules to match funding, and requests for waiver of existing contractor claims. Contractors may see their option periods waived, forcing them to negotiate new contracts at lower prices, and face increasingly price-sensitive competition.
- **New Contracts:** It is most likely that government contractors will see a decrease in the number of new contracts awarded, as agencies eliminate programs not absolutely essential to their missions. Types of contracts may also change, with agencies moving away from contract vehicles that place cost and performance risk on the government. For example, agencies are less likely to use cost-reimbursement and labor-hour contracts (previously favorites in the government services arena), instead favoring fixed-price contracts for a greater degree of cost certainty and lower risk. Indefinite Delivery/Indefinite Quantity contracts will also become more attractive for the government because they allow agencies to negotiate at the task order level. In addition, government contractors are already seeing a trend away from "best value" procurements toward lowest-price, technically acceptable sources.
- **Bid Protests:** Stiffer competition for contracts will likely bring an increase in bid protest litigation, particularly from incumbents seeking to extend their performance on contracts, and offerors who need the awards to remain viable players in the government contracting space.

- **Procurement Integrity Violations:** Intensified competition for fewer contracting opportunities can create a high-risk environment within companies, making them susceptible to employee misconduct, particularly with regard to following the rules of the competitive contracting process. In an effort to win contracts, curb layoffs and staff reductions, employees (particularly those in the contract "capture" process) may feel motivated to ignore or marginalize their company ethics and compliance programs and use whatever information is at their disposal—even prohibited government or competitor acquisition data—to give them an edge in the bidding process. Such ill-advised actions will lead to government investigations, prosecutions, suspensions and debarments, and increase the risk for contracting officials who might be entirely unaware of such behaviors within their companies.
- **State and Municipal Contracting:** Although federal budget reductions have an obvious impact on federal contractors, the potential impact on companies that contract at the state and municipal levels should not be ignored. States and municipalities are already reeling from the loss of tax revenue due to the recession. It reasonable to assume that follow-on cuts in federal spending in education, healthcare, transportation and housing, for example, will result in additional reductions in the number and value of contracts administered at state and local levels. Increased competition for fewer contract dollars could result in similar or even more serious problems with procurement fraud, problems less likely to be discovered in a timely manner given the scarcity of oversight resources at these levels of government.

Proposals that incorporate ethics assessments, training, and education at the project level provide evidence of commitment to controls and accountability important to government agencies in this new environment.

How Can Contractors Position Themselves to Weather the Budget Storm?

There are several proactive steps government contractors can take to mitigate the risks of budget cuts, improve their competitive posture, and survive the unpredictable environment that has become the "new normal" of government contracting:

- **Develop strategies for an increasingly competitive market.** It is important for government contractors to consider new ways to make themselves attractive and differentiate themselves from their competitors. Strong ethics and compliance programs, for example, have become a competitive differentiator on government contracts, as agencies can ill afford to deal with ethics and integrity problems in either the bidding or execution phases of mission-critical projects. Regular independent assessments of a contractor's ethical culture and ethics & compliance programs can help make the case that a company deserves the public trust. In addition, proposals that incorporate ethics assessments, training, and education at the project level provide evidence of commitment to controls and accountability important to government agencies in this new environment.
- **Be mindful of "scope creep."** As agencies try to stretch contracting dollars, contractors should verify that their program managers understand the company's obligations under the contract and remind them to notify upper management of any potential expansion of the contract scope

immediately. If it appears that the government has changed the contract, a company must provide prompt notice of the change and take steps to ensure that it captures the costs associated with the new work.

- **Submit claims early.** When a contractor has legitimate claims against the government, it makes sense to try to resolve them as early in the process as possible. This is especially true when the federal budget is tight; a contract with unresolved or unexplained cost overruns makes an easy target for budget watchdogs. If a contractor can establish—through a request for equitable adjustment or contract claim, for example—that the government bears responsibility for some or all of the cost growth, the agency may reconsider its plan to terminate a program. At minimum, a valid claim can reduce the likelihood that the government will terminate the contract for default rather than for convenience.

Contractors can help themselves by helping agencies document the results achieved, outcomes realized, and reasons why their activities are mission-essential.

- **Pay attention to quality and performance.** It bears repeating that in a tightening budget environment, the quality of contractor performance will be scrutinized and there will be other companies claiming that they can do a better job. Contractors can help themselves by helping agencies document the results achieved, outcomes realized, and reasons why their activities are mission-essential. Contractors should review performance assessments and seek to promptly correct reports that unduly attribute blame to them for matters beyond their control. Adverse assessments not only affect future business, they can weaken arguments for maintaining current budget levels on existing programs. Contractors should understand the circumstances under which they may challenge performance assessments under the Contract Disputes Act.
- **Identify opportunities created as government emphasis shifts.** There are some areas in which government spending is likely to increase. For example, the proposed DoD FY 2013 budget increases spending on cyber-defense, intelligence, surveillance, reconnaissance, and space. With the potential cancellation of multiple major programs, DoD focus may shift to more proven, rapidly deployable, commercial technology. It is also widely believed that the second term Obama Administration will increase federal spending on infrastructures that were previously delayed or ignored by the states; thus, contractor opportunities may arise in highway and bridge construction, high-speed rail projects, airport redevelopment, and other job-creating projects.
- **Pay attention to subcontractors and team members.** With potential partial terminations and deductive changes, prime contractors are apt to face disputes among subcontractors and team members over remaining work share. Contractors who anticipate these scenarios and address them in teaming agreements and subcontracts will be in a better position to resolve such matters favorably. In addition, contractors should be aware that agencies are paying attention to the activities of their subcontractors, vendors, and suppliers, and exercise effective third-party due diligence to ensure that these team members meet expectations.

- **Be ready for increased government oversight.** Suspensions and debarments of contractors by government agencies reached an all-time high in 2011, with no signs of abating in 2012. It is likely that decreasing budgets and the increasing importance of contract integrity and performance will drive even more aggressive enforcement of Federal Acquisition Regulations in 2013. For its part, the Defense Contract Audit Agency (DCAA) has more tools than ever to collect monies from contractors, including the ability to withhold payments if the agency finds a significant deficiency in the contractor's business systems. Contractors will need to guard against unsupportable payment withholds by DCAA. Finally, the political discourse in 2012 indicated that declining taxpayer tolerance for waste, fraud, and abuse of public funds will continue to drive prosecutorial priorities in 2013 and beyond.
- **Assess the opportunities and risks of international markets.** With declining U.S. government budgets, many contractors are setting their sights overseas. While foreign governments and international markets present opportunities, contractors should be aware of potential pitfalls associated with international business, including the complexities of complying with Export Control Laws and the Foreign Corrupt Practices Act, which both the DOJ and SEC are vigorously enforcing.
- **Expect a smaller, less-experienced government workforce.** Several years of declining growth in the federal workforce, combined with pay freezes and proposals to change federal retirement and benefits, have taken a toll on many agencies' senior staffs. Among those affected is the federal acquisition workforce, which has been predicting for years that inexperience will wreak havoc with the contracting system. Government contractors have already experienced fallout from a less skilled and experienced public contracting workforce. For example, many have received inappropriately disclosed acquisition-sensitive information from inexperienced agency officials, who increasingly rely on contractors to catch these mistakes and serve as their "internal control."
- **Tend to corporate ethics and compliance programs: you may need them.** An already log-jammed legal system is likely to support the trend toward use of settlements and deferred/non-prosecution agreements to resolve both criminal and civil cases involving contractor misconduct. Many agreements will continue to contain ethics and compliance-related provisions, including requirements for remediation in areas of values-based ethics, internal controls, and ethical culture.

Suspensions and debarments of contractors by government agencies reached an all-time high in 2011, with no signs of abating in 2012.

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Marcia Narine
ECA Expert Panelist

Marcia Narine is a recognized leader in the ethics, compliance, and legal fields with deep experience leading and managing corporate ethics, compliance, and risk management programs and initiatives. Marcia supports our partners across a number of key focus areas to include Labor & Employment, E&C Program Management, Supply Chain, and Privacy.

Marcia recently served as vice-president and deputy general counsel of Ryder System, Inc., a Fortune 500 global transportation and supply chain management solutions company. At Ryder, Marcia oversaw the company's global compliance, business ethics, privacy, government relations, enterprise risk management, corporate responsibility, and labor and employment legal programs. Prior to this role, Marcia served as group director of human resources for Ryder's supply chain solutions division.

In addition to the above leadership roles, Marcia has recently been appointed by the U.S. Secretary of Labor to serve on the Whistleblower Protection Advisory Committee.

The Department of Justice recently issued a 120-page guidance on the Foreign Corrupt Practices Act.

Labor and Employment

2013 Employment Law Update

Compliance and ethics officers (CECOs) have so much on their plates that they can sometimes forget how their roles can overlap with others within the organization. As senior members of the leadership team charged with ensuring board members are comfortable with the state of the compliance program, here are the top issues CECOs may want to discuss with the employment lawyers and HR professionals in the organization.

Incentives

HR professionals are experts in designing incentives programs through salaries, bonuses, promotions, and other rewards strategies. Similarly, compliance officers know that incentives are a key component of effective compliance programs under the Sentencing Guidelines.[1] The Department of Justice recently issued a 120-page Guidance on the Foreign Corrupt Practices Act.[2] While the HR department might not think that bribery issues are within their purview, CECOs and HR professionals know that employees may confide in their managers before they call anonymous hotlines, the law department, or faceless people in compliance whom they have never met. On the flip side, the employee may be disgruntled and bypass the company altogether, going straight to the government to seek a reward under the Dodd-Frank whistleblower program.[3]

Compliance, legal and HR should work together to ensure that all relevant management and line personnel with exposure to government employees, inspectors, agents, and others in a position to ask for, give, or accept bribes understand the nuances of the DOJ's Guidance and the government's expectations. They may not want to give cash incentives to employees for reporting bribery—would reporting suspected bribery be more "valuable" than reporting sexual harassment for example? But a public acknowledgement from the company CEO provides significant intrinsic rewards and can be valued more by employees.

Furthermore, incentive programs can backfire. Many companies provide bonuses for individuals or departments if, for example, they have no accidents or injuries within a specific time period. At first blush this would appear to promote a culture of safety. These programs have the added bonus of lowering workers compensation costs. However, in 2012 the Occupational Health

1 USSG § 8B2.1(b)(6)

2 http://www.justice.gov/criminal/fraud/fcpa/guide.pdf

3 http://www.sec.gov/whistleblower. Under the Dodd-Frank whistleblower program, the employee could, under certain circumstances, receive 10-30% of any recovery over $1,000,000 that the SEC receives.

and Safety Administration (OSHA) reiterated its position that safety incentive programs can be considered acts of discrimination if they provide employees with justification for not reporting legitimate accidents or injuries.[4] It's worth examining the training, policy manuals, emails, documentation, recordkeeping, and especially employee perceptions to assess whether the company has vulnerabilities in this area. OSHA recommends rewarding safety training, repairing hazardous workplace conditions, and reporting accidents. Although the company may have been acting in good faith, OSHA has sent memos to regional field offices to step up enforcement in this area of safety incentives that may penalize workers.

