Tuesday, October 21
11:00 am-12:30 pm

510 A Practical Approach to Compliance Challenges in the International Arena

Steven Lauer
Corporate Counsel
Global Compliance

Gail Lilley
Partner
Blake Cassels & Graydon LLP

Martin Mueller
Chief Compliance Counsel
Nexen, Inc.

Evan Slavitt
Vice President, Business and Legal Affairs
AVX Corporation

Faculty Biographies

Steven A. Lauer

Steven A. Lauer is corporate counsel for Global Compliance Services in Charlotte, NC.

Prior to joining Global Compliance Services, Mr. Lauer was general counsel for Prudential Insurance Company. During that time, he held increasing responsibility for the management of legal affairs for the company's commercial real estate investment units. Mr. Lauer was also project director for the Prudential law department's outside counsel utilization task force, where he designed and managed the preparation and distribution of 109 distinct work packages by which Prudential restructured its purchase of legal services.

Mr. Lauer is a faculty member of the Law Partnering Institute, a member of Law Partnering Advocates, and the vice chair for programs of the corporate counsel committee of the American Bar Association Section of Business Law. Additionally, Mr. Lauer is vice chair of the corporate compliance committee of the Section of Business Law, as well as a member of the ACC Compliance and Ethics Committee. Mr. Lauer also co-founded and co-chairs the Open Legal Standards Initiative. He has authored numerous articles on compliance, the relations between in-house and outside attorneys, the selection of counsel by corporate clients, the evaluation of legal service, litigation management and other topics relevant to corporate compliance programs, and corporate legal service.

Mr. Lauer received a BA from the State University of New York at Buffalo and is a graduate of Georgetown University Law Center.

Gail D. Lilley

Gail D. Lilley is a partner with Blake Cassels & Gradon LLP in Toronto. Ms. Lilley's practice involves a wide range of corporate commercial transactions, with a principle focus on mergers and acquisitions of business for both Canadian and multi-national clients. She has particular expertise in the Canadian aspects of global acquisition transactions, including the cross border structuring and financing of those acquisitions.

Ms. Lilley has also advised clients on corporate reorganizations, private financings and equity issues, and other more general commercial relationships and arrangements. In addition, she has given advice to a large Canadian pension fund on private equity investments, both in Canada and other jurisdictions.

Ms. Lilley received a BS from Queen's College and is a graduate of the University of Western Ontario.

Martin Mueller

Martin Mueller is chief compliance counsel for Nexen, Inc. in Alberta, Canada. Prior to assuming his current role, Mr. Mueller served as vice president, international business development, and general counsel, chemical division, for Nexen.

Before joining Nexen, Mr. Mueller practiced corporate and commercial law in Düsseldorf, Germany and in Toronto, Ontario. The focus of his practice was international corporate and commercial law representing European companies in their North American business activities. He has been a director for many of these European companies on their North American boards.

Mr. Mueller received a BA and LLB from the University of New Brunswick, Fredericton.

Evan Slavitt

Evan Slavitt is the vice president of business and legal affairs for AVX Corporation, a NYSE-listed global manufacturer of electronic components and connectors, in Charleston, SC. In that capacity, he is the general counsel and chief legal officer for the company and its subsidiaries.

Mr. Slavitt began his legal career in the US Department of Justice, first in the antitrust division and then as an assistant US attorney for the District of Massachusetts. In private practice, Mr. Slavitt worked in several large partnerships before becoming a founding member of Bodoff & Slavitt, LLP. In private practice, Mr. Slavitt concentrated on complex commercial litigation, white-collar criminal defense, and corporate investigation. Mr. Slavitt was also the general counsel for the Massachusetts Republican Party and its 2004 candidate for attorney general.

Mr. Slavitt has been an active member of a variety of bar associations, including helping to establish and acting as the first co-chair of the bankruptcy litigation committee for the American Bankruptcy Institute, chair of the environmental crimes committee of the ABA's section on environmental law, and participated in the educational committees of the Boston Bar Association and the Massachusetts Continuing Legal Education Foundation. He is a frequent lecturer on legal topics and has written or co-authored numerous articles and books. Currently, Mr. Slavitt chairs the Publications Committee for ACC's Compliance and Ethics Committee.

Mr. Slavitt has a BA and MA from Yale University and a JD from Harvard Law School where he was an editor of the Harvard Law Review.

Moving from Rules to Culture

- Standard Model
  - Focus is on specific rules
  - Punishment based
  - Value derives from protection of company from enforcement
  - Stance toward employees is suspicion

Advantages of Rule Based Ethics

- Less affected by local norms
- Clarity in applicable situations
- Conceptually easier to implement
- Consistent with US corporate governance framework

Disadvantages of Rule-Based Ethics

- Detail is hard to master
- Requires significant training
- Discourages asking questions
- Hard to extend to unforeseen circumstances
- Needs continual revision
- Lacks collegiality/six sigma

Considerations in Moving from Rule to Value Based Ethics

- Resources
- Buy-in of senior management
- Commitment of legal/compliance function
- Tolerance for change
- Perceived need

Resources

- Standard needs
  - Personnel
  - Money
  - Time
- Proponents must be realistic
- Must be able to justify priority

Commitment of Proponents

- Implementation will take time
- Requires willingness to deal with conflict
- Must be comfortable with uncertainty
- Priority must be realistic
- Recognition of setbacks/intrusion of real world

Buy-In from Senior Management

- Intellectual
- Cultural
- Long-term
- Must extend to second & third levels
- Dangers
  - Nominal v. Real
  - Conceptual v. Realistic

Tolerance for Change

- Something of leap of faith
- Cannot be totally inconsistent with rest of company culture
- Tolerance must be evaluated
  - At corporate level
  - At facility level
  - At department level

Perceived Need

- Can't be evanescent/incident based
- Disadvantages must be truly understood
- Cannot be imposed

Key components

- Roll out strategy
- Endorsement by board/CEO
- Training
- Support materials
- Guidance procedures
- Updates/newsletters/wiki

Strategies

- Topical
- By region/subsidiary
- Cold Turkey

Personal Observations

- Gaining commitment is hard
- Getting resources is even harder
- Experiences of other companies helpful but not decisive
- History of company is more important than first thought
  - Culture
  - Success

Personal Observations -- II

- Not just improvement – paradigm change
- Outside counsel not helpful
- Relationship to other management priorities helpful – six sigma
- Still optimistic – but recognize long term
- Trying to work in new areas – SA8000

Nexen – Who We Are

- Canadian based energy corporation
  - Head office located in Calgary - Canada
- 2007 operating and financial results:
  - Production (before royalties) - 254,000 boe/d
  - Cash Flow - $3.5B
  - Capital Expenditures - $3.4B
- ~ 4300+ employees and contractors world-wide
- Inter-listed on the TSX and NYSE
  - Governed by OSC & SEC regulations
- Operations/representation in 9+ countries

Closing Point

- As a matter of personal inclination prefer rule based, but also recognize drawbacks
- Only time will tell

Nexen – Who We Are

- Our mission is to grow value responsibly
- Driven by maximizing shareholder value
  - Won't pursue profit at any cost
- Believe that sustainability begins with:
  - Ethical and transparent business practices
  - Maximizing social & economic benefits
  - Minimizing our environmental footprint
  - Solid returns to shareholders

Nexen – Who We Are

- To sum it up integrity at Nexen, is to live your values. I think we all share positive values and at the end of the day we try to make the right choices for the right reasons. And I think its just that simple.

  Charlie Fischer CEO Nexen

- Employees are subject to the laws, rules and regulations of the countries in which the business is being conducted. Where differences exist between local customs, laws, rules or regulations, the Employee must apply the highest ethical standard.

  Nexen Ethics Policy

- Maintaining Nexen's reputation for integrity is critical to our success in the global marketplace and is not, under any circumstances, to be sacrificed for the sake of short-term results.

