

International Business Law News

A Publication of the Minnesota State Bar Association International Business Law Section

Fall 2002

In This Issue

- | | |
|---|----|
| The Changing Face of Export Controls:
How the War on Terrorism is Affecting Your
Company's Export Compliance Obligations
<i>Richard Y. Sako and Louis B. Lambert</i> | 2 |
| Should You, and Can You Monitor Your
Employee Use of E-mail? A Message from the
U.K. and Minnesota, U.S.A.
<i>Anastasia Fowle and Rhona Schmidt</i> | 5 |
| Bisnes Commercial Overview-Russia and Siberia
<i>Elena Ovsiannikova</i> | 10 |



www.mnbar.org

From the Chair

By: Paula R. Johnson, Jostens, Inc.

This edition of the Newsletter helps us kick off the MSBA International Business Law Section's 2002-2003 season. An active agenda is planned for this year. In keeping with tradition, we will be hosting speakers on topics of interest to you at our regularly scheduled monthly meetings. But to make it more convenient for those not officed in downtown Minneapolis, our November and December meetings will take place at 4:30pm – this will also allow all of us to have some socializing time! Specific dates for all of these meetings will be announced shortly – be sure to mark your calendars to attend.

We are also excited about the Annual Spring Institute! Planning will begin in earnest in October. Diane Miller Esch, the Institute Chair, is actively seeking help. If you are interested in assisting her in any way, please feel free to contact her at dcmilleresch@hotmail.com. This is not a huge commitment. Even an email will be appreciated if you have any ideas or suggestions.

Finally, if you've ever had the urge to be published, don't overlook the great opportunity to contribute to the Newsletter. Jennifer Kalvestran would be delighted to receive your submissions. (She reserves her editorial right to judge relevancy, timeliness and, of course, factual accuracy...). Feel free to contact her at jkalvestran@meagher.com.

As always, if you have suggestions to improve the Section, I know I speak for the officers and the Council when I say that you can contact any of us, anytime. In particular, if you have any suggestions about how to make the Section more relevant to international law practitioners in greater Minnesota, please let us know. Our goal is to make the Section provide more value to your practice. We look forward to hearing from you!

Internationally yours,

Paula Johnson

The Changing Face of Export Controls: How the War on Terrorism is Affecting Your Company's Export Compliance Obligations

By: Richard Y. Sako and Louis B. Lambert, Faegre & Benson, LLP

"Oh, that's not even an issue, we only sell our products here in the U.S."

"We don't have to worry about that—we only sell to Canada, the U.K. and those other friendly countries in Europe."

These are some of the typical responses from U.S. companies regarding their compliance with U.S. export control laws. Although statements like these may have been close to the truth years ago, the War on Terrorism has accelerated a change in export controls. Businesses will now find an increased emphasis on so-called "activity-based controls" that focus not just on where the product is going, but with whom you're doing business.

This change in philosophy is not recent. But the War on Terrorism has further fueled the prevailing sentiment that activity-based controls need to play a more prominent role in protecting U.S. national security interests. This change has significant consequences for U.S. companies because activity-based controls are not limited to the export of products and technology to parties in foreign countries. Some of these controls even prohibit U.S. parties from engaging in transactions occurring solely within the United States.

As a result, U.S. companies need to implement appropriate procedures to comply with activity-based controls on all commercial transactions—both foreign and domestic. Analyzing export issues solely on the basis of the old-school model—you're safe unless you export to certain countries—could lead to disastrous results.

Control Lists vs. Activity-Based Controls

More than 25 federal statutes, commonly known as the Export Control Laws, govern the dissemination of sensitive U.S. technology and know-how in two ways: a *control-list* approach and an *activity-based* approach.

The control-list approach focuses on the nature of the product or technology itself, and regulates export through product control lists and country charts, such as the Commerce Control List under the Export Administration Regulations,¹ the U.S. Munitions List under the Arms Export Control Act,² and the Nuclear Equipment and Materials List.³ Typically, under this approach, an exporter first determines whether its product is covered by the product list and, if so, then consults the product list to determine what restrictions, if any, apply to the export of the product. The exporter then consults country charts to determine whether a license is required to ship the product to its destination.