The regulatory agenda

A number of states are considering or have passed laws on unemployment discrimination making it unlawful to refuse to hire someone because they have been out of work for too long.

Now that the elections are over, cash-strapped state and federal regulatory agencies are moving into high gear in terms of enforcement and collections of fines and penalties. Additionally, state legislatures typically enact new laws that go into effect in January or July. It is critical that CECOs check with their law departments and HR professionals to make sure that they are in compliance with any new laws.

The poor economy has led to a new category of laws that makes employers particularly vulnerable. A number of states are considering or have passed laws on unemployment discrimination making it unlawful to refuse to hire someone because they have been out of work for too long. Because of the economy and foreclosure crisis, some states now forbid employers from inquiring about credit during a background check. These kinds of issues can not only subject the company to significant financial liability, but the firm can also suffer reputational harm.

In the past two years, a number of states have enacted controversial or particularly onerous laws from a compliance perspective. For example, 17 states have passed guns-in-the-workplace laws, but there are a number of exceptions. Is your workplace one of them? Do your employees travel to such "exceptional" work sites? Do your employees cross state lines to meet regularly with customers where the laws may be different? With the increase in workplace violence, managers need to be prepared to deal with these issues.

Other states have passed medical marijuana laws. But what if some of your workforce is subject to federal drug testing laws? Adding to the complexity, what if your employees live in states that have recently legalized marijuana for recreational use? You will need to make sure that your HR, in-house, and outside legal counsel have thought these issues through and have clearly communicated policies and talking points for managers who may watch local news, or try to interpret the laws themselves by looking to the Internet or other unapproved sources for answers.

At the federal level, on December 17, 2012, the Equal Employment Opportunity Commission (EEOC) released its 2013-2016 Strategic Enforcement Plan (SEP). The SEP lists the following priorities: 1) eliminating barriers in recruiting and focusing on practices that steer individuals into specific jobs due to their status

4 http://www.osha.gov/as/opa/whistleblowermemo.html

into a particular group; 2) protecting vulnerable workers, particularly migrants and immigrants, and specifically focusing on job segregation, human trafficking, disparate pay, and harassment; 3) focusing on the Americans with Disabilities Act, and the employer's use of the undue hardship and direct threat defense; 4); reviewing the pregnancy-related limitation both under the ADA and under Title VII of the Civil Right Act; 5) seeking protection for lesbian, gay, bisexual and transgender individuals under Title VII; 6) enforcing equal pay laws; 7) proceeding against employers who use overly broad settlement waivers or engage in retaliation; and 8) preventing harassment through educational outreach and litigation.

The EEOC has also indicated that it will continue to consider the use of criminal background checks as a screening tool as a possible violation of Title VII. The EEOC has cited social science statistics indicating that background checks tends to disfavor blacks and Hispanics, who are arrested and convicted at a higher rate than whites. Applications asking for date of birth and pre-employment tests are also red flags for the EEOC. Employers should review their hiring, pay, and promotion practices to ensure that there is a clear connection to documented, bona fide job requirements. The EEOC will continue to aggressively pursue large systemic cases, especially those showing adverse impact.

The National Labor Relations Board has also been active in the past year, and its rulings impact non-organized workforces as well. In addition to key social media decisions, which have been covered elsewhere in this publication, the NLRB issued rulings on at-will employment and off-duty access policies.

Employers commonly state in employee handbooks that the employee's status is "at will," meaning that they can be terminated at any time for any reason with or without cause so long as the reason is not unlawful. In two cases this year, the NLRB found that clauses which stated that the at-will status "could not be amended, modified or altered in any way" were unlawful. Although these may have been cases of in-artful drafting, in a recent speech the Acting General Counsel of the NLRB made it clear that if a worker believes that unionization or a valid collective bargaining agreement cannot alter their at-will status, then the at-will disclaimer could be unlawful. The takeaway for a company is that even if an at-will disclaimer has different words, an employer may need to consider what the reasonable worker might think while reading it.

The Acting General Counsel of the NLRB made it clear that if a worker believes that unionization or a valid collective bargaining agreement cannot alter their at-will status, then the at-will disclaimer could be unlawful.

Many employers, particularly those in hospitality or other workplaces open to the public, have a "no-access" rule, where off-duty workers are not allowed to come on site except under limited circumstances. Under NLRB rules, a no-access rule is valid under only three conditions. The rule must (1) limit access solely with respect to the interior of the employer's premises and other working areas; (2) be clearly written and distributed to all employees; and (3) apply to off-duty employees seeking access to the facility for any purpose and not just to those engaging in union activity.[5]

Finally, the Department of Labor (DOL) has probably been among the busiest regulatory agencies over the past few years, and 2013 promises to be no different. In addition to overseeing OSHA, which was discussed above, the DOL

5 On Friday January 25, 2013, an appellate court ruled that President Obama's recess appointments to the NLRB were unconstitutional which in turn potentially invalidates any rulings handed down during their service. Companies should work with their outside counsel to determine whether the court's actions affect any company policies.

is responsible for wage and hour compliance under the Fair Labor Standards Act. The Fair Labor Standards Act generally provides that employees must be paid an overtime premium for any hours worked over 40 in a work week, unless they are subject to an exemption. Companies that have not already faced an individual wage and hour claim, or a wage and hour class or collective action, should be working with their HR and legal teams to make sure that they have already commenced an attorney-client protected wage and hour audit to protect themselves from a potential multi-million dollar lawsuit. A number of employers are facing litigation in the state courts as well.

But how should organizations prioritize wage and hour audits? It depends on the business model. Organizations using a number of temporary agencies may have joint employer risk. Consider, for example, the temporary worker whose assignment is to replace someone who is out for three months, yet has been at the work site for two years. That temporary worker can claim to be the company's employee. That risk multiplies when a company outsources a major part of its workforce to another company, and it isn't clear who manages what part of the workforce.

All companies need to ensure that they have not misclassified their workers as exempt (salaried) rather than non-exempt (hourly).

All companies need to ensure that they have not misclassified their workers as exempt (salaried) rather than non-exempt (hourly). It is critical to look at more than just job descriptions, or what employees say in interviews. Instead auditors must focus on what the employees actually do, remembering that what employees do at one location may be very different than what the employees with the same job title do at another location in a different city, or even down the street. Similarly, what employees do at your company may be different from what employees at your peer companies with the same job title do. Additionally, what employees tell the company auditor that they do may be very different from what they will tell a DOL investigator behind closed doors, or what the investigator will actually see while watching the employee do his or her job. Employers also face increased risk for unpaid overtime with more workers telecommuting, working through lunch, and checking email from home, because they are worried about keeping their jobs.

Employers using the salaried non-exempt classification or fluctuating work week should check with their employment counsel, because the Department of Labor stated in 2011 that anyone who pays their employees any bonuses or premiums cannot use the fluctuating work week. The DOL's statements and interpretations of court rulings are not binding. Nonetheless, companies should not ignore the risks and may want to consider basing bonuses on metrics such as performance, productivity, sales, or safety. You should work with counsel and review relevant court decisions in your jurisdiction.

Finally, although the national unemployment statistics are getting better, many people still cannot find work, and overqualified people are willing to work as interns with the hopes of gaining full time paid employment. The DOL has very specific rules regarding who qualifies as an unpaid intern, and increasingly, unemployed people who volunteer to work as interns are filing wage-an-hour claims.

5 http://www.dol.gov/whd/regs/compliance/whdfs71.htm#.UNOBh4njnAU

Who's The Boss?

In the spring or summer of 2013, the Supreme Court will rule on a case that could fundamentally change the workplace. Title VII forbids employers from practicing workplace harassment, discrimination, or retaliation, and from doing so through their agents, which include supervisors. The Court agreed to hear *Vance v. Ball State University* from the Seventh Circuit, which involves an African-American kitchen worker. Vance alleged that her co-employees actually served in the capacity of her supervisors because they directed her day-to-day activities, and that their actions, including racial epithets and physical threats, created a hostile work environment. Both the lower court and the Seventh Circuit ruled that a supervisor is a person who has the actual authority to take a specific workplace action—such as hiring, firing, transferring, demoting, disciplining, or promoting an employee. Currently there is a split in the circuits, with some holding that an employee with the authority to control what a fellow worker does on a daily basis is a supervisor as well.

Although the economy is improving, job applicants who are not hired, or current employees who are disciplined, demoted, passed over for promotion, or terminated will not hesitate to bring legal action against the company.

The Supreme Court ruled on vicarious liability in the context of sexual harassment in 1998, but did not rule on the definition of a supervisor. The EEOC has always taken the position that co-workers can subject employers to vicarious liability for harassment and liability. The Vance case could therefore be a watershed ruling for employers.

Conclusion

Although the economy is improving, job applicants who are not hired, or current employees who are disciplined, demoted, passed over for promotion, or terminated will not hesitate to bring legal action against the company. The Supreme Court may make that even easier if it relaxes the definition of a supervisor. Similarly, organizations must contend with the alphabet soup of regulatory agencies—the EEOC, NLRB, DOL and OSHA have promised aggressive enforcement against companies, and states are enacting new and often confusing regulations. The plaintiffs' bar is emboldened by large victories in class and collective actions against employers. 2013 will therefore once again be a busy one for CECOs, and they must stay closely aligned with their colleagues in the HR and legal organizations to make sure that nothing falls through the cracks.

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Robert Bond
ECA Expert Panelist

Robert Bond has been a solicitor and notary public of England and Wales for over 30 years, and brings deep expertise and global perspective to our LRN ECA partner audience in areas of privacy and data protection, information security, global ethics and corporate responsibility, social and digital media, e-commerce, and Internet law among other important risk areas. Robert is a widely published author and recognized global authority in his areas of expertise.

Privacy and Data Protection

2013 Global Risk Perspective

This article examines current trends for the next year in Global Data Privacy and Information Security, with a focus on the EU and Asia, and considers what global companies should be doing to manage compliance and mitigate risk.

A year ago I looked at the draft EU Data Protection Regulation and it will be revisited here, but in addition, I will look at the increase in privacy law in the Asia-Pacific region and the continued challenges of implementing ethical hotlines in the EU.

I recently conducted a survey of multinational corporations as to their key concerns for data privacy compliance, and the greatest concerns in ascending order were:

- Cyber Crime
- Consumer Rights
- Cloud Computing
- Jurisdictional Issues
- EU draft Data Protection Regulation
- Cookie Compliance
- Global Data Transfers

Other issues of concern included:

- Managing Subject Access Requests
- Social Media in the workplace
- Bring your own device (BYOD) and data security

Interestingly, topics that were not particularly mentioned as concerns were:

- Privacy by Design
- Screening and monitoring of Employees
- Data Leakage
- Data Management
- Engaging the board

While it is not surprising that issues such as data transfers, cookies law, and the EU regulation were high on the list, we do expect that before too long key topics will include:

This article examines current trends for the next year in Global Data Privacy and Information Security.