  Nexen Statement of Values

Our Culture of Integrity

- Integrity Program introduced in late 1990's
  - Strong Tone at the Top (Board & Management)
  - Values based rather than simply following a set of rules – establish the corporate culture
  - Nexen was one of the contributing members of the International Code of Ethics for Canadian Business
  - Program updated in 2005 to meet changing regulatory prescriptive requirements
  - More accountability to Board of Directors
  - Increased focus on the ethical climate
  - Transparency / Accountability / Disclosure
  - Continuous learning / no one right way

Prescriptive versus Culture

- Nexen's mission is to grow value ***responsibly***
- We can choose how we pursue this mission
  - Prescriptive-based perspective (check the box)
  - Values-based perspective (emphasis on culture)
- We are continually trying to ensure that we have a **culture-focused** approach to integrity and ethical business conduct supported by sound policies, procedures and risked based training.
- Show the value.
- Integration of values based approach with prescriptive elements

Our Culture of Integrity

- Company policies
  - International Code of Ethics
  - Ethics Policy (annual review by Board)
  - Integrity-related policies
- Integrity Resource Centre (IRC)
  - Integrity Leaders world-wide
  - Compliance Committee with high level participation
  - Alliance with Audit/Legal/HR/Security
- Integrity education and awareness
  - Mandatory Integrity Workshop (In-person)
  - Anti-corruption Workshops (In-person)
  - On-line ethics training (targeted teams)
  - Video / Intranet articles / Lunch n Learns

Our Culture of Integrity

- Annual statement of compliance
- Case management
  - Case Management Reporting / Investigation
  - Case Management Tracking System
- Board and management reporting/engagement
  - Quarterly Compliance Update
  - Real time senior management involvement
  - Established Chief Compliance Counsel role

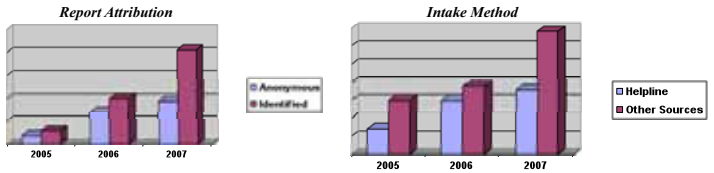
Our Culture of Integrity

Over the last 3 years we have seen an increase in reported incidents. We have also seen a shift from a predominance of employee relations issues to ones relating to security, and legal and regulatory compliance. We view this change in incident reporting as a positive development, reflecting a culture where employees are confident raising integrity-related concerns.

Our Culture of Integrity

- Is it working ? We are continually working at getting effective metrics.
  - Reporting statistics.
  - Annual Employee Survey.
  - Annual Statement of Compliance.
  - People Strategy Principles and Values
  - Internal and Third Party audits and reviews.
  - Outside recognition.

Our Culture of Integrity



In most instances, integrity concerns can be raised directly with a supervisor or Integrity Leader. Dialogue is preferred and we encourage direct dialogue with management as the first avenue of approach.

Our Culture of Integrity

Annual Employee Survey asks employees about:

- If they would feel comfortable in raising concerns if asked to do something illegal, unethical, inappropriate, or against personal beliefs
- If they know where to take my concerns if asked to do something illegal, unethical, inappropriate, or against personal beliefs
- If co-workers display integrity and ethical conduct at all times
- If their manager displays integrity and ethical conduct at all times
- If Senior Leadership displays integrity and ethical conduct at all times

Our Culture of Integrity

NEXEN: PRINCIPLES

IN ALL OUR BUSINESS OPERATIONS, NEXEN IS COMMITTED TO THE FOLLOWING PRINCIPLES.

- Employees of Nexen and its subsidiaries will:
- Obey the law;
- Act with honesty in all their interactions with fellow employees as well as people with whom they conduct business outside the company;
- Sustain, through leadership at all levels, a culture where ethical conduct is recognized, valued and exemplified by all employees;
- Acknowledge and accept personal accountability for the ethical quality of their decisions;
- Behave with personal integrity and do not sacrifice principles for personal gain;
- • • • • •

In Summary – What it takes

- Time and more time
- Commitment
- Management support at all levels
- Responsibility and Consequences
- Performance Evaluation – Reward the Values
- Transparency
- Reinforcement of the Values - Continuously
- Walk the Talk - Employees need to see your culture in action
- Show the value

Multi-jursidictional operations

- Challenges – can be either operational or substantive (or both)
- Solutions vary and must be tailored to the situation
- You need top-down policies but bottom-up implementation

Some challenges you can encounter

- Multiple cultures within an organization
- Geographic dispersion of personnel
- Insufficient enterprise-wide communication
- Some terms and concepts don't translate easily, especially in the area of ethics
- Differing legal requirements
- Difficult-to-learn-about developments (official websites are late in posting)

Some tools to overcome challenges

- Web-based delivery of code of conduct and other material
- Global hotline(s) for concerns, questions and reports of possible policy violations
- Corporate intranets for posting material
- Internal employee groups (*e.g.*, local ethics officers in an enterprise-wide group)
- Third-party vendors with varied client base

More tools to consider

- Well-designed awareness campaigns
- Internal newsletters, FAQs, etc.
- Formal training programs on ethics and compliance topics (fundamental and at-risk courses)
- Comprehensive compliance programs (see Sentencing Guidelines and other standards)

Beware of possible local roadblocks

- Local-language requirements
- Implementation requirements (*e.g.*, may have to be disseminated over signature of in-country manager)
- Required notification to and possible approval by government agencies (*e.g.*, hotline)
- Other parties' roles (*e.g.*, works councils)

Suggestions

- Involve local experts (internal or external)
- Design flexibility into your program
- Be sensitive to local attitudes (hotlines)
- Look for both official and unofficial sources of information
- Join relevant associations (*e.g.*, ACC Europe, SCCE, ECOA, ICC, etc.)

Hotlines and data protection

- Scope of permissible allegations varies among EU member states
- Anonymity allowed in most member states, but can't be encouraged (be aware of Spain)
- Some agencies must be notified; some must approve prior to implementation
- Data-transfer issues
- Cultural resistance

More suggestions

- Network with others in companies, law firms, etc.
- Electronic newsletters
- Attend conferences
- Some official websites allow registration for e-mail updates
- Use the Internet

ACC Association of Corporate Counsel

Data protection and discovery

- Personal information is protected in many countries regardless of the context
- U.S.-originated discovery can require production of personal information (*e.g.*, names, e-mail addresses, titles, etc.)
- Data subjects have rights to deny collection or processing, to correct incorrect data, etc.
- How to reconcile data protection and production

ACC Association of Corporate Counsel

Official concern over U.S. discovery

CNIL statement:

"Requests to communicate information have raised problems regarding the application of French rules pertaining to international legal assistance. They also violate the "Information Technology and Liberties" law related to information and to the consent of persons, to the proportionality of the processing and transfer of data outside of the European Union."

the GLOBAL COMPLIANCE LANDSCAPE:

A Resource File

If you're the chief compliance officer, you know how important it is to keep the company's ethics and compliance program current with the law, including the recent changes in the United States Sentencing Guidelines for Organizational Defendants (the "Guidelines"). But if your company is a multinational, it isn't enough just to keep up with US law—you also need to know how developments in other countries affect your compliance program.

And international compliance is a big issue. Compliance is difficult enough when a company operates in just one country. Keeping up with the myriad of laws, regulations, and industry-specific standards is a significant ongoing burden, as is keeping your employees up-to-date about changes in your firm's compliance policies. But the difficulties become much greater when a company does business in multiple countries. For instance, acts that might violate the laws of one country might be accepted or even preferred behavior in another.

In this article, we examine some of the challenges facing multinational firms in developing and implementing global ethics and compliance policies and offer you resource files on the following topics:

- Developments around the world affecting corporate compliance and ethics programs in certain (but by no means all) countries of particular current interest to global compliance officers. (See "Mapping Global Compliance Developments," on p. 44.)
- Two hot topics: efforts to eliminate corruption in business dealings and the use of hotlines to enable whistleblowers to report questionable business activities. (See "International Anticorruption" on p. 42 and "Whistleblower Hotlines" on p. 36)
- Creating an effective global compliance program that supports your company's business goals. (See "Tips for Global Compliance Programs," on p. 40.)

The business case for compliance is a strong one. Even given the complexities it involves, global compliance is good business. It will keep your company out of hot water—and more than that, it can provide your company with a competitive advantage in the market.

By Alan Greenwood and Steven Lauer

THE FORCES DRIVING GLOBAL COMPLIANCE STANDARDS

Until recently, the US government followed a laissez-faire approach to business, and the EU countries similarly trusted companies to act responsibly. Recent events, however, have exposed the vulnerabilities of these approaches. In the United States, scandals at Enron, WorldCom, Adelphia, and other corporations over the past five years have proved to many that business does not deserve unquestioning trust. More recent corporate scandals involving European companies, such as Parmalat, Ahold, Royal Dutch Shell, and Adecco, have increased pressures on regulators in the EU countries to be more active in monitoring and regulating corporate conduct.