The activity-based approach, by contrast, focuses on the nature of the transaction and the identity of the exporter and its partners in the deal. It is *not* limited to an examination of the specific product being shipped. The purpose of an activity-based approach is to control certain dangerous activities, such as the proliferation of nuclear or chemical weapons or the advancement of terrorist organizations. This approach is exemplified by provisions restricting engagement in proliferation activities under the Export Administration Regulations,⁴ trade embargoes administered by the U.S. Department of Treasury,⁵ anti-boycott legislation,⁶ and many prohibited parties restrictions.⁷

These two approaches are not mutually exclusive. In most cases, activity-based controls apply in addition to control-list restrictions. Many U.S. companies, however, have become accustomed to thinking about export controls only in the context of the control-list approach.

The events of September 11 have turbo-charged this changing trend in U.S. export control legislation. The "bad guys" are no longer limited to a particular country. As a result, all transactions, even those that seem purely domestic, and transactions in "friendly countries," now fall under the scope of export control laws.

Prohibited Parties Restrictions

As the job of promoting and protecting U.S. national security interests becomes geographically boundless, the role of one form of activity-based control—the prohibited parties restrictions—has taken on increased significance as a mechanism for enforcing U.S. export control policy.

Prohibited parties restrictions make it unlawful for U.S. companies to engage in commercial transactions with entities or people who, for one reason or another, have been identified on name lists maintained by various export control authorities. Typically, the entities or people on the lists are parties that have either violated export rules or orders in the past, or who have been linked to terrorist organizations or other undesirables.

There are currently six primary sources of prohibited parties restrictions that should be consulted before engaging in any commercial transaction. These so-called “bad parties” lists are maintained by the various export control regulatory authorities. These lists consist of the following:

1. Denied Persons List⁸
2. The Entity List⁹
3. Specially Designated Nationals and Blocked Persons List¹⁰
4. Specially Designated Narcotics Traffickers List¹¹
5. List of Terrorists¹²
6. List of Debarred Parties¹³

Each of these lists is briefly summarized below.

Denied Persons List. This list is administered by the Department of Commerce and identifies individuals and entities that have been denied export privileges by the Commerce Department for previously violating the Export Administration Regulations. Every export transaction involving a party on the Denied Parties List requires prior written authorization from the Department of Commerce. *Even transactions involving products or technology that are not controlled under the Export Administration Regulations require prior authorization if they involve a party on the list.* Many of the parties on this list have known addresses in the United States and, therefore, the list should be checked before finalizing even domestic transactions.

The Entity List. This list is also administered by the Department of Commerce. It identifies individuals and entities known to be engaged in activities supporting the

proliferation of weapons of mass destruction, including nuclear, chemical and biological weapons, as well as missile technology used to deliver these weapons. The parties on this list are foreign-based entities. Many of the parties on the list, however, are parties that may not, at first glance, raise red flags among U.S. exporters. As in the case of the Denied Persons List, any export transaction with a party on this list—even an export involving a product that is not a controlled item under the Export Administration Regulations—is prohibited unless a license is obtained from the Department of Commerce.

Specially Designated Nationals and Blocked Persons List. This list is administered by the Office of Foreign Assets Control (“OFAC”) of the Department of Treasury and identifies individuals and entities that U.S. companies and their affiliates are prohibited from engaging in business with under OFAC-administered trade sanction and embargo programs. One purpose of this list is to put U.S. companies on notice to minimize inadvertent violations of trade sanction and embargo programs by U.S. companies who do business with entities that seem to have no connection with a sanctioned country.

Specially Designated Narcotics Traffickers List. This list was created by President Clinton pursuant to an Executive Order. The list identifies foreign narcotics traffickers whose property or interests in property in the U.S. have been blocked, and with whom U.S. businesses and their affiliates are prohibited from engaging in any transaction. The Executive Order creating this list states that the list may include any additional parties that the Department of Treasury designates in the future.

List of Terrorists. As part of his response to the terrorist acts on September 11, President Bush issued an