- Data Security
- Data Breaches
- Data Management
- Managing Consumer Concerns

Data Privacy Laws in Asia-Pacific

Asia Pacific is certainly a region to watch due to its rapid development in privacy laws, particularly in 2012. The Philippines' Data Privacy Act, which was signed into law in August, 2012, is the first uniform privacy law for the country. It is a European-style data protection law with procedures to be followed in the collection, processing, and handling of personal information. The Act also sets out the rights of data subjects and creates a National Privacy Commission.

Asia Pacific is certainly a region to watch due to its rapid development in privacy laws, particularly in 2012.

Singapore passed its Personal Data Protection Bill in mid-October, 2012. It creates an overarching data protection regime that applies across the economy. Organizations are prohibited from sending marketing messages to Singapore telephone numbers registered on a new Do Not Call Registry (the DNC Registry). A Personal Data Protection Commission is established to promote awareness of data protection and to enforce the bill. The bill is likely to be passed as an Act in early 2013, with a 12-month for the DNC Registry provisions and an 18-month transition period for the rest of the bill.

Most of Hong Kong's Personal Data (Privacy) (Amendment) Ordinance 2012 took effect on October 1, 2012. One new requirement is that when data users use personal data, or provide personal data to another for use in direct marketing, they must provide data subjects with prior notice, and obtain their consent or indication of no objection. Moreover, the data users have to take reasonable steps to ensure the security of personal data that they hold, and will also be responsible for any acts performed by any data processors whom they appointed.

Another piece of legislation that came in effect on October 1, 2012 is Taiwan's Personal Data Protection Law. The definition of "personal data" has expanded under the new legislation, which applies to all individuals, legal entities, and enterprises collecting personal data.

Australia passed the Privacy Amendment (Enhancing Privacy Protection) Bill in late November, 2012. It sets out the Australian Privacy Principles and strengthens the power of the regulator. Another development is Australia's consultation on mandatory data breach notification. The deadline to submit response to the discussion paper ended in late November, and the results are due for release in 2013.

On December 28 the People's Republic of China (the PRC) passed the Resolution Relating to Strengthening the Protection of Information on the Internet (the "Resolution"). This nationwide, legally binding set of rules follows a series of developments in the PRC, such as the Several Regulations on Standardizing Market Order for Internet Information Services from March, 2012. Although it is brief and limited to electronic personal information, the Resolution obliges Internet service providers and other businesses to adopt necessary security measures to protect personal information, to state the purposes of the collection and to obtain consent from data subjects. It is unclear how the Resolution will be applied.

Last but not least, on January 1, 2013, Malaysia's Personal Data Protection Act 2010, also a European-style legislation, has finally come into force. It is noteworthy for the heavy penalties that it introduces for non-compliant companies.

A number of other jurisdictions in the region have introduced or updated their privacy laws in recent years:

- Macau has a Personal Data Protection Act 2007 which could trace its European origins from the jurisdiction's historical links to Portugal.
- Japan's Act on the Protection of Personal Information has been effective since 2005 and provides moderate regulation.
- The high standard required by South Korea's Personal Information Protection Act 2011 has led to some commentators calling it the strongest law in Asia, if not the world.
- India issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules in 2011 which widens the scope of its Information Technology Act 2000.
- Vietnam's Law for the Protection of Consumer's Right 2010 took effect in July, 2011, and introduces some obligations on the collection of consumer information.
- Thailand also has a Personal Data Protection Bill in the pipeline.

So far, Europe has been shaping global data protection standards. However, as the value of data to businesses continues to grow across a broad range of sectors, the number of non-European countries with privacy laws is also increasing rapidly. The risk of non-compliance is significant, and companies should be aware of developments in jurisdictions beyond Europe.

So far, Europe has been shaping global data protection standards. However, as the value of data to businesses continues to grow across a broad range of sectors, the number of non-European countries with privacy laws is also increasing rapidly.

Ethical Hotlines and EU Data Protection Laws

The use of hotlines and other reporting mechanisms as part of compliance with the Sarbanes-Oxley Act of 2002 ("SOX"), and anti-bribery and anti-trust laws, must take account of data protection, labor, and human rights legislation in the EU and perhaps other countries. For example, internal company investigations resulting from whistleblower reports or other litigation must now also take into account EU and other country data protection laws, when such matters or discovery involve the acquisition or transfer of personal data to the U.S., or the taking of adverse personnel action in that EU country.

Currently at least 14 jurisdictions have published guidance or opinions on the implementation of ethical hotlines in the EU, namely Austria, Belgium, France, Finland, Germany, Hungary, Ireland, Italy, Netherlands, Norway, Portugal, Spain, Sweden, and the UK. Poland has not yet issued an opinion but their regulator, the GIODO (the Polish DPA), is aware of the need to provide guidance.

Current guidance

While the EU Article 29 Data Protection Working Party has issued its own opinion on the topic of whistleblower hotlines, different countries within the EU implement the ED Data Protection directive (the "Directive") to a different extent.

For instance, data protection laws in Hungary are particularly strict and do not implement all of the legal grounds for processing data under the Directive. Some aspects of SOX could therefore be construed as being in conflict with the local law. Nevertheless, new guidance published by the Hungarian Data Protection Authority (DPA) allows companies to run hotlines, albeit with a restricted scope. On the other hand, in countries like Belgium, Finland, Ireland, and Norway no direct conflicts between local laws and SOX requirements exist.

Most DPAs have issued guidance assisting companies to set up hotlines which are compliant with their own local laws. Austria did not publish its own guidelines, but rather a statement setting out that it agrees with the Article 29 Data Protection Working Party opinion on whistleblower hotlines. Also Hungary, the Netherlands, and Ireland subscribe to that same Article 29 Opinion.

Filings

Do not forget that the requirement to notify the Data Protection Authority when setting up a whistleblower hotline exists in a number of EU member states including Austria, Belgium, Finland, Spain, and Portugal. However, there is no such formal requirement in Germany, Ireland, Italy, and the UK.

Data subjects in general need to be notified when personal data about them is being processed because in some of the continental Europe countries, e.g. France, whistleblowing is directly associated with denunciation, and as such, perceived as morally wrong.

While there is not a requirement to notify separately in Hungary, in the light of the stringent Hungarian laws, I would recommend that companies do notify the Hungarian DPA to ensure that the company is fully compliant, not only with SOX, but also with Hungarian legislation.

In France, the whistleblowing procedures need to be authorized by the local DPA—CNIL. In Portugal, a company must obtain special authorization before it can process data through a whistleblower hotline. In Poland, local law requires prior notification to GIODO before any transfer of data outside the European Economic Area, which is very likely when implementing and operating whistleblower hotlines.

Italy imposes an obligation for a public notice to be posted on the company's premises notifying of the existence of the hotline. Portugal even goes one step further and prescribes that employees should not only be made aware of all aspects of the scheme, but also the fact that it is voluntary in nature, and that there are no consequences for not reporting. There is an additional requirement in Portugal to inform the employees that abuse of the scheme or use of it in bad faith may expose the offender to disciplinary and legal proceedings. A different type of requirement exists in Switzerland and Poland where employees' representatives (or works council if one exists) need to be consulted with regard to the setup of a hotline.

Data subjects in general need to be notified when personal data about them is being processed because in some of the continental Europe countries, e.g. France, whistleblowing is directly associated with denunciation, and as such, perceived as morally wrong.

Restrictions on hotline providers

Data controllers and hotline providers must ensure that they take appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, disclosure, or access, and against all other unlawful forms of processing.

Is anonymous reporting allowed?

Out of the countries above, only Spain and Portugal have a straightforward categorical prohibition on anonymous reporting. Belgium and Germany permit anonymous reporting only in very restricted circumstances, and anonymous reporting is discouraged in Portugal, Netherlands, Austria, and Finland.

Limitations on scope of reports

Only a few of the jurisdictions allow setting up of whistleblower hotlines without significant restrictions. Austria and Belgium limit reporting to ”serious acts,” ”serious irregularities,” or ”crimes,” and only in situations where reporting clearly could not take place within the normal line of command. Norway follows similar wording with severe issues and legal offences, including corruption, financial crime, breaches of company ethics code, hazardous working conditions, and harassment.

Spain limits the scope of hotlines to substantial breaches that may result in the employee in question being disciplined or dismissed. No reports are permitted relating to general ethical breaches, workplace norms, worker grievances, or minor breaches. Entities that wish to extend the scope of their whistleblower hotlines to include sexual harassment, misconduct regarding protection of the environment, inhuman working conditions, etc., will need to justify in much more detail the legitimacy and need for the proposed processing.

Only a few of the jurisdictions allow setting up of whistleblower hotlines without significant restrictions.

Hungarian guidance on the matter refers to grave violations of company policies, and prohibits use of the system to control employees’ work performance.

Germany limits its scope to criminal offences against the interests of the company (e.g. fraud, misconduct, insider trading), or conduct that violates human rights or environmental interests.

France restricts hotlines pre-authorized by CNIL to reporting with regard to internal control in the financial, accounting, banking, and anti-bribery areas.

Portugal also restricts reporting to accounting, internal accounting controls, auditing, banking, financial crime, and anti-bribery matters. Whistleblowing schemes for companies’ internal policies are expressly prohibited. Reporting is also restricted to key management personnel only.

Finally, in Sweden, only serious irregularities that concern accounting, internal accounting controls, auditing matters, combating bribery, or banking and financial crime may be reported through whistleblowing channels. However, serious irregularities that concern vital interests of the company, or an individual’s life and health, may also be reported. Only employees in management or key positions within the company may be reported.

Understanding and planning to comply with the EU Data Protection Regulation

The intention of the Regulation is “to build a stronger and more coherent Data Protection Framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.” However, the Regulation in its

current draft form imposes significant changes to the way in which businesses will have to comply with Data Protection laws and regulations in the EU.

Based on the current version of the Regulation, businesses with entities in Europe that process personal data, use equipment in the EU for processing personal data, or are not in the EU but who process EU data subjects or monitor their behavior, will incur significant compliance obligations.

As the Regulation applies to both data controllers and data processors, and dramatically extends the enforcement powers of the regulators and the fines for non-compliance (2% of worldwide revenue for negligent or reckless breach), businesses will need to prepare for investment in EU data protection compliance.

Businesses with entities in Europe that process personal data, use equipment in the EU for processing personal data, or are not in the EU but who process EU data subjects or monitor their behavior, will incur significant compliance obligations.

The current amended Regulation is expected to be finalized in the spring of 2013, and will likely come into force by the end of 2014.