In parallel with this growing international concern over corporate behavior, the integration of global capital markets has fueled a growing international consensus that companies need well-defined governance practices. Every country with a stock market—including China, Mexico, and Zimbabwe—has adopted corporate governance codes in which codes of ethics and/or compliance programs for the board and members of the organization are either explicitly mandated or strongly recommended as a central component of good governance. Supranational entities such as the OECD (Organization for Economic Co-operation and Development) and OAS (Organization of American States), together with a variety of nongovernmental organizations (NGOs), including Transparency International and the Fair Labor Association, monitor the activities of governments and private business and highlight failures to adhere to governance and compliance standards. (See "Look Who's Watching You Now," on this page.)

The internationalization of compliance standards has also been fueled by recent globalization. If a company is subject to the compliance rules of a government or supragovernmental organization, the company is usually expected to satisfy these standards in all of its locations throughout the world. Business leaders have generally supported these trends because they tend to promote similar standards and values and thus avoid confusion about what behavior is expected of employees no matter where they are working.

US government agencies have played a key role in this internationalization of standards. The Guidelines, promulgated by the United States Sentencing Commission in 1991 and modified greatly in 2004, have served as one of the primary catalysts for the development and increasing maturity of corporate ethics and compliance programs. Because the Guidelines apply to organizations based in the United States and so many of the world's largest companies are domiciled there, the Guidelines have had a huge impact on corporate ethics and compliance programs worldwide,

(continued on page 38)

Look Who's Watching You Now

- Transparency International and Amnesty International each monitor private actors in the international arena.
- Worldwide Responsible Apparel Production describes itself as "an independent, non-profit corporation dedicated to the certification of lawful, humane and ethical manufacturing throughout the world."
- The Fair Labor Association works "to promote adherence to international labor standards and improve working conditions worldwide."
- The International Council of Toy Industries has developed ethics guidelines intended to ensure safe and humane workplace environments for all workers in toy factories.

WHISTLEBLOWER HOTLINES

You Know How to Whistle, Don't You?

The United States leads the way in the use of hotlines and similar mechanisms to promote whistleblowing, but over the past dozen years, there has been a growing international trend towards protecting whistleblowers. Nearly all common law countries, including Australia, Canada, New Zealand, South Africa, and the United Kingdom, have adopted national or local rules that protect whistleblowers in many parts of society. "Whistleblower protections are also gaining ground in Europe, Asia, and Latin America. Several international instruments, including multilateral treaties, institutional regulations and codes of conduct now include protections for whistleblowers."[5]

COUNTRY	STATUTE	DESCRIPTION
Australia	Workplace Relations Act of 1996 (as amended) §170CK Available at *www.austlii.edu.au/au/legis/cth/consol%5fact/wra1996220/s170ck.html*	Protects a worker from termination of employment that is based, at least in part, on the employee's having filed "a complaint, or . . . participat[ed] in proceedings, against an employer involving alleged violation of laws or regulations or recourse to competent administrative authorities." Provides remedies in the event of a retaliatory discharge, an administrative process for the issuance of implementing regulations, and a judicial process by which terminated employees might seek redress for violations of the statute.
New Zealand	New Zealand's Protected Disclosures Act of 2000 §§ 6(1)–9 Available at *www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes*	Provides that an employee may disclose information in the manner provided by the Act if (a) the information is about serious wrongdoing in or by that organization; and (b) the employee believes on reasonable grounds that the information is true or likely to be true; and (c) the employee wishes to disclose the information so that the serious wrongdoing can be investigated; and (d) the employee wishes the disclosure to be protected. Requires that the disclosure be made according to the organization's internal procedures "for receiving and dealing with information about serious wrongdoing." However, disclosure may be made to "an appropriate [governmental] authority" if the employee believes that "the head of the organization is or may be involved" in the wrongdoing, that exceptional circumstances require immediate reference to an appropriate authority, or no response to an earlier disclosure has occurred and at least twenty days have passed.

And of course in the United States, Sarbanes-Oxley has had an effect. A survey conducted in July 2003 (one year after the enactment of the statute) found that 79.2 percent of the responding companies had established some type of hotline that enabled employees to anonymously raise ethics or compliance issues.[ii] Moreover, the 2004 changes to the Guidelines have created an additional incentive for companies to encourage whistleblowing. The Guidelines (§8B2.1 (b)(5)(C)) provide that a company's sentence can be reduced if it has established a method that lets the organization's employees and agents anonymously "report or seek guidance regarding potential or actual criminal conduct without fear of retaliation."

COUNTRY	STATUTE	DESCRIPTION
South Africa	The Protected Disclosures Act, 2000 §3	An employee is guarded against "occupational detriment" on account of having made a protected disclosure. Such a protected disclosure can be, in certain enumerated circumstances, a revelation to someone other than that employee's employer, such as a public official or a third party. The term "occupational detriment" covers discipline, transfer, suspension, harassment, intimidation, and other types of harmful actions.
United Kingdom	Public Interest Disclosure Act of 1998 Available at *www.opsi.gov.uk/acts/acts1998/80023—b.htm#2*	Any worker is protected who makes a "qualifying disclosure" in good faith to his or her employer, or in certain situations to another person, about a crime or a failure to satisfy a legal obligation, among other subjects. The worker is protected against "any detriment by any act" so long as his "qualifying disclosures" are made in the manner prescribed by the law.
United States	The Sarbanes-Oxley Act of 2002 15 U.S.C. §78f(m)(4), as added by §301 of the Sarbanes-Oxley Act of 2002, Pub. L. 107-204. Congress had earlier adopted the Whistleblower Protection Act of 1989, but that statute protects only federal employees, not employees in private industry. See 5 USC §§1201–1222.	Audit committees of publicly traded companies must "establish procedures for . . . the receipt, retention, and treatment of complaints received by the [company] regarding accounting, internal accounting controls, or auditing matters; and . . . the confidential, anonymous submission by employees of the [company] of concerns regarding questionable accounting or auditing matters." These mandated procedures are largely intended to encourage whistleblowing.

NOTES

i. R. Vaughn, T. Devine, and K. Henderson, *The Whistleblower Statute Prepared for the Organization of American States and the Global Legal Revolution Protecting Whistleblowers*, 35 GEO. WASH. INT'L L. REV. 857, 861 (2003) (footnotes omitted).

ii. "Business Ethics and Compliance in the Sarbanes-Oxley Era: A Survey by Deloitte and Corporate Board Member Magazine," available at *www.deloitte.com/dtt/cda/doc/content/us_assur_ethicsCompliance%281%29.pdf.*

(continued from page 34)

and have become a de facto global standard. To the extent that there is an EU approach to this issue, it has been much less up-front and less legalistic: The EU Commission actively supports the development of CSR (Corporate Social Responsibility), but it has stopped short of promoting compliance programs.

The definition provided by the Guidelines of when an ethics and compliance program can be called "effective" has animated many countries' efforts to elevate corporate behavior. In some countries, the authorities have not adopted any of the Guidelines per se, but have just suggested or strongly recommended that business organizations adopt higher standards of conduct through better ethics and compliance programs. The specifics of how to achieve this goal are left to businesses, with the expectation that those businesses will use the Guidelines as a template.

THE BUSINESS CASE FOR COMPLIANCE

Compliance programs can serve a variety of business purposes. For instance, the training that your company provides for compliance purposes should help employees perform their jobs, and should not focus merely on satisfying their compliance responsibilities.

Quality control. Information gleaned from hotline submissions can help improve business operations. As one prominent consultant has noted, organizations "are making greater efforts to listen for feedback and signs of trouble, just as one might monitor quality on a production line."[1] Since the quality of a business process that consists entirely, or almost entirely, of a service can be difficult to measure (unlike the output of a production line), a hotline might in fact serve as the best means of assuring such quality.

Risk management. The same prominent consultant has also observed that "[o]verall, existing business ethics activities are perceived to improve business performance, *not* hinder it." Business ethics protect companies from risks involved in violating the law, legal regulations, or company policies—including the risk of damage to a company's reputation. Business ethics can thus even help to create competitive advantage.[2]

Stock performance. There is also evidence that good corporate governance procedures are strongly correlated with above-average stock returns. A study of stock prices in the 1990s found that

> [a]n investment strategy that purchased shares in the lowest-*G* firms ("Democracy" firms with strong shareholder rights) and sold shares in the highest-*G* firms ("Dictatorship" firms with weak shareholder rights) earned abnormal returns of 8.5 percent per year… The results for both stock returns and firm value are economically large and are robust to many controls and other firm characteristics.[3]

The self-interest of corporations thus counsels a strategy that takes ethical concerns into account in their business activities.

Stakeholder expectations. Finally, compliance programs also serve companies' broader interests by helping them meet the expectations of internal and external stakeholders. Whether those stakeholders are the company's employees, shareholders, government agencies, extranational organizations, or NGOs, a business that incorporates certain behavioral norms into its day-to-day operations will fare far better. With fewer concerns for adverse publicity on account of ethical lapses and a deeper fund of societal goodwill to draw from, such a business should enjoy a smoother journey.

A WORLD OF COMPLIANCE

As chief compliance officer, how should you

(continued on page 49)

TIPS FOR GLOBAL COMPLIANCE PROGRAMS

Seven Ways to Improve Your Global Program

Be globally conscious. When implementing a compliance program or developing compliance policies and procedures covering multiple countries, make sure to remember your company's international status. Avoid policies focused on the United States that ignore the needs and practices of other countries where your company does business. Company encouragement for whistleblowers, for instance, is widely accepted in the United States and other common law countries, but it is looked upon with great suspicion in France and Italy, where people have unpleasant memories of collaborators during World War II. For example, in June 2005, McDonald's was told by La Commission Nationale de l'Informatique et des Libertés of France that it must excise from its code of conduct references to its reporting hotline, which the French government would not allow. East Europeans are even more hostile to the idea of anonymous reporting because of their recent experiences of life under a spying, totalitarian system.

Create consensus. Create a consensus throughout your company on the goals for the compliance effort and take the time to gain understanding and support for your program, especially in countries with works councils and labor unions. Some of these bodies may consider whistleblower and hotline procedures as infringing on bargained-for grievance procedures and may raise issues such as those raised in the Wal-Mart case cited below. (And see "Mapping Global Compliance Developments," on p. 44.) One useful approach is to form a group whose mission is to provide direction for the program. The group should include personnel from multiple countries and business units, to better reflect the interests of all significant parts of the company.

Identify shared values. With the assistance of a multinational coordinating employee group, identify the ways in which all employees share values. Make sure to highlight these shared values in the ethics and compliance program. This helps foster a greater sense of community among your far-flung employees, helping them to focus on what they have in common, rather than their differences.

Emphasize resource diversity. Distribute your company's ethics and compliance resources throughout various countries where your company does business. This helps ensure that your compliance procedures are sensitive to local needs. For the same reason, ethics and compliance positions should be staffed by people from a variety of countries.

Translate carefully. Make compliance and ethics materials available in multiple languages. But be aware that terms commonly used in the United States, such as "ethics," may not readily translate into some other languages. As one commentator notes, because the term "ethics" often does not translate well, some organizations reframe the concept through other terms such as integrity, business practices, or responsible business conduct. (See Nathan Hurst on Corporate Ethics, as cited in "From this point on," on p. 48.) All translations should appropriately reflect the vocabulary and idioms used by local people. This might require translation into a locally used dialect or language. For example, the Spanish spoken in some countries in South America varies from Castilian Spanish.

Train. Do not simply distribute the code of conduct and expect all employees to properly follow its rules. Particularly in light of linguistic complexities, some training and assistance must accompany the code.

Publicize the benefits. Business units often resent new initiatives that emanate from corporate with little apparent regard for the exigencies of the operating businesses. Hostility can be even more pronounced when initiatives from the company's headquarters affect employees in a distant country that has a very different social milieu. (Such resentment may have fueled the opposition to Wal-Mart's implementation of its corporate code of conduct. See *www.dw-world.de/dw/article/0,1564,1519102,00.html.*) To minimize such resistance to compliance rules, show the employees that compliance rules help your company's business and are not just another time-wasting corporate exercise. Make sure that the business units have an investment in the program and that they recognize the benefits they will gain from an effective compliance effort.

INTERNATIONAL ANTICORRUTION

The Growing Global Effort Against Corruption

Many countries have adopted anticorruption legislation in accordance with a growing international effort to eliminate corruption. (For more information, see "From this point on," on p. 48.) Those laws usually make it a criminal offense to accept bribes, but fail to punish those who give bribes. But there is growing demand for stronger anticorruption compliance policies.

Entity	Convention or Law	Description
EU	1998 Joint Action on corruption in the private sector, arts. 2.1 and 3.1 Available at *http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_358/l_3581 9981231en00020004.pdf*	Criminalizes both active and passive corruption conducted "in the course of business activities," even if no public figure or government action is involved. "Passive" corruption is (generally speaking—see the Joint Action definition) violating a duty by requesting or receiving an undue advantage in exchange for performing (or not performing) an act, whereas "active" corruption is offering or giving such an undue advantage.
OAS	The Inter-American Convention Against Corruption in 1996 (art. III, §10) Available at *www.oas.org/main/main.asp?sLang=E&sLink=http://www.oas.org/juridico/english/fightcur.html*	Includes identified "mechanisms to ensure that publicly held companies and other types of associations maintain books and records which, in reasonable detail, accurately reflect the acquisition and disposition of assets, and have sufficient internal controls to enable their officers to detect corrupt acts."
OECD	Convention on Combating Bribery of Foreign Officials in International Business Transactions, Art. 1, §1 Available at *www.oecd.org/document/21/0,2340,en_2649_34859_2017813_1_1_1_1,00.html#text*	The contracting nations agree to criminalize giving "any undue pecuniary or other advantage. . . to a foreign public official. . . in order that the official act or refrain from acting in relation to the performance of official duties," in order to gain improper advantage in the conduct of international business.
UN	The United Nations Declaration against Corruption and Bribery in International Commercial Transactions, adopted by the General Assembly in 1996	Covers both the private and public sectors. This document, more of a political commitment by the voting nations than a legal one, is part of an international effort to promote transparency in business transactions.
US	Foreign Corrupt Practices Act (FCPA), 15 U.S.C. §78dd-3	Prohibits firms that are registered in the United States and foreign corporations the shares of which are traded on United States stock exchanges from offering or giving anything of value to foreign officials or other specified persons, except for certain types of payments.

Six Compliance Hotspots

CHINA

Some might be surprised to learn that in China, certain types of compliance programs have entered the landscape, in spite of—or in the absence of—any lead from the state. The chief drivers have been the compliance certification programs of the global business supply chain in the industries where China is playing an increasingly dominant role, such as textiles and garments.

For the central government, the task of combating corruption remains the primary focus. Thousands of officials are prosecuted each year for corruption, but the problem remains massive, because the number of officials employed by all levels of government in China exceeds the populations of many countries.

Another government priority—induced by China's accession to the WTO in 2001—has been to abolish more than 2,600 laws and regulations and, in a number of areas, to publish new laws providing for greater transparency. China's commitments to the WTO include opening its capital markets to foreign competition by 2007, which serves as a powerful stimulant for further regulatory transparency.

Even though (with the exception of the annual anticorruption drives) there is no prospect of any domestically sponsored initiative to promote compliance programs, China is no stranger to focused compliance programs, certifications, and audits, many driven, as stated above, by the global supply chains of industries in which China now plays such an important role. The standards endorsed by international NGOs have therefore been introduced into a number of industries, such as clothing and garments.

EUROPE

United States and European multinationals have served as active propagators of codes of conduct in many countries. Such efforts often are driven by nonlegal factors, particularly the desire to create a common set of values throughout the organization. The deployment of such codes is not always smooth sailing, however, especially in civil law countries. France and Germany, for example, have strong traditions of labor contracts and collective agreements. Wal-Mart, which operates more than 90 stores in Germany, recently discovered this in the venue of the Labor Court (Arbeitsgericht) of Wuppertal. The Arbeitsgericht Wuppertal is reported to have recently granted an injunction filed by the group works council of Wal-Mart against parts of Wal-Mart's Code of Conduct for employees. The court said in its decision that certain guidelines (concerning the love life of employees or the telephone ethics hotline which employees are asked to use to report code violations) contradict German labor law. It ordered the company to delete from its Code guidelines relative to relationships between coworkers that prohibited "any kind of communication that could be interpreted as sexual." (The Arbeitsgericht Wuppertal has yet to issue a written decision, and this description is based on various newswire reports. See, for example, *www.indexonline.org/en/indexindex/articles/2005/2/germany-wal-mart-ethics-code-blocked-by-cour.shtml.*)

IRELAND

Ireland has become an increasingly attractive location for corporations in the United States that wish to enter the EU market, because Ireland is the EU member closest to the United States geographically and shares many attributes with the United States. In December 2004, Ireland's Office of the Director of Corporate Enforcement (ODCE) issued regulations of great potential interest to such companies. These regulations are designed to help companies comply with the Companies (Auditing and Accounting) Act of 2003.