- The Regulation applies both to data controllers and data processors that have either legal entities in the EU, or that process personal data of EU data subjects, irrespective of the location of the controller or processor; but the Regulation does not apply where the processing is by an individual purely for personal or household activities.
- Most of the current definitions of data subject, personal data, and the like, remain the same, except that sensitive personal data now includes genetic and biometric information, Consent is defined as “any freely given specific, informed and specific indication of” the data subject’s consent. Also, “personal data breach” is now defined with respect to breach of security for which new obligations arise.
- Fair processing statements or privacy notices will have to be in plain and intelligible language, and drafted with certain data subjects in mind, “in particular for any information addressed specifically to a child.”
- In a privacy statement or privacy notice, there needs to be specific information given to a data subject with respect to the nature and purposes of the processing of their data and of their rights, specifically using icons to guide consumers. There are also detailed requirements in relation to profiling and the collection of data via social network services.
- There are redefinitions of the obligations for the data controller, joint data controllers, and the data processor. In addition, the data processor will have direct liability for compliance, which does not exist in the current regime.
- While the concept of registration with a data protection authority is limited to prior authorizations for certain data processing and data sharing, there is now a new obligation for the controller and processor to maintain an internal register of compliance, and to make this register available on request to the Data Protection Authority by virtue of its new powers.
- There are enhanced requirements for data security, and there is a mandatory breach notification procedure for all but small enterprises.
- There are new details in relation to Privacy Impact Assessments and specific prior authorizations and prior consultations before data processing or data transfers may be permitted. In relation to data transfers, there is considerably more detail on binding corporate rules as a solution to transborder data flows or transborder data transfers.

With respect to breaches of the Regulation, there are a whole new range of penalties and sanctions with fines for minor breaches of 0.5 percent of a business's annual worldwide turnover, rising to 2 percent of annual worldwide turnover in the case of intentional or negligent breach of the Regulations.

- For the first time, the role of the Data Protection Officer is introduced for all businesses that process data about more than 500 individuals per year. This will require businesses to put in place not only contracts for this new position, but also appropriate training and authority for purposes of compliance. The Data Protection Officer will be the person responsible for maintaining internal compliance registers, and serve as the interface between the business and the regulators.
- While there are other specific issues, the last one we wanted to mention is in relation to the new powers of enforcement for the Data Protection Authorities who will monitor, audit, provide guidance, hear complaints, conduct investigations, opine on compliance issues, and issue licenses for international data transfers. Furthermore, with respect to breaches of the Regulation, there is a whole new range of penalties and sanctions with fines for minor breaches of 0.5 percent of a business's annual worldwide turnover, rising to 2 percent of annual worldwide turnover in the case of intentional or negligent breach of the Regulations.

While there is no guarantee that the current version of the Regulation will be the final published Regulation, we anticipate that at this stage few significant changes or additions will be made, and therefore we are starting the process of considering the full range of compliance, policies, practices, and procedures that will be necessary for small, medium, and large enterprises, whether operating in a single EU member state or operating globally.

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Mike Salvarezza
LRN Knowledge Leader

Mike Salvarezza is a tenured and accomplished leader with a career that includes extensive experience in the complementary disciplines of information technology, records and information management and compliance systems, enabling him to succeed in traditionally difficult areas by combining unique perspective and knowledge. Working in the defense industry for nearly a decade, Mike transitioned to a successful career at Altria Group, Inc., where he embraced various positions of increasing responsibility within the IT function to include a role as Group Director, IT, that included responsibility for setting technology standards on a global basis.

In his current role, Mike serves as the Chair of the LRN Living HOW Council and People & Principled Performance Council and the LRN Governance System and helps to pioneer, communicate, and integrate knowledge in the areas of legal, compliance, governance and risk; ethical leadership; social responsibility and environmental responsibility.

Mobile devices are now the business appliance of choice. Smart phones, tablets, and other PDAs are generating and holding more records than ever before.

Records & Information Management for 2013

RIM for the Next Generation

2013 Risk Perspective

Records and Information Management continues to struggle with some fundamental challenges. The rapid advance of technology, the proliferation of mobile devices equipped with numerous data-producing and aggregating "apps," the migration to cloud computing infrastructures, and the transformational nature of social media platforms have made the difficulties of managing records more daunting than ever before. Executives responsible for ethics and compliance must now address growing complexity in the management of records and information within their organizations.

The Advance of Technology

Today's businesses rely on technology for virtually everything. Business records are almost exclusively becoming electronic and are generated by numerous devices, systems, and applications. Records Managers who have employed Retention Schedules to detail the appropriate retention periods and records disposition actions are faced with adjusting their thinking to accommodate new and different types of records.

Mobile devices are now the business appliance of choice. Smart phones, tablets, and other PDAs are generating and holding more records than ever before. Information Technology functions are now abandoning efforts to "control" which devices are used by employees in favor of a BYOD (Bring Your Own Device) approach. With this flexibility come numerous risks to the records manager:

- Inability to access company records that are housed on mobile devices
- Rapid sharing and proliferation of records from device to device and from one to many people.
- Difficult and expensive discovery efforts when records are needed for litigation, regulatory review, and other business purposes
- Co-mingling of business and personal records
- Difficulty in preserving and managing records through their lifecycle when located on mobile devices
- Difficulty in gaining compliance with legal hold requirements

Rapid expansion of data requirements, expenses associated with running company data centers, complex infrastructure upgrade projects, and numerous other traditional IT challenges are made even more difficult with the explosion of data volumes and cost pressures on companies whose focus must be on their core business. As a result, many IT departments are electing to move all or part of their infrastructure "to the cloud." Cloud computing enables companies to reduce their investment and take advantage of greater infrastructure flexibility over time. For the records manager, associated risks have emerged:

- Difficulty in having offsite data managed according to company retention requirements when in a shared environment
- Difficulty in accessing records during discovery and other business requests
- Difficulty in implementing and achieving compliance with legal hold requests

The explosion of social media is transforming the world as we know it. The nature of these platforms is changing the way that people connect, collaborate, and communicate, and it is dramatically changing the way businesses fundamentally operate. More and more, companies are marketing through social media, collaborating with business partners over social media, connecting with customers through social media, and even developing new products based on social media. Many of these interactions constitute business records, and most companies struggle with managing these records. The Financial Industry Regulatory Authority (FINRA) and the Securities and Exchange Commission (SEC) require that all business records related to financial transactions over any media, including social media, be preserved appropriately.

Professionals using social media to conduct business conversations need to be educated in how to responsibly and respectfully communicate using these media so as not to create enhanced risk.

Courts are becoming increasingly interested in social media communications in the context of litigation. Social media platforms encourage casual and informal communication, which is often seen as more "authentic" compared with carefully managed corporate communications. Professionals using social media to conduct business conversations need to be educated in how to responsibly and respectfully communicate using these media so as not to create enhanced risk.

The risks that records managers face from social media are:

- Inability to collect and manage company records created and located on social media
- Difficulty in searching for and finding appropriate records for litigation, regulatory, or business requirements
- The spontaneity and informal nature of social media communications increasing the risk of inappropriate company records
- Large and expanding volumes of unstructured data to manage

The Way Forward

Records Management is existentially and has historically been about "governance." The efficacy of records management programs has generally depended upon compliance, using the lens of a fear of running afoul of regulations, or suffering legal consequences for poorly managed records.

The United States Federal Office of Management and Budget (OMB) issued a memorandum in August, 2012, which refers to records management in different terms:

"Records are the foundation of open government, supporting the principles of transparency, participation, and collaboration. Well-managed records can be used to assess the impact of programs, to improve business processes, and to share knowledge across the Government. Records protect the rights and interests of people, and hold officials accountable for their actions. Permanent records document our nation's history."

Although this was a document focused on Government agencies, its implications can be extended to the public sector. Executives tasked with managing corporate records must view their programs and services as business enablers, striving to achieve the appropriate controls while creating programs that can work in today's ever-changing world to provide business benefit and advantage.

Records managers should implement governance structures that include business leaders in determining how to address records management concerns. The perspective of the business is vital to the creation of workable policies and procedures.

Records managers should implement governance structures that include business leaders in determining how to address records management concerns. The perspective of the business is vital to the creation of workable policies and procedures. Next-generation workers should also be invited to help shape the programs, especially as they relate to the usage of new technologies.

In order to manage records in the cloud, records management executives must first address service level agreements and contracts with cloud providers to ensure that records are managed in accordance with company needs, regulatory requirements, and legal obligations.

Social media platforms present unique challenges in terms of access and preservation of records. Records managers should investigate emerging management systems technology to capture records and preserve them for records management purposes, but should also be aware of the casual nature of social media communications, which heightens risk for inappropriate records creation. Without discounting the value of effective social media policies and guidelines, extra attention must be placed on education of workers who are engaged with social media platforms from a records management perspective.

Advanced search technologies will prove more valuable to records managers than comprehensive records management systems. Search technologies can be very cost-effective alternatives to costly manual searches for records, especially in the context of litigation and document discovery. In complying with their records retention requirements, records managers should consider search technology as a potential alternative to complex, and often ineffective, records management systems based on a repository model.

A Future Challenge:

Looking ahead, records management needs to fundamentally change by challenging the very requirements imposed by the regulators and courts, so that companies may derive financial benefits from more realistic programs—which stand a better chance of compliance over time. Simply put, the ability

to "manage records" may become impossible using traditional methods with the advent of new technologies that enable the rapid creation of rich content, immediate sharing of data worldwide to thousands of people, and the transformative nature of today's technology platforms. To address this challenge, records management executives, legal professionals, consortiums, and professional organizations must come together to fundamentally re-examine these practices and determine what can be changed, so that compliance with requirements is actually possible, and that businesses can derive value from the financial investments made in managing records. Companies must make a real effort to change the regulations and laws which inform the programs they try to implement.

To be successful in the long term, records management professionals must begin to challenge the very requirements that they are attempting to comply with, examining those requirements with an eye to overhauling and removing those that are outdated and impossible to achieve.

There are serious discussions taking place globally to update various laws and requirements to do just this. Efforts are underway to overhaul the existing and outdated EU Data privacy requirements, and similar efforts are taking place in many other countries as well. Records management executives should strive to help shape these changes in ways that are reasonable and contemporary, and that can withstand the advance of technology for years to come.

Conclusion

Government agencies are increasingly focused on addressing the obsolescence of existing policy and law as technology rapidly transforms the world around us. Ethics and Compliance executives in 2013 must remain committed to the governance of records in their companies while addressing significant technology challenges. Funding is necessary for management systems to address the identification, capture, and preservation of company records that exist in the cloud, on mobile devices, and on social media platforms. In order to attain that funding, records management executives must encourage the business to identify the risks and, more importantly, the business benefits associated with properly managing corporate records. To be successful in the long term, records management professionals must begin to challenge the very requirements that they are attempting to comply with, examining those requirements with an eye to overhauling and removing those that are outdated and impossible to achieve.

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Bradley J. Bondi
ECA Expert Panelist

Bradley J. Bondi brings a strong background and expertise to our LRN community in areas of SEC compliance and enforcement, insider trading compliance programs, and internal investigations on a global scale.