Section 45 of the Companies (Auditing and Accounting) Act of 2003 requires company directors (a title that applies to corporate officers who would be considered senior management in the United States) to prepare a "compliance statement" that specifies the company's "(a)…policies respecting compliance with its relevant obligations; (b) its internal financial and other procedures for securing compliance with its relevant obligations; (c) its arrangements for implementing and reviewing the effectiveness of the policies and

Compliance Hotspots (Cont'd)

procedures referred to in paragraphs (a) and (b)." (See *www.oireachtas. ie/documents/bills28/acts/2003/a4403.pdf.*) The ODCE guidance—much like SEC pronouncements on securities statutes in the United States—provides guidance to companies subject to the statute on how to prepare the required statements. (It can be found at *www.odce.ie/_fileupload/publications/Revised_ Guidance_on_Directors_Compliance_Statements_Final.doc.*)

The statute also requires company directors to issue an annual statement in which they affirm the ongoing effectiveness of the procedures for assurance of compliance. The annual statement seems to resemble the certification required by § 302 of Sarbanes-Oxley.

JAPAN

Japanese society has long frowned on those who expose unpleasant facts, and Japanese business has a long tradition of sweeping corporate misconduct under the rug. In 1998, for instance, a bond trader at Daiwa Bank incurred $1.1 billion in losses, but the bank's directors withheld disclosure of the losses from US bank regulators until the directors had completed their own internal assessment. The bank was later required to shut down its US banking operations.

After lengthy deliberations, the Japanese Diet in March 2004 enacted the Whistleblower Protection Act (law No. 122 of 2004). This law does not come into effect until April 2006 and is reported to have been substantially inspired by and modeled on the UK Public Interest Disclosure Act (1998). In contrast to some of the many other countries with whistleblower laws, including Ghana, Israel, and Australia, the Japanese law applies to disclosures in the private as well as public sectors.

In another interesting private sector development, the Japanese Pharmaceutical Manufacturers Association (JPMA) has expanded on its Charter for Good Corporate Conduct by issuing the JPMA Compliance Program Guidelines. These 2001 guidelines provide guidance for JPMA members on how to meet appropriately high ethical standards of behavior. According to these guidelines, the compliance programs of all JPMA member companies should at minimum satisfy the eight requirements for an effective compliance program set out in the US Guidelines. (Available online at *www.jpma.or.jp/12english/publications/guide/02.html.*)

KOREA

Since the Korea Independent Commission Against Corruption (KICAC) began operating in 2003, this government-established organization has been working to protect whistleblowers and to encourage their activities by providing "appropriate rewards." The KICAC has had reasonable success in uncovering corruption. In one case, for instance, a high official of IBM Korea Inc. was prosecuted for offering bribes to government officials and illegally colluding with competitors in order to obtain government contracts worth 66 billion won (approximately $55 million).

UNITED KINGDOM

Corporate failures in the 1980s led the UK government to establish a series of groups to study business governance and other issues. Those groups issued reports that recommended a variety of corporate reforms. (One such report, which proved very influential, is known as the Cadbury Report. It is available online at *http://rru.worldbank.org/Documents/PapersLinks/1253.pdf.*) The government responded by issuing the Combined Code, which incorporates the reports' recommendations on corporate governance and internal control. (The Combined Code is available online at *www.fsa.gov.uk/pubs/ukla/lr_comcode.pdf.*)

Among other things, the Combined Code "contains the corporate governance principles and code provisions applicable to all listed companies incorporated in the United Kingdom." In addition to setting out specific best practices, the Combined Code contains principles that underlie those practices, so as to provide guidance for situations for which specific answers might not exist in the Combined Code itself.

From this point on . . .
Explore information related to this topic.

ACC RESOURCES ON INTERNATIONAL COMPLIANCE

ACC's committees, such as the International Legal Affairs Committee, are excellent knowledge networks and have listservs to join and other benefits. Contact information for ACC committee chairs appears in each issue of the *ACC Docket*, or you can contact Staff Attorney and Committees Manager Jacqueline Windley at 202.293.4103, ext. 314, or *windley@acca.com* or visit ACC Online℠ at *www.acca.com/networks/committee.php.*

- *Doing Business Internationally*, an ACC InfoPAK℠, available on ACC Online at *www.acca.com/infopaks/intbus.html.*
- E. Scott Gilbert, *603: Globalized Risk: Internal Investigations Outside the US,* ACC 2004 Annual Meeting course material, available on ACC Online at *www.acca.com/am/04/cm/603.pdf.*
- *The Global Law Department*, an ACC InfoPAK, available on ACC Online at *www.acca.com/infopaks/global.html.*
- Leading Practices in Global Law Department Design and Service Models: What Companies Are Doing, an ACC Leading Practices Profile, available on ACC Online at *www.acca.com/protected/article/international/lead_globallaw.pdf.*
- Richard Mosher and Owen Warnock, *"All For One and One for All: Navigating Trade Unions and Work Councils in Europe"* ACC Docket 23, no. 2 (February 2005): 48–67, available on ACC Online at *www.acca.com/protected/pubs/docket/feb05/union.pdf.*
- Lori Shapiro and Philip Weis, *803: Codes of Conduct for Multinational Corporations*, ACC 2004 Annual Meeting course material, available on ACC Online at *www.acca.com/am/04/cm/803.pdf.*

If you like the resources listed here, visit ACC's Virtual Library℠ on ACC Online℠ at www.acca.com/resources/vl.php. Our library is stocked with information provided by ACC members and others.

If you have questions or need assistance in accessing this information, please contact Senior Staff Attorney and Legal Resources Manager Karen Palmer at 202.293.4103, ext. 342, or palmer@acca.com. If you have resources, including redacted documents, that you are willing to share, email electronic documents to Julienne Bramesco, director of Legal Resources, bramesco@acca.com.

FOR ADDITIONAL INFORMATION

- Anticorruption Resources
  - Anticorruption efforts in countries belonging to the Anti-Corruption Gateway for Europe and Eurasia, available at *www.nobribes.org/en/country_ information/default.asp.*
  - "Combating Corruption: OGP Progress Report," Report No. 1.21/334 (December 2002), p. 7, issued by the International Association of Oil and Gas Producers, available at *www.ogp.org.uk/pubs/334.pdf.*
  - "First to Know: Robust Internal Reporting Programs," by Trace International, ISIS Asset Management, and The International Business Leader Forum (2004), available at *www.isisam.com/uploadfiles/co_gsri_first_to_know_jul_2004.pdf*
- T. Dworkin, *Whistleblowing, MNCs and Peace*, 35 Vanderbilt J. of Transnat'l L. 457, 461 (2002).
- Nathan Hurst, *Corporate Ethics, Governance and Social Responsibility: Comparing European Business Practices to Those in the United States*, The Markkula Center for Applied Ethics, Santa Clara University, Spring 2004, p. 6, available at *www.scu.edu/ethics/publications/submitted/hurst/comparitive_study.pdf.*
- R. Vaughn, T. Devine, and K. Henderson, *The Whistleblower Statute Prepared for the Organization of American States and the Global Legal Revolution Protecting Whistleblowers*, 35 Geo. Wash. Int'l L. Rev. 857, 861 (2003).

(continued from page 38)
approach your company's international compliance procedures? You should start by closely reviewing recent compliance-related developments in those countries where your company either does business or contemplates doing business in the near future.

Once you have digested that information, you should outline the international trends that you have identified in ethics and compliance programs. You should highlight how these growing expectations are already satisfied by your company's program. To the extent your program doesn't fully meet these emerging standards, you should determine how to revise the program in the near future. You will also need to be prepared for foreseeable future developments that might create new challenges for the company's compliance rules.

With all that done, you'll be on top of the international compliance issues that face your company, including the issues that arise under the Sarbanes-Oxley Act and the revised Guidelines. Finally, you'll be able to sit back and relax, and enjoy your view of the global compliance landscape.

Notes

1. *Ethical concerns and reputation risk management*, Arthur Andersen and London Business School, 1999, p. 12, available at *www.globalethics.org/andersonrpt.pdf.*
2. *Id.*
3. Paul Gompers, Joy Ishii, and Andrew Metrick, Corporate Governance and Equity Prices, Quarterly J. of Econ. 118(1) (Feb. 2003): 107, available at *http://finance.wharton.upenn.edu/%7emetrick/gov.pdf.*

Implementing a hotline for European operations: A single EU-wide approach or a country-centric design?

©2008 Steven A. Lauer
Corporate Counsel
Global Compliance Services, Inc.[i]

In the United States, privacy is recognized as a legal, enforceable right only in certain specific contexts. Putting aside the area of criminal law,[1] Congress and the state legislatures have created a right to privacy only in respect of various types of information in relatively delineated sectors of society.[2]

This "sectoral" approach differs considerably from the approach taken in many other parts of the world. The European Union (the "EU"), for example, has enshrined "the right to protection of personal data concerning him or her" in its Charter of Fundamental Rights. Similarly, Asia-Pacific Economic Cooperation ("APEC") adopted a Privacy Framework that includes the recognition that "personal information protection should be designed to prevent the misuse of such information and the principles of notice, collection limitation, proper use of personal information, choice for the individual in respect of the collection, use and disclosure of his or her personal information, accuracy, security, access and accountability.

While that basic approach to personal information or data differs greatly between the United States, on the one hand, and much of the world community, on the other, even among the countries outside the United States, the approaches vary in many details. Those differences suggest some significant implications for business organizations' data-management activities, as a review of some of those differences, even among just countries within the EU, will demonstrate.

Actions by the EU regarding data protection and hotlines

To enshrine the status of privacy as a fundamental right, especially in light of recent technological advances, the EU enacted a directive (the "Directive") "on the protection of individuals with regard to the processing of personal data and on the free movement of such data."[3] The Directive adopted by the EU serves as the basis for the protection of "personal information" within the EU and provides direction to the member states of the EU as to how they should protect the fundamental "right to the protection of personal data" of their citizens.[4] Within the Directive, however, the EU also established a mechanism by which to provide more-specific direction to those member states through the creation of the Article 29 Working Party (the "Working Party"), the role of which is "to contribute to the uniform application of [national measures adopted under the Directive]."[5]

In that capacity, the Working Party has prepared a number of reports and decisions in which it has addressed various issues regarding the use and processing of personal information. In one opinion, the Working Party discussed how corporate whistleblowing mechanisms might be affected by the EU's data protection regimes and how the Directive and member states' implementing legislation would apply to whistleblowing mechanisms implemented by businesses.[6] In a distinct paper, the Working Party discussed the scope of the term "personal data."[7]

The Working Party's report on whistleblowing schemes provides a good window on the challenges facing corporate compliance and ethics executives in that the data-protection agencies of several member states have issued opinions, decisions and guidance documents on that topic since the Working Party's report appeared. What did the Working Party say in that report?

The Working Party limited Report WP117 to specific issues related "to the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime."[8] Because some EU member states' laws specifically provide for whistleblowing mechanisms while other states' laws include no specific provision for such a mechanism, the Working Party established what would constitute an acceptable justification for implementing a whistleblowing mechanism: "the purpose of meeting a legal obligation imposed by [EU] or Member State law, and more specifically a legal obligation designed to establish internal control procedures in well-defined areas." (Report WP117, p. 7.) According to the Working Party, "an obligation imposed by a foreign legal statute or regulation which would require the establishment of reporting systems may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate." (*Id.*, at 8.) (The Working Party cited the Sarbanes-Oxley Act as an example of such a foreign law that would "not be considered as a legitimate basis for processing on the basis of Article 7(c)" of the Directive.)

The Working Party reviewed several principles established in the Directive and explained how, in its view, those principles would apply in respect of the processing of personal data that would apply to corporate whistleblowing schemes: fair and lawful processing, proportionality, and accuracy. In respect of proportionality, the Working Party indicated that "the company responsible for the whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistleblowing scheme" and "the company putting in place a whistleblowing scheme should carefully assess whether it might be

---

[1] The Supreme Court has invalidated convictions on account of citizens' rights to privacy with respect to access to information about birth control, for example, in *Baird*.

[2] Congress enacted laws to protect personal health-related information (see the Health Insurance Portability and Accountability Act – known as HIPAA) and the financial-account information of consumers (see the Gramm-Leach-Bliley Act).

[3] See Directive 96/46/EC of the European Parliament of October 24, 1995, posted at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[4] The status of the efforts of the member states of the EU to implement the Directive's rules in their respective legal frameworks is summarized by the EU's agency for Freedom, Security and Justice in a document posted at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.

[5] See Article 30(1)(a) of the Directive.

[6] Rather than its somewhat unwieldy title ("Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime"), I'll refer to that report in this article, using its identifying number, simply as "Report WP117." The Working Party has posted the report at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

[7] See "Opinion 4/2007 on the concept of personal data" (document WP136), posted at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[8] Report WP117, p. 4.

possible to limit the number of persons who may be reported through the scheme." (*Ibid.*)

The data quality principle requires steps to assure that the data collected and processed are accurate. Untrue or incomplete data must be erased or rectified.

The Directive also created specific rights on the part of an individual (a "data subject" in the lexicon of the Directive) whose personal data are collected and processed by a data controller. Those rights include not only a right to know that data concerning him or her has been or is being collected, but also to check the accuracy of the data so collected, to rectify it if inaccurate and to have it erased once outdated/

Actions by member states regarding data protection and hotlines

With the above actions (and others) by the EU as backdrop, let's examine how some EU member states have addressed questions regarding corporate whistleblowing hotlines. Have they created hurdles for multinational organizations operating in their respective jurisdictions? The short answer to that question is "yes," and an examination of a few issues will illustrate those hurdles. Specifically, the approaches that some countries in the EU have taken to the issues of (i) allowable allegations, (ii) the ability to accept reports that do not identify the caller/reporter and (iii) whether and how a subsidiary corporation can include its parent corporation in another country within the distribution of reports received over a hotline exemplify the challenges that such organizations face. Let's examine recent decisions or guidance documents issued by the data protection authorities of Belgium, France, Germany, Netherlands and Spain.[9]

The permissible scope of a whistleblowing hotline

The Directive states that personal data can be processed only for legitimate purposes and, with respect to a corporate hotline, the relevant purposes are that the "processing is necessary for compliance with a legal obligation to which the [data] controller is subject" and that "processing is necessary for the purposes of the legitimate interests pursued by the [data] controller … except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)" of the Directive.[10]

None of the member states mentioned will accept satisfying the requirements of the Sarbanes-Oxley Act as a legitimate purpose for the collection and processing of personal information incident to the operation of a whistleblowing hotline. Rather, as suggested by the Working Party, they look to their respective organic laws to determine whether such a mechanism might be required within their jurisdictions and, if so, what the permissible scope would be. Unfortunately, those government agencies have reached disparate conclusions. What have they said?

Belgium: The Belgian Privacy Commission agreed with the Working Party that "a legal provision of Belgian law must be involved" to support the implementation of a whistleblowing system. Such a system "can only involve reports concerning problems that clearly would not be processed by the normal line of command and for which there is no specific procedure or body legally regulated." For issues not so described, the other, primary mechanism within the organization should be engaged. Because a whistleblowing system can only be a supplementary communication channel, reports must relate "to serious acts (violation of regulations applicable to the organization in question or internal written company rules (particularly in the departments of finance and accounting) or if a crime is involved," all of which means that it must involve "serious wrongdoing" or "serious facts or situations that must be reported in the general interest of the company or for the proper governance of the organization and for which the whistleblower considers it not or no longer possible through normal channels."

France: The Commission Nationale de l'Informatique et des Libertés (CNIL) issued guidelines in November 2005 "for the implementation of whistleblowing systems in compliance with the French Data Protection Act." CNIL identified a basis in French law for a whistleblowing system "relating to the internal control of credit and investment establishments" and for systems "whose purpose is to combat bribery." In France, as in Belgium, the whistleblowing system "must be designed as solely complementary to other reporting systems."