Brad is a partner at the Law Firm of Cadwalader, Wickersham & Taft, LLP, where he focuses on securities, corporate, and financial laws, and enforcement cases. Prior to joining Cadwalader, Brad was a member of the executive staff of the Securities and Exchange Commission where he served as Counsel to key SEC Commissioners advising on enforcement actions and regulatory rulemaking.

SEC Enforcement – Hot Topics and Trends

Review of 2012 and Outlook for 2013

Current Enforcement Activity

The Enforcement Division of the U.S. Securities and Exchange Commission (SEC) continues to aggressively pursue violations of federal securities laws by corporations, financial institutions, and individuals. Compliance and legal personnel must be proactive to ensure that appropriate controls and policies are in place to prevent or catch misconduct.

The SEC has been active this year with high-profile enforcement actions and investigations. According to its annual report, the SEC brought 734 enforcement actions this past year, the second highest number ever filed in a fiscal year (and one less than the 735 filed the prior year). Of these actions, 150 were filed in investigations designated as National Priority Cases, representing the Division's most important and complex matters—an approximately 30 percent increase over 2011. During 2012, the SEC obtained for $3.1 billion in penalties and disgorgement.

Much of these enforcement actions relate to conduct preceding or during the financial crisis. For example, during the past year, the SEC initiated enforcement cases relating to the financial crisis against top executives of the two largest government-sponsored entities for allegedly making misleading statements regarding the extent of each company's holdings of subprime mortgage loans; against former investment bankers and traders at a financial institution for allegedly overstating the prices of subprime bonds during the financial crisis; against former executives of a commercial bank for allegedly misleading investors about the size of the bank's loan losses during the financial crisis; and against former executives of a bank for allegedly participating in a scheme to understate millions of dollars in losses and mislead investors and Federal regulators during the financial crisis. In addition, the SEC remains active in investigating and bringing actions for insider trading, violations by asset management firms, accounting misconduct, and violations of the Foreign Corrupt Practices Act (FCPA).

The SEC remains active in investigating and bringing actions for insider trading, violations by asset management firms, accounting misconduct, and violations of the Foreign Corrupt Practices Act (FCPA).

The current enforcement focus of the SEC is a manifestation of the five specialized enforcement groups that SEC Enforcement Director Robert Khuzami established in late 2009: Asset Management, Market Abuse, Structured and New Products, Foreign Corrupt Practices, Municipal Securities and Pension Funds. With specialized enforcement groups focused on these areas, there undoubtedly will be further investigations and enforcement actions in these areas.

In addition to having personnel and resources allocated to them, these specialized enforcement groups are armed with new tools under the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank" or the "Act"), namely, the ability to offer whistleblowers, who provide original information that leads to an enforcement action, between 10 to 30 percent of the SEC's recovery. The year 2012 marked the first ever payout by the SEC to a whistleblower under the Dodd-Frank whistleblower bounty program. This program has the potential to change the landscape of the SEC's enforcement efforts.

Emerging Enforcement Trends

Certain trends in SEC enforcement likely will emerge over the next year that will determine the cases the SEC chooses to investigate and bring as enforcement actions. Monitoring these trends will be important as companies strive to remain compliant with federal securities regulations.

Increased Importance of Whistleblowers

The year 2012 marked the first ever payout by the SEC to a whistleblower under the Dodd-Frank whistleblower bounty program. This program has the potential to change the landscape of the SEC's enforcement efforts.

As part of Dodd-Frank, Congress created powerful incentives to encourage persons to report (i) potential violations of the federal securities laws to the SEC and (ii) potential violations of the Commodity Exchange Act (CEA) to the Commodity Futures Trading Commission (CFTC). While the Sarbanes-Oxley Act (SOX) encouraged up-the-ladder reporting by employees and allowed for self-policing and self-reporting by companies of potential violations, the Dodd-Frank whistleblower provisions create incentives for external reporting to regulators, thus hindering a company's self-policing efforts.

The SEC's rules to implement those provisions of the Act that are within the SEC's authority raise serious challenges for public corporations, financial services firms, and other companies that are subject to the federal securities laws. Companies can expect an increase in the number of complaints that circumvent internal reporting mechanisms, and that instead, go directly or through plaintiffs' lawyers to the government.

Under Dodd-Frank and rules passed thereunder, the SEC may award a cash bounty of 10 to 30 percent of recovery to any individual whistleblower who *voluntarily* provides the SEC with *original* information derived through independent knowledge of a possible violation of any federal securities law. The information must lead to a successful enforcement action resulting in monetary sanctions exceeding $1 million in order for the bounty to be awarded. While certain legal, compliance, and audit professionals are generally excluded from qualifying as whistleblowers, current and former employees, competitors, vendors, customers, and even wrongdoers (provided the wrongdoer is not convicted of a related crime) all may qualify as whistleblowers under the rule. The SEC has formed the Whistleblower Office in the Division of Enforcement to handle the inflow of tips from whistleblowers, and the agency is actively searching for whistleblowers in certain cases. (The CFTC also passed similar rules for its whistleblower bounty program and took similar actions in establishing a whistleblower office). The SEC estimates that it will receive approximately 30,000 tips, complaints, and referrals submissions each year pursuant to the Dodd-Frank whistleblower provisions.

Importantly, the SEC's whistleblower bounty program specifically allows and incentivizes individuals to utilize internal reporting channels *before* going to the SEC. The SEC's rules seek to accomplish internal reporting in three ways. First, the SEC rules provide that an internal whistleblower may be eligible for an award where the company reports to the SEC information received from the whistleblower or the results of an investigation initiated in response to the whistleblower's information. In those circumstances, all the information reported by the company will be deemed attributable to the internal whistleblower. Second, a whistleblower is deemed to have reported directly to the SEC at the same time he or she has reported internally, so long as the whistleblower voluntarily reports original, independent information to the SEC within 120 days of having first reported the information internally to the company. Third, the SEC will consider whether and to what extent an individual made use of internal compliance procedures when assessing the amount of the bounty.

Importantly, the SEC's whistleblower bounty program specifically allows and incentivizes individuals to utilize internal reporting channels before going to the SEC.

On November 15, 2012, the SEC issued its Second Annual Report on the Dodd-Frank Whistleblower Program (the "Report"), covering the period between October 1, 2011 and September 31, 2012. The Report, which satisfies congressional reporting obligations found in sections 922(a) and 924(d) of the Dodd-Frank Act, provides insight into the effectiveness of the Commission's whistleblower bounty program,[1] the activities of the office charged with administering the program, and the Investor Protection Fund from which bounty payments are made. The issuance of the Report offers an opportunity for companies to understand the focus of the Commission's whistleblower program and to reevaluate their own compliance and internal reporting systems.

The SEC made its first whistleblower award in fiscal year 2012. According to the Report, the whistleblower received the maximum award of 30 percent for helping the Commission stop an "ongoing multi-million dollar fraud."[2] The Report indicates that fines in the judicial action already exceed $1 million, with further judgments and sanctions possible.[3] Because the government collected approximately $150,000 by the end of the fiscal year, the Commission was able to pay nearly $50,000 to the whistleblower.[4] While the percentage awarded was the maximum of 30 percent, the total dollar amount is relatively modest considering that most securities cases involve hundreds of millions of dollars in fines and penalties, and thus the potential remains for far greater awards than the one discussed in the Report.[5] Because few details about the whistleblower, the fraudulent activity involved, or the company have been provided due to confidentiality provisions in the Dodd-Frank Act,[6] the larger

1 For more information on the SEC's whistleblower bounty program and best practices for companies dealing with whistleblowers, please see Bradley J. Bondi, Jodi Avergun, Thomas Kuczajda & Steven D. Lofchie, Cadwalader, Wickersham & Taft LLP, "The Dodd-Frank Whistleblower Provisions: Considerations for Effectively Preparing for and Responding to Whistleblowers," BUSINESS FRAUD ALERT, May 26, 2011, http://www.cadwalader.com/PDFs/newsletters/201105263321_BusinessFraudAlert_May_26.pdf.

2 U.S. SEC. & EXCH. COMM'N, ANNUAL REPORT ON THE DODD-FRANK WHISTLEBLOWER PROGRAM FISCAL YEAR 2012 8 (2012) [hereinafter "ANNUAL REPORT"].

3 Id.

4 Id.

5 Indeed, the amount pales in comparison to the whistleblower award of $104 million announced by the Internal Revenue Service (IRS) on September 11, 2012, in connection with the government's investigation of tax evasion by a Swiss bank. See David Kocieniewski, "Whistle-Blower Awarded $104 Million by I.R.S.," N.Y. TIMES, Sept. 11, 2012, available at http://www.nytimes.com/2012/09/12/business/whistle-blower-awarded-104-million-by-irs.html. The whistleblower, who was involved in that offense and who served two and a half years in prison, assisted the IRS in collecting over $780 million in fines and penalties from the bank. Id. By contrast, the SEC's whistleblower bounty rules do not permit a whistleblower to recover a bounty where the whistleblower was convicted of a related crime.

6 15 U.S.C. § 78u-6(h)(2).

significance of the award is hard to ascertain.[7] Interestingly, the SEC also denied another tipper in the same matter an award, reportedly because that person's information did not contribute significantly to the SEC's investigation.

The Report also provided information on the number of whistleblower tips, complaints, and referrals (TCRs) made during fiscal year 2012. According to the Report, 3,001 TCRs were received by the SEC's Office of the Whistleblower during the reporting period.[8] Nearly 50% of those TCRs fell within three complaint categories: Corporate Disclosures (18.2%), Offering Fraud (15.5%), and Manipulation (15.2%).[9] The 3,001 TCRs came from not only the United States (including all fifty states, the District of Columbia, and Puerto Rico), but forty-nine other countries as well.[10] With respect to domestic TCRs, of which there were 2,507, nearly 50% came from six states: California (17.4%), Florida (8.1%), New Jersey (4.1%), New York (9.8%), Texas (6.3%), and Washington (4.1%).[11] As for foreign TCRs, nearly 60% of the 324 came from Commonwealth countries,[12] with another 8.0% from the People's Republic of China.[13]

Educating employees on the SEC rules and the important fact that the employee may qualify as a whistleblower even after reporting the information through internal compliance channels are key.

Although only one award was paid out in fiscal year 2012, the SEC's Office of the Whistleblower posted 143 Notices of Covered Action—notices of enforcement judgments and orders that imposed monetary sanctions of $1 million or more.[14] According to the Report, the Office of the Whistleblower continues to review and process applications for whistleblower awards based on those notices received during fiscal year 2012.[15]

In response to the new whistleblower bounty program, potentially affected companies should undertake a critical review of internal policies, procedures, and training to determine whether changes should be made. Educating employees on the SEC rules and the important fact that the employee may qualify as a whistleblower even *after* reporting the information through internal compliance channels are key.

Compliance procedures must be clear and easy for employees to understand. Companies should implement an overall risk system that integrates compliance, legal, human resources, internal audit, and external audit to create a risk-

7 ANNUAL REPORT at 8.

8 Id. at 4.

9 Id. at 4–5.

10 Id. at 5. One hundred and seventy (170) TCRs received in Fiscal Year 2012, representing 5.7% of the total received, were submitted without any geographical information provided. Annual Report at Appendix B: Whistleblower Tips Received by Location – United States and its Territories – Fiscal Year 2012.

11 Id. at Appendix B: Whistleblower Tips Received by Location – United States and its Territories – Fiscal Year 2012.

12 While the relatively high percentage of TCRs from Commonwealth countries may suggest a common culture that encourages whistleblowing activity, the number probably reflects the more mundane fact that residents of those countries are more likely to speak English, the language in which Form TCR and the Commission website are written.

13 The relatively high percentage of TCRs from China may be due to the SEC's significant focus on issuers from China, and in particular Chinese reverse merger companies listed on U.S. exchanges. See, e.g., Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges N.Y.-Based Fund Manager and Others With Securities Laws Violations Related to Chinese Reverse Merger Company (July 30, 2012), available at http://www.sec.gov/news/press/2012/2012-146.htm; Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges China-Based Company and Others with Stock Manipulation (Apr. 11, 2012), available at http://www.sec.gov/news/press/2012/2012-59.htm; Press Release, U.S. Sec. & Exch. Comm'n, SEC Approves New Rules to Toughen Listing Standards for Reverse Merger Companies (Nov. 9, 2011), available at http://www.sec.gov/news/press/2011/2011-235.htm; Luis A. Aguilar, Comm'r, U.S. Sec. & Exch. Comm'n, Facilitating Real Capital Formation (Apr. 4, 2011), available at http://www.sec.gov/news/speech/2011/spch040411laa.htm; Scott Eden, "China Reverse Mergers Continue Wild Ride," THE STREET, June 23, 2011, http://www.thestreet.com/story/11083003/1/china-reverse-mergers-continue-wild-ride.html.

14 ANNUAL REPORT at 6, 8–9. Individuals have 90 days to apply for an award based on the posted notices of covered action.

15 Id. at 9.

based approach to preventing, detecting, and responding promptly to potential violations. As part of such a system, user-friendly internal reporting mechanisms are essential to encourage employees, agents, and others to bring any potential wrongdoing to the attention of the company. For example, companies should consider:

- **Hotlines.** Anonymous and confidential hotlines for employees, contractors, vendors, and customers to report potential securities law violations and other misconduct;
- **Audit.** An independent and robust internal audit function and an audit committee with active oversight and involvement in the audit function;
- **Prioritization.** Processes and procedures that ensure that internal complaints are prioritized and evaluated quickly, and thoroughly investigated based on risk factors. Results and trends from such complaints should be integrated into the company's assessment of its compliance risks and financial reporting controls;
- **Internal Reporting Requirements.** Internal rules that require employees to report any suspected wrongdoing to legal or compliance personnel; and
- **Training.** Training programs that credibly reiterate an institutional commitment to integrity and fair dealing, and that clearly set out internal complaint procedures.

Insider Trading

The SEC's Market Abuse unit in the Division of Enforcement likely will remain heavily focused on investigations and enforcement actions for insider trading.

In 2012, the SEC filed 58 insider trading actions with a focus on financial professionals, hedge fund managers, and corporate insiders. Some of these insider trading actions involved high-profile individuals such as the former global head of McKinsey and Co.

Companies and financial services firms must establish compliance policies and procedures to address insider trading and interactions with potential tippers, including outside consultants, agents, and expert networks.

The SEC's Enforcement Division remains focused on employees and agents (including lawyers and consultants) of public companies who trade on material, nonpublic information gained from their work relationship. Employees are prohibited by law from trading on material, nonpublic information gained from their employment. Similarly, agents and contractors may be liable for insider trading if they violate their confidentiality to the source of the information by trading on material, nonpublic information or providing it to someone else who trades. The SEC remains active in bringing cases where employees and agents illegally capitalize based on their relationship with a company.

In addition, the Department of Justice (DOJ) has increased efforts to prosecute inside trading as a crime. The DOJ possesses law enforcement tools such as the use of wiretaps, trap-and-trace devices, confidential informants, search warrants, and grand juries to gather information where the SEC is unable. Of course, the SEC ultimately may use much of this information following a criminal trial. With the presence of criminal prosecutors and federal agents, the stakes could not be higher for companies, financial services firms, and individuals.

Companies and financial services firms must establish compliance policies and procedures to address insider trading and interactions with potential tippers, including outside consultants, agents, and expert networks. Effective

policies and procedures should address, as applicable: (1) the prevention of selective release of information in violation of Regulation FD (Fair Disclosure); (2) protecting the release of material, nonpublic information, including the use of social networks; (3) the implementation of information barriers between the firm's public and private sides; (4) the interaction with expert networks and experts; (5) rules for trading by employees; and (5) the monitoring, surveillance, and supervision of employees with material, nonpublic information. All employees at the company should be trained thoroughly on the laws governing insider trading and the firm's policies and procedures. A culture should be created to encourage employees to report to compliance or legal personnel any unusual or problematic activity. Companies should document both the processes implemented and the steps personnel take in compliance with these processes, thereby creating a detailed record of the firm's efforts to meet its legal and regulatory obligations.

Foreign Corrupt Practice Act

The SEC, together with the DOJ, continues to be aggressive in pursuing violations of the Foreign Corrupt Practice Act. The DOJ and SEC settled several high profile FCPA matters, and according to news reports, initiated several new investigations.

During 2013, the DOJ and SEC are likely to be involved in more investigations stemming from the topple of governments. Threats common to foreign businesses caught in the midst of revolution include extortion, nationalization, expropriation, and physical violence against executives and employees.

During 2013, the DOJ and SEC are likely to be involved in more investigations stemming from the topple of governments. The recent wave of Arab Spring upheavals that continue to ripple across the southern and eastern shores of the Mediterranean may present the threats common to foreign businesses caught in the midst of revolution, including extortion, nationalization, expropriation, and physical violence against executives and employees. These modern revolutions also pose new challenges to international firms, as evidence or allegations that they engaged in corrupt behavior may be made public through documents in a ransacked government ministry building, or through an incarcerated former official, an enterprising journalist or prosecutor in the new regime, or a whistleblower within the foreign company itself. If such allegations come to the attention of U.S. authorities or other governments, the company could face severe criminal and civil penalties for violations of the Foreign Corrupt Practices Act, among other laws.

Corporate Accounting and Internal Controls

In the aftermath of the financial crisis, companies both in the United States and around the globe have struggled to meet investor expectations and remain competitive on the international stage. Faced with challenging financial conditions, companies have focused efforts on essential cost-cutting measures, while also exploring opportunities in emerging markets and developing new products and services for this decade and beyond. During challenging times, some employees may become tempted to cut corners and engage in fraud.

At the same time, regulators, faced with increased scrutiny for their apparent shortcomings prior to and during the financial crisis, have increased investigative and enforcement efforts to combat a perceived growth in corporate fraud. The SEC, in particular, will continue to focus on corporate accounting involving significant accounting judgment such as revenue recognition, capitalization of costs, valuation, and percentage-of-completion accounting.

For example, in 2012, the SEC charged a financial services firm and three of its senior executives for allegedly participating in an accounting scheme involving life settlements. According to the SEC, the company overstated the value of assets held on the company's books and created the appearance of a steady stream of earnings from brokering life settlement transactions.

The best global companies of today and the future must make corporate integrity and ethics the centerpiece of their culture—permeating every level of the organization, from the board and senior management down to entry level employees in foreign subsidiaries.

Against this backdrop, companies must remain focused on building and maintaining a strong fraud prevention and compliance program. The best global companies of today and the future must make corporate integrity and ethics the centerpiece of their culture—permeating every level of the organization, from the board and senior management down to entry level employees in foreign subsidiaries. Focus must be placed not only on compliance with the law, but compliance with the tenets of honesty, ethics, and the highest levels of integrity. Creating such a culture is not easy, but must become a reality for any organization that hopes to compete on the global stage.

A strong anti-fraud program is not only an essential business requirement in today's modern world, it is a crucial factor for regulators when determining sanctions after problems arise. The United States Department of Justice and the Securities and Exchange Commission have written policies that allow for leniency when sanctioning companies that have established and maintained robust compliance programs and internal controls.

Conclusion

This year likely will see an increase in enforcement actions by the SEC. The SEC enters 2013 with the nomination as agency Chairman of Mary Jo White, a former U.S. Attorney with a strong reputation in law enforcement. The SEC's Division of Enforcement also is likely to see the benefits of the whistleblower bounty program. The SEC is likely to bring fewer cases this upcoming year relating to the financial crisis and more cases in the area of insider trading, accounting misconduct, and investment management. With this in mind, legal and compliance personnel should be proactive in assessing compliance programs, internal controls, and anti-fraud programs to ensure that proper policies and procedures are in place.

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Michael Connor
ECA Expert Panelist

Michael Connor is a seasoned, award-winning media executive, entrepreneur and journalist with extensive experience in television, print and the Internet. Michael brings deep expertise to LRN and ECA partners in areas of Social Media management and risk, strategic communication planning, and business ethics. Michael has launched and managed numerous ventures on multiple media platforms in the U.S., Europe and Asia and is a recognized thought leader in the fields of business ethics, corporate responsibility and sustainability.

Social Media for 2013

From the Boardroom to the Factory Floor

"When you give everyone a voice and give people power," says Facebook founder and CEO Mark Zuckerberg, "the system usually ends up in a really good place."

The challenge for ethics and compliance professionals, of course, is how to help ensure that "the system" surrounding social media platforms like Facebook does indeed wind up in a "really good place" at their companies. While these new technologies present exciting new ways for marketers to reach customers, and for employees to communicate and collaborate with one another, when used improperly they can also present real threats to privacy, reputation, intellectual property, and data security.

According to a recent survey by McKinsey, more than 1.5 billion people around the globe now have an account at a social network site, and almost one in five online hours is spent on social networks—increasingly via mobile devices. By 2011, 72 percent of the companies McKinsey surveyed reported using social technologies in their business and 90 percent of those users reported that they are seeing benefits.

More than 1.5 billion people around the globe now have an account at a social network site, and almost one in five online hours is spent on social networks—increasingly via mobile devices.

In addition to a dramatic growth in popularity, social media are transforming the very nature of the Internet, from a medium dominated by static web sites to one featuring multiple levels of interaction on platforms like Facebook, Twitter, LinkedIn and YouTube. And as more people access the Internet via mobile devices, they're regularly using a plethora of applications ("apps") for everything from news and shopping to photography and games. By one estimate, some 98 billion apps will be downloaded by 2015; the current $6.8 billion market for apps is expected to grow to $25 billion within four years.

Keeping pace with these technologies from a compliance perspective requires attention at all levels of the enterprise, from the factory floor to the board room.