Germany: The German Ad Hoc Working Group on "Employee Data Protection" of the Düsseldorfer Kreis stated that a whistleblowing system is "intended as an additional mechanism for employees to report misconduct internally" and that it "supplement[s] the regular information and reporting channels." That working group identified the proper purposes of a system as the "goal of ensuring financial security in international financial markets," especially "the prevention of fraud and misconduct with respect to accounting, internal accounting controls, auditing matters, as well as the fight against bribery, banking and financial crime or insider trading."

Netherlands: In additional to the familiar litany of "accounting and auditing abuses," the Dutch Personal Data Protection Board referred to reports that "concern a substantial abuse" as among those that a whistleblowing system might accept, although it specified certain protections that an organization should implement with regard to ensuring that such reports are indeed so focused. A whistleblowing system also "cannot take the place of the normal handling options" for complaints.

Spain: In its opinion on reviewing the specifics of a whistleblowing system submitted for its approval, Spain's Agencia Española de Protección de Datos (AEPD) indicated that such a system should be "limited to reports involving internal or external topics or rules, the violation of which could have an actual impact on the maintenance of the contractual relationship between the company and the person incriminated." AEPD thus set out a somewhat broader scope of permissible allegations by tying that scope to the relationship between the organization and the party named in a report. Whereas other data protection authorities have expressed disapproval for reports of wrongdoing that does not relate to criminal violations,[11] then, AEPD seems to allow the receipt of a complaint over a

[9] Translations of the decisions discussed here can all be found on Global Compliance's website, at http://www.globalcompliance.com/legislation-knowledge-center.html.

[10] Directive Article 7(c) and Article 7(f).

[11] For example, in it decision, the German Düsseldorfer Kreis stated that "[i]n the case of conduct which falls under [the phrase 'conduct which adversely affects company ethics'] ('soft criteria') the legitimate nature [of a report] can only be appraised on a case by case basis…. For this group … it is assumed that the legitimate interests of the data subjects [*i.e.*, individuals whose personal information appears in hotline reports and therefore is processed as part of the whistleblowing report] involved are compelling…. [A] connection between the breach and considerable loss for the company … cannot be identified so that at this point doubt arises as to the legitimate interest of the data controller [*i.e.*, the company]. Therefore in such

whistleblowing hotline so long as the subject matter of the complaint could serve as the basis for discipline of the data subject.

Caller anonymity

One issue that troubled the Working Party is the possibility that whistleblowing systems might receive anonymous reports. Whereas in the United States anonymity is an accepted – sometimes even encouraged[12] - protection for such matters, in Europe anonymity occupies a much less esteemed position. Indeed, according to the Working Party, "anonymous reports raise a specific problem with regard to the essential requirement that personal data should only be collected fairly. As a rule, the Working Party considers that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement."[13]

To understand this view, you need to keep in mind the history of Western Europe. "In some Western countries such as France, Greece and Luxembourg, … whistleblowing is seen as little different from informing the government about a neighbor's dissident views. This, in turn, is frowned upon at least in part because it is considered an attribute of totalitarian or Communist states. In Germany, whistleblowing is thought unnecessary because of moral superiority."[14] The national data protection authorities expressed views very similar to that of the Working Party, but their decisions nonetheless create considerable challenge to multinational companies.

Belgium: Belgium's Privacy Commission "favors a general prohibition of anonymous reporting," although it then "subscribed to the argument developed by [the Working Party] that authorizes the processing of anonymous reports on a very restricted basis." The Commission outlined the procedural safeguards necessary to allow the receipt and processing of anonymous reports: absolute anonymity for the reporter, the need to conduct an initial investigation and reach a determination that the report contains well-grounded or baseless charges before any further dissemination within the company, such complaints must be processed by someone specifically appointed to handle complaints subject to professional obligations of confidentiality and with sufficient autonomy to insulate the processing from compromise and pressure from senior management, the need for utmost discretion in the processing of anonymous reports, and the obligation to cease processing a report if the confidentiality of the whistleblower has been intentionally violated.

France: CNIL expressed its belief that "[t]he possibility to file anonymous reports can only increase the risk of slanderous reports." Nonetheless, CNIL realized that "the existence of anonymous reports, even and especially in the absence of organized confidential whistleblowing systems, is a reality. It is difficult for company management to ignore this type of report, even when not in favour of them on principle." CNIL then delineated the need to have specific precautions for the handling of anonymous reports.

Germany: The Düsseldorfer Kreis agreed with the Working Party that anonymous reports should be accepted "only in exceptional cases." The group urged the protection of the identities of whistleblowers, with full information to those callers of the protection of identities in the system as a mechanism to discourage the filing of anonymous reports and the reduction in the need for them.

Netherlands: Personal Data Protection Board also recognized that "many reports are made anonymously and … it is not easy for many companies to deny such reports. The handling of these anonymous reports requires that special guarantees must be made, namely with regard to the first assessment of the report. An organization may not encourage the use of anonymous reports and must bring a system to life whereby the point of departure is that the identity of the informant is established. The reports themselves must be based on facts and not on individuals."

Spain: AEPD, in its opinion on the legality of a whistleblowing system submitted by an unnamed company for approval, quoted at length from Report WP117 on the acceptance of anonymous reports, even though disfavored and despite the advice required to be given to the caller. AEPD went on to say, however, that "procedures guaranteeing the confidential processing of reports filed through the whistleblowing systems must be established, so that the existence of anonymous reports is avoided" and that "[a]n initial filter of confidentiality and an additional possible final allegation of anonymity would not be sufficient for the operation of the system." The Spanish agency seems to prohibit even the acceptance of anonymous reports, then, which puts it squarely at odds with its counterparts in Belgium, France, Netherlands and Germany and the Working Party.

Transfer of hotline reports to a parent corporation in another country

With increasingly global business operations that span national borders and that involve multiple levels of corporate structure, corporate families often and regularly transfer data between and among related entities in the course of their business operations. To what degree do such transfers of data received through reports over a hotline implicate data transfer rules? How have the member states dealt with that issue?

The Working Party recognized the need for transfers between affiliated companies, such as from a company within the EU to a parent corporation outside the EU, even if that other country does not adequately protect personal information by law. The Working Party stressed that "the nature and seriousness of the alleged offense should in principle determine at what level, and thus in what country, assessment of the report should take place. As a rule, … groups should deal with reports locally … rather than automatically share all the information with other companies in the group." That Working Party did recognize, however, that "data received through the whistleblowing system may be communicated within the group if such communication is necessary for the investigation, depending on the nature of the seriousness of the reported misconduct, or results from how the group is set up.

Belgium: "Data transfers to a parent company in a country outside the European Union can only be justified if it involves particularly serious issues for which it has become obvious that the processing of the report cannot or can no longer be properly done

---

cases it can be assumed in principle that there is a compelling legitimate interest of the data subjects involved, and the processing or use of the personal data is not legitimate in this respect."

[12] See, for example, §301 of the Sarbanes-Oxley Act, which added a provision to the Securities Exchange Act of 1934 that requires corporate boards of directors to establish procedures by which employees could submit "confidential, anonymous submission[s] … regarding questionable accounting or auditing matters."

[13] Report WP117, at 11.

[14] Dworkin, "Whistleblowing, MNCs, and Peace," 35 Vanderbilt J. of Transnational Law 457, 470-471 (2002) (internal footnotes omitted).

exclusively at the European organization level or that the processing may have repercussions beyond the company located in Belgium or in the European Union." Enterprise-wide compliance programs, then, would face hurdles in achieving enterprise-wide reporting and managing of allegations received through a whistleblowing mechanism.

France: CNIL recognized that, within a corporate family, "data received through the whistleblowing system may be communicated within the group if such communication appears necessary to the requirements of the investigation and results of the organization of the group. Such communication will be considered as necessary to the requirements of the investigation for example if the report incriminates a partner of another legal entity within the group, a high level member of management official of the company concerned." This may be a slightly more relaxed requirement than the Belgian one just cited. CNIL went on to warn, though, that "[i]f such communication appears necessary and the recipient of the data belongs to a legal entity established in a country outside the European Union which does not provide adequate protection [to personal information], the specific provisions of the EC Directive 95/46 of 24 October 1995 and of the French Data Protection Act of 6 January 1978, as amended, relating to international data transfers apply."

Germany: "The Düsseldorfer Kreis cited its general view that "[i]n principle it is not legitimate to transfer personal data of either the whistleblower or the incriminated person to third parties" and cited the transfer of such information in connection with further investigation of a report or with ensuing court proceedings as exceptions to that principle. Otherwise, that group did not address questions relating to intra-group data transfers.

Netherlands: The Dutch agency noted that "the forwarding of personal data to a third country may be appropriate" with appropriate safeguards regarding confidentiality. The agency's opinion provides no further detail regarding the appropriateness of transfers within a corporate group.

Spain: The AEPD discussed the transfer of personal data, received in hotline reports, to offices in other countries. With respect to transfers to countries outside the EU, AEPD stressed the need to use data transfer agreements, such as the EU-approved standard clauses.

Deletion or retention of data

The Directive provides that data "which permits identification of data subjects [must be kept] for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[15] The Working Party interpreted this to mean that "[p]ersonal data processed by a whistleblowing scheme should be deleted, promptly, and usually within two months of completion of the investigation of the facts alleged in the report."[16] What implications does that requirement hold for corporate hotline programs?

[15] See Article 6(1)(c) of the Directive.
[16] Report WP117, p. 12.

Belgium: The Belgian authority stated that the "complaint manager"[17] must "ensure that personal data … are kept for a period of time that does not exceed what is necessary for processing the report, including any legal or disciplinary procedures with regard to the person incriminated (in case of a justified report) or with regard to the whistleblower in case of unjustified reports or libelous accusations."[18]

France: CNIL took a similar view: "[d]ata relating to a report found to be unsubstantiated … must be deleted immediately" and "[d]ata relating to alerts giving rise to an investigation must not be stored beyond two months from the close of verification operations unless a disciplinary procedure or legal proceedings are initiated against the person incriminated in the report of the author of an abusive report."

Germany: The Dusseldörfer Kreis agreed that "data should be destroyued within two months after conclusion of the investigation" and that "[s]toring data for a longer period may only be legitimate until further legal measures … have been clarified." As to data included in an unsubstantiated report received over the hotline, however, that group determined that the data "have to be deleted without undue delay," a slightly different formulation than that used by the Belgian and French authorities.

Netherlands: The Dutch Personal Data Protection Board agreed with the two-month limit on data retention for concluded investigations , subject to longer a period for data if "disciplinary measures were taken against the informant (false reporting) or the person on whom the report was made (justified reporting)." As for an unjustified report, "[t]he processing … must be immediately suspended and the data destroyed."

Spain: AEPD quoted the Spanish data protection law as follows: "personal data shall be erased when they have ceased to be necessary or relevant for the purpose or which they were obtained or recorded." Thus, under Spanish law, "it would be essential for a maximum term to be established to preserve data related to the reports, in order to prevent the data from being kept for a longer period that could prejudice the rights of the incriminated person and also those of the whistleblower."

Where does this leave you?

To a large degree, the protections for personal data represented in the Directive and the clash between the views of EU data protection regulators and their U.S. counterparts reflect their countries' very disparate histories. The Working Party alluded to this in its opinion when it said the following:

> The number of issues raised by the implementation of whistleblowing schemes in Europe in 2005, including data protection issues, has shown that the development of this practice in all EU countries can face substantial difficulties. These difficulties are largely owed to cultural

[17] Under Belgian law, "[t]he report must be collected and processed by a person in the organization specifically appointed to hear complaints," who must be "bound to professional confidentiality when processing the report, even with regard to executives (unless immediate precautionary measures are required), other members of the staff, labor union organizations and third parties." See page 5 of the opinion of the Belgian Privacy Commission.
[18] *Id.*, at 6-7.

> differences, which themselves stem from social and/or historical reasons that can neither be denied nor ignored.[19]

The Chairman of the Working Party described those differences somewhat more explicitly in a letter to the Director of the Office of International Affairs of the Securities and Exchange Commission: "anonymous reporting evokes some of the darkest times of recent history on the European continent, whether during World War II or during more recent dictatorships in Southern and Eastern Europe. This historical specificity makes up for a lot of the reluctance of EU Data Protection Authorities to allow anonymous schemes being advertised as such in companies as a normal mode of reporting concerns."[20] We thus face very different views of the value of whistleblowing: in many countries within the EU, that technique conjures up images of "denunciation" as practiced in Nazi Germany or wartime France, while in the United States it evokes "Deep Throat" of Watergate renown.

For that reason, the implementation of a whistleblowing hotline in an organization with European operations must be well-planned. An effective awareness campaign by which the employees learn about the hotline occupies an essential place in that implementation, and not simply to satisfy the expectations of EU data protection regulators regarding how such a mechanism is "positioned."[21] That campaign should take into account the various requirements of EU regulators summarized above (as well as others).

In addition to such an awareness campaign, an organization that plans to implement a hotline should also consider training. Should the implementation of the hotline be accompanied at the same time, or at least relatively contemporaneously, by training on one or more topics relevant to the hotline? For example, if the organization will allow employees to use the hotline to report issues or concerns relative to accounting, auditing and similar issues consistently with the guidance issued by CNIL and the other EU member states discussed above, it might wish to provide its employees guidance on how to recognize such issues. A course on financial integrity or on what information might suggest financial irregularities or fraud has taken place could add considerable value to the hotline as part of a fraud prevention program.[22]

The variation of the data-protection requirements discussed above obviously presents hurdles for an effective implementation of a hotline for multiple countries within the EU. The scope of permissible allegations among EU member states, for example, represents one challenge to a multijurisdictional program. The ability to receive anonymous reports within the various countries also varies considerably.

One possible approach is to adopt what some call a "pan European" solution. An organization following this approach will design its program to meet the most stringent (from the perspective of the implementing organization) regulations among the EU regulators. For example, because the permissible allegations under CNIL's approach are at least as narrow as those allowed by other member states' data protection authorities, allegation scope aligned with CNIL's guidance should suffice. By prohibiting the acceptance of anonymous reports, a company would satisfy the expectations expressed by AEPD in its June 2007 opinion.

This approach also carries, however, a significant risk. It works so long as the stringent standard on which it is based remains the most stringent standard. If any one or more jurisdictions issue guidance even more stringent on a substantial issue, however, the entire EU-wide program would require amendment. Had a program designed prior to June 2007 accepted anonymous reports as permitted by the Working Party, CNIL and other regulators, the Spanish decision would have affected that program's ability to accept anonymous reports anywhere within the EU.

For these reasons, flexibility has become an indispensable characteristic of an effective hotline. Country-specific regulations call for country-specific program design. While meeting the varying expectations of EU data protection regulators requires close analysis of their respective laws and guidance documents, once that analysis is complete for a country, it remains accurate for that country until that country's regulator changes its standards.

---

[19] Report WP117, p. 4.

[20] See page 3 of the letter dated July 3, 2006, by Peter Schaar, Chairman of the Working Party, to Ethiopis Tafara, posted at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006-07-03-reply_whistleblowing.pdf.

[21] According to CNIL, for example, "[c]lear and complete information on the system must be given to potential users by any appropriate means." Other EU regulators have expressed similar views.

[22] See Lauer, "Compliance Programs And Fraud Prevention," The Metropolitan Corporate Counsel, vol. 14, no. 5 (May 2006), p. 61.

Canada – Unexpected Differences

- Even in a country like Canada with so many similarities to the USA, legally and culturally, there are hurdles to rolling out global policies and compliance programs
- Will discuss three specific areas that create challenges – employment, privacy & data protection and trade.

Employment

- Human rights and privacy & data protection legislation can affect:
  - Drug and alcohol testing;
  - Background checks;
  - Routine medical checks
- Policy violations may not be just cause for dismissal under Canadian law

Privacy & Data Protection

- Collection, use and disclosure of personal information by private sector organizations regulated at both federal and provincial levels
- Standard forms of consent may not be adequate

Privacy & Data Protection, cont'd…

- Legislation does not explicitly restrict transfer of personal information outside of Canada but Privacy Commissioner has expressed concerns so most organizations notify if data is to be stored, processed or accessed outside of Canada
- Administrative requirements such as identification of individual accountable for organization's compliance with the privacy legislation

Trade

- Extraterritorial Laws
  - Cuban Assets Control Regulations
  - *Cuban Liberty and Democratic Solidarity (LIBERTAD) Act*
- *Foreign Extraterritorial Measures Act*
  - FEMA Order
- Export and Import Controls