Status Update from the Board

At the senior management and director level, new research suggests, there is often a serious disconnect between executives' knowledge about social media and its use at their companies.

A 2012 survey of 180 senior executives and corporate directors of North American public and private companies found that while 90 percent of respondents claim to understand the impact that social media can have on their organization, only 32 percent of their companies monitor social media to detect risks to their business activities and 14 percent use metrics from social media to measure corporate performance.

The survey—conducted by Stanford University's Rock Center for Corporate Governance and The Conference Board—also found that only 24 percent of senior managers and 8 percent of directors surveyed receive reports containing summary information and metrics from social media. About half of the companies do not collect this information at all. The vast majority of respondents (90.7 percent) said their companies have not assigned oversight of social media monitoring to a board committee.

"Companies that fail to incorporate social media into their business operations miss out on its potential opportunities and also expose themselves to many fundamental risks," the report concluded. Among the risks: ignoring a source of public information from which to gain insight into how stakeholders (customers, employees, suppliers, shareholders, etc.) view a company; being caught off-guard in crisis situations; and inadequately controlling proprietary information.

Privacy may well be the leading operational risk regarding social media; as marketers collect more consumer data, there's need for vigilance regarding compliance with federal and state privacy laws.

Privacy Concerns

As companies increasingly turn to social media to market and promote, business units should have appropriate policies and operational guidelines in place. It's also critical to determine to what degree the company's social media projects utilize third-party consultants and agencies, all of whom need to comply with organizational policy.

Privacy may well be the leading operational risk regarding social media; as marketers collect more consumer data, there's need for vigilance regarding compliance with federal and state privacy laws.

In September, 2012, the U.S. Federal Trade Commission (FTC) published a nonbinding guide to inform mobile application developers on how to best comply with truth-in-advertising and basic privacy principles. The agency noted that once a business begins distributing a mobile application, "you become an advertiser," subject to laws and regulation for advertising. Among other recommendations, the FTC says businesses should build privacy considerations in from the start of their development process and collect sensitive information only with consent.

In October, 2012 California Attorney General Kamala D. Harris began formally notifying scores of mobile application developers and companies that they are not in compliance with the California Online Privacy Protection Act, which requires operators of online services that collect personally identifiable information from Californians to conspicuously post a privacy policy. In December, the attorney general filed suit against Delta Airlines seeking to enjoin Delta from distributing its app without a privacy policy. She also warned that companies face a fine of $2,500 for each download of an app not in compliance with state law.

Children's privacy is a particular concern, subject in the U.S. to the federal Children's Online Privacy Protection Act (COPPA) and the FTC's COPPA Rule. A group of 14 child advocacy organizations recently filed a complaint with the FTC charging that six major advertisers—including McDonald's and Time Warner's Cartoon Network—had violated children's online privacy laws by asking young visitors to share their experience with branded games with friends by providing their friends' email addresses. The FTC issued a staff report in December 2012 examining privacy disclosures and practices of apps

offered for children. “While we think most companies have the best intentions when it comes to protecting kids’ privacy, we haven’t seen any progress when it comes to making sure parents have the information they need to make informed choices about apps for their kids. In fact, our study shows that kids’ apps siphon an alarming amount of information from mobile devices without disclosing this fact to parents,” said FTC Chairman Jon Leibowitz. “All of the companies in the mobile app space, especially the gatekeepers of the app stores, need to do a better job. We’ll do another survey in the future and we will expect to see improvement.”

In Europe, proposed revisions to the European Union’s General Data Protection regulation include a proposal that would give consumers the ability to choose what information an app can store on them without losing the ability to use the software.

Employee Online Behavior

Social media empower users to become their own publishers—typically using Facebook, Twitter, or LinkedIn to update the world on their status and opinions, often accompanied by photos or video. Unfortunately, not all employees (including senior executives) are experienced communicators, sometimes resulting in posts that are defamatory to other employees or the company, damaging to the company’s reputation, or revealing proprietary or potentially material information.

Not all employees (including senior executives) are experienced communicators, sometimes resulting in posts that are defamatory to other employees or the company, damaging to the company’s reputation, or revealing proprietary or potentially material information.

Case in point: In July, 2012 Netflix CEO Reed Hastings boasted in a Facebook post that more than one billion hours of Netflix programming had been viewed in June. In December, the Securities and Exchange Commission sent Netflix a “Wells notice” saying the agency may file civil claims against the company and Mr. Hastings for violating the Regulation Fair Disclosure (Reg FD) rule. Mr. Hastings says the information he initially disclosed was not material to the company, adding in a subsequent Facebook post: “Fascinating social media story.”

Some companies block workplace access to all or some social media outlets, though blocking is proving less popular, if only because so many employees can access networks on their personal mobile devices. Fewer than 30 percent of large organizations will block employee access to social media sites by 2014, compared with 50 percent in 2010, according to the tech consulting firm Gartner.

An effective social media policy should be simple, consistent, and tightly-aligned with a company’s Code of Conduct; whatever the company code for in-person encounters, and whatever the rules for general good behavior, they apply in the online world as well. Potential penalties for violations, including dismissal, should be made clear.

Developing an effective policy can prove challenging. In the U.S., the National Labor Relations Board (NLRB) has focused considerable energy on social media issues, with a series of rulings emphasizing that corporate guidelines must not violate Section 7 of the National Labor Relations Act (NLRA) by disciplining or firing an employee because the employee was using social media to engage in “protected concerted activity,” which occurs when two or more employees act together to protest or complain about wages, benefits, or other terms and conditions of employment.

In September, 2012, the NLRB issued its first formal decision on an employer's social media policy. It rejected the social media policy developed by retail giant Costco as overly broad and likely to have a "chilling effect" on employees' rights under the NLRA. The ruling (Costco Wholesale Corporation and UFCW Local 371) indicates that the NLRB is following the lead of its general counsel who in June had issued three public memos explaining how social media policies can interfere with employees' rights to organize. The general counsel held that a number of corporate social media policies—including those of General Motors and Target Brands—were overly broad and violated federal law.

However, the NLRB's general counsel also endorsed the social media policy of another retail giant—Wal-Mart—and found it entirely lawful, to the extent that in his decision he reproduced the policy in full. Wal-Mart's policy, he said, "provides sufficient examples of plainly egregious conduct so that employees would not reasonably construe the rule to prohibit Section 7 conduct." On its web site, Wal-Mart also features guidelines directed to consumers for social media engagement.

It's absolutely critical that organizations have a social media policy for employees at all levels. The challenge lies in determining what goes into a good policy. And while there are many similarities in the way that different countries and jurisdictions approach these issues, there are also some key differences, so considering the local rules in each case is essential.

Co-branded Employees?

Who owns a social media account that an employee sets up for the purpose of promoting his employer's business? That's an increasingly common, and occasionally litigious, question. *The Wall Street Journal* reports that more and more "co-branded" employees are using social media to build a personal, public identity—a brand of their own—based on their work. But when the rules about ownership aren't clear, problems can develop.

Who owns a social media account that an employee sets up for the purpose of promoting his employer's business? That's an increasingly common, and occasionally litigious, question.

In *Eagle* v. *Morgan*, a federal district court for the Eastern District of Pennsylvania addressed the issue of ownership of employer social media accounts by dismissing the complaint of an executive who had launched a LinkedIn account, under her own name, which promoted the company. When her company was purchased by another and her employment terminated, she discovered that her LinkedIn password and account profile had been changed.

In December, 2012 a settlement was reached in a highly-publicized case where the mobile phone site PhoneDog sued former employee Noah Kravitz when he left the company, alleging that he took as many as 17,000 of its Twitter followers with him. Terms of the settlement were not disclosed. In announcing it, Kravitz said: "If anything good has come of this, I hope it's that other employees and employers out there can recognize the importance of social media to companies and individuals both. Good contracts and specific work agreements are important, and the responsibility for constructing them lies with both parties. Work it out ahead of time so you can focus on doing good work together—that's the most important thing."

A number of similar lawsuits regarding ownership of social media accounts are reportedly working their way through the U.S. courts.

Looking Ahead

Social media networks are likely here to stay—in fact, the process of exchanging information and collaborating on a frequent basis has become so popular that many companies are deploying enterprise social software which adapts Facebook-like and Twitter-like features for workplace use, including employee profiles, activity streams, micro-blogging, discussion forums, wikis, content tagging, rating, and reviewing.

By one estimate, the demand for enterprise social software is growing at an annual compound rate of 61 percent, growing from a market of $600 million in 2010 to an estimated $6.4 billion by 2016.

By one estimate, the demand for enterprise social software is growing at an annual compound rate of 61 percent, growing from a market of $600 million in 2010 to an estimated $6.4 billion by 2016. Market leading firms include IBM, Jive, Communispace, Telligent, Socialtext, Mzinga, Lithium, and Yammer.

These internal social networks are in their early stages, however, and anecdotal evidence suggests that they require considerable attention if they're to be successful. Depending on its culture, an organization needs to ensure that management and employees are ready for the switch. Is participation optional or mandated? Is the IT department ready and prepared to integrate internal social applications with existing software? Can intellectual property be protected? What's the return-on-investment? And what are the compliance risks?

Founders of tech start-ups often like to refer to their new ventures as "disruptive" technologies, capable of transforming traditional social and business models. While not all current social media technologies will survive and prosper, it's clear that this new phase of communications is really in its earliest stages. For organizations large and small, the social media compliance challenge—as Facebook's Mark Zuckerberg has put it—is how to "give people power" while making sure the "system" thrives and prospers.

CLICK HERE
TO RETURN TO
TABLE OF CONTENTS

Marian Ladner
E&C Expert Panelist

Marian Ladner is the Managing Partner of the law firm of Ladner & Associates PC. She primarily centers her practice on Regulatory Compliance with import, export and FCPA requirements.

Among other key areas of support, Marian helps companies create and streamline strategic sourcing and supply-chain operations, with an emphasis towards minimizing duties through participation in government preference programs, such as NAFTA, FTZs, CBI, GSP, and AGOA. Her practice also specializes in assisting multinational companies build, test, and sustain global import, export and FCPA compliance programs.

Throughout her career, Marian has provided legal interpretations and advice nationwide to leading members of the trade community, including multinational importers and exporters, customs brokers, freight forwarders, shippers, and to Customs employees, such as auditors, import specialists, Fines, Penalties, and Forfeitures Officers; agents; and inspectors.

Key challenges in the trade compliance focus area in 2013 will center on changes resulting from the Export Control Reform Initiative and ongoing changes to US sanctions and embargo programs in response to geopolitical developments.

Trade Compliance for 2013

Current Issues, Risks and Challenges in Export Controls

Key challenges in the trade compliance focus area in 2013 will center on changes resulting from the Export Control Reform Initiative and ongoing changes to U.S. sanctions and embargo programs in response to geopolitical developments. The key areas addressed in this article that organizations should be aware of for the coming year and beyond include:

- Increased compliance responsibility on companies resulting from the movement of goods and technology from State Department to Commerce Department export jurisdiction
- Enhanced trade sanctions against Iran and the increased liability of U.S. companies for the activities of their foreign subsidiaries
- Alignment of export compliance programs with U.S. Government enforcement priorities

Export Control Reform Initiative

The Obama Administration's efforts to reform the U.S. export control system remain the dominant theme in the export trade compliance field. More than three years after it was announced, the Export Control Reform (ECR) Initiative continues its slow but steady progress. In 2011, the new License Exception Strategic Trade Authorization (STA) was introduced. It was designed to authorize certain exports of items moved from the U.S. Munitions List (USML) under the International Traffic in Arms Regulations (ITAR) to the Commerce Control List (CCL) under the Export Administration Regulations (EAR). Efforts during 2012 focused on the continued review of the USML to identify items that are candidates for transfer from the rather onerous USML to the EAR. The Bureau of Industry and Security (BIS) at the Commerce Department, which is responsible for administration of dual-use exports under the EAR, and the Directorate of Defense Trade Controls (DDTC) at the State Department, which is responsible for exports of defense articles under the ITAR, are working in close cooperation to conduct the review of the USML under the ECR Initiative.

BIS and DDTC have published coordinated proposed rules covering nine of the USML categories. The proposed rules identify items that the Administration believes should be transferred from ITAR jurisdiction to EAR jurisdiction. None of those rules has advanced beyond the proposed stage, but with the President's reelection, it is expected that all will now proceed to the final rule stage, and that export jurisdiction over many items will, in fact, be transferred from State to Commerce.

For exporters whose products are transferred from State to Commerce jurisdiction, the change will mean much more flexibility in getting those products from the U.S. to their customers abroad. However, the change also shifts a greater compliance burden onto the exporter. Most exports under the ITAR require a license from DDTC, meaning the government takes responsibility for vetting transactions and parties to the transactions. In contrast, the EAR provide a variety of export modalities, including exports with "no license required," exports under License Exceptions, and exports under validated licenses. Exporters of dual-use items under the EAR are able to self-determine the classification of their products and the appropriate export authorization required. Companies whose products are transferred from State to Commerce jurisdiction will need to ensure they have sufficient and properly trained compliance resources in place to manage the higher degree of export self-determination available under the EAR.

For exporters whose products are transferred from State to Commerce jurisdiction, the change will mean much more flexibility in getting those products from the U.S. to their customers abroad. However, the change also shifts a greater compliance burden onto the exporter.

Another important compliance issue addressed by the ECR Initiative is the definition of the term "specially designed." That term is used extensively in the EAR, but with the exception of a limited universe of items subject to control under the Missile Technology Control Regime (MTCR), the term is not defined by the regulations. In a criminal enforcement case that began in the late 1990s and ran through the late 2000s, the Government put forth a definition of "specially designed" that was at odds with the general understanding of the term that industry believed the Government had been using for decades. The result was a high level of uncertainty over the compliance risk companies were carrying with respect to the export of "specially designed" items. In 2012, BIS and DDTC published coordinated proposed rules that implement a definition for the term "specially designed" that would apply not only to the EAR but also the ITAR. While many companies and industry groups have submitted comments suggesting modifications to the proposed definition, the fact that any definition will be available is a step toward greater certainty on the application of export controls and the concomitant diminution of compliance risk.

While the Obama Administration has made no official announcement of expected dates of publication for final rules on the transfer of items from the USML to the EAR, or for the establishment of the "specially designed" definition, all indications are that those rules should begin to emerge near the end of 2012 or early 2013. Additional significant aspects of the ECR Initiative, including establishment of a single control list, a single export control agency, and a single export enforcement agency, will require Congressional action. Prospects for such Congressional action remain uncertain at best.

OFAC Embargo and Sanctions Programs

The Office of Foreign Assets Control (OFAC) at the Treasury Department is responsible for administering a variety of economic and trade sanctions programs. Those programs are intended to impose restrictions on trade by U.S. persons with countries, organizations or individuals that the U.S. Government has determined pose foreign policy or national security concerns.

During 2012, sanctions against Iran were substantially strengthened by OFAC pursuant to a mandate under the Iran Threat Reduction and Syria Humans Rights Act of 2012 (ITRSHRA). Significantly, the ITRSHRA provides that liability will attach to U.S. firms for the actions of their foreign subsidiaries where those

actions would be subject to sanctions if performed by a U.S. person. As far as U.S. companies with foreign subsidiaries are concerned, this effectively changes the definition of "U.S. person" to include foreign subsidiaries for purposes of enforcement of the Iran sanctions. The U.S. embargo on Cuba is the only other OFAC sanctions program that uses a similar definition of the term "U.S. person" such that the actions of foreign subsidiaries are subject to U.S. penalties.

The ITRSHRA also provides that foreign firms and their officers and principals may be subject to U.S. sanctions for involvement in services, insurance and reinsurance services, and shipping related to the energy sector in Iran. Sanctions that were already in place under existing Iran sanctions included:

- A prohibition on receiving Export-Import Bank credits
- A prohibition on receiving licenses under various export control regimes
- A prohibition on receipt of large loans from U.S. financial institutions
- For financial institutions, restrictions on their ability to deal in U.S. government bonds and to serve as a repository for government funds
- A prohibition on government procurement from the violating entity
- A prohibition on "transactions in foreign exchange that are subject to the jurisdiction of the United States and in which the sanctioned person has any interest"
- A prohibition on transfers of credit or payments that involve "any interest of the sanctioned person" through U.S. financial institutions
- A prohibition on any person from participating in any property transaction "with respect to which the sanctioned person has any interest"
- Additional sanctions to restrict imports from the sanctioned party, in accordance with the International Emergency Economic Powers Act

It is important to remember that OFAC currently maintains nearly total embargoes on trade with Cuba, Iran, and Sudan.

Additional sanctions within the ITRSHRA are:

- A prohibition on U.S. persons investing in or purchasing significant amounts of equity or debt instruments of a sanctioned person
- A prohibition on visas for entry into the U.S. by corporate officers or principals of, or shareholders with a controlling interest in, a sanctioned entity
- Imposition of available sanctions on the principal executive officers of any sanctioned person, or on persons performing similar functions and with similar authority

Another significant development in 2012, was OFAC's relaxation of sanctions against Burma/Myanmar. While the Burmese Sanctions Regulations remain in place, OFAC issued general licenses that permit U.S. persons to engage in most export and import transactions with Burma/Myanmar. Restrictions remain in place on transactions involving jadeite or rubies mined in Burma/Myanmar, as well as on transactions with persons whose property has been blocked by OFAC. Such persons are identified on the Specially Designated Nationals List maintained by OFAC.

It is important to remember that OFAC currently maintains nearly total embargoes on trade with Cuba, Iran, and Sudan. Changes have been made to the Cuban embargo in recent years, including implementation of licensing policy changes in 2011 intended to promote people-to-people contact, to support civil society, and to help the free flow of information in Cuba. Those

policy changes allowed for increased licensing of travel for educational, cultural, religious, and journalistic purposes. They also permitted expanded licensing of remittances by U.S. persons to individuals in Cuba. Despite these modest steps to relax the U.S. embargo on Cuba, that embargo remains comprehensive with only very limited opportunities for the licensing of trade in agricultural products and medicine.

OFAC maintains less comprehensive, targeted sanctions on Belarus, Burma, Democratic Republic of the Congo, Iraq, Ivory Coast (Cote d'Ivoire), Lebanon, Libya, North Korea, Somalia, Syria, Yemen and Zimbabwe. Sanctions are also stabilization efforts in the Balkans, narcotics trafficking, terrorism, undermining Lebanese sovereignty or democratic processes or institutions in Lebanon, the former Liberian regime of Charles Taylor, proliferation of weapons of mass destruction, trade in rough diamonds, and transnational criminal organizations.

OFAC maintains less comprehensive, targeted sanctions on Belarus, Burma, Democratic Republic of the Congo, Iraq, Ivory Coast (Cote d'Ivoire), Lebanon, Libya, North Korea, Somalia, Syria, Yemen and Zimbabwe.

Export Enforcement Priorities

For several years the Office of Export Enforcement (OEE) at the Commerce Department has focused on three primary areas of concern with respect to export compliance violations:

1. Weapons of mass destruction
2. Terrorism
3. Unauthorized military use

Exporters should use these priorities to assist them in focusing their internal compliance resources on areas presenting higher levels of risk of export control violations. While the Government does not expect every commercial company to become expert in chemical/biological/nuclear weapons, terrorism, or foreign military activities, companies must understand if and how their products might be used in any of those activities. Appropriate screening and due diligence procedures need to be in place to review proposed transactions and business partners, to ensure there are no apparent risks of diversion of products to such prohibited activities or parties. While there is no guarantee that products will escape diversion to proscribed activities, despite appropriate screening and due diligence efforts performed by the seller/exporter, the implementation and use of thorough due diligence over the transaction will help reduce risk and provide important mitigation of any potential penalties should such a diversion occur.

Vigilance in a Changing Regulatory Environment

One constant in the export compliance field for many years, but certainly over the past several years, is change. The focus of U.S. export controls 25 years ago was the Soviet Bloc and China. The result was a relatively static regulatory framework of licensing and enforcement priorities. Over the past 15 to 18 years the focus for controls has changed from one that is country-based to one that is more concerned with individual bad actors. A focus on non-state bad actors coupled with a dual-use export control system demands a high degree of self-regulation by exporters. The resulting challenge for U.S. exporters is maintaining knowledge of the rapidly changing collection of export controls, while at the same time building enough flexibility into their compliance programs and processes to ensure maximum reaction time for vetting business opportunities that allow you to remain competitive in the global marketplace.

CLICK HERE TO RETURN TO TABLE OF CONTENTS

About LRN: Inspiring Principled Performance

Since 1994, LRN has helped over 20 million people at more than 700 companies worldwide simultaneously navigate complex legal and regulatory environments and foster ethical cultures. LRN's combination of practical tools, education, and strategic advice helps companies translate their values into concrete corporate practices and leadership behaviors that create sustainable competitive advantage. In partnership with LRN, companies need not choose between living principles and maximizing profits, or between enhancing reputation and growing revenue: all are a product of principled performance. LRN works with organizations in more than 100 countries and has offices in Los Angeles, New York, London, and Mumbai.

For more information, visit www.LRN.com**,** join our community on Facebook at facebook.com/howistheanswer**,** or call: **800 529 6366** or **646 862 2040.**

The **LRN Ethics & Compliance Alliance (ECA)** is a leading online solution that provides cutting-edge resources, tools, and practical content across all major ethics and compliance risk areas, including access to leading subject-matter experts for one-on-one collaboration and support. For more information on this valuable solution, please reach out to our LRN ECA Leadership Team at ECA_Management@lrn.com or visit us at www.LRN.com/ethics-compliance-alliance.

LRN® *Inspiring Principled Performance*℠

©Copyright LRN Corporation. All rights reserved. L1044-0113-01-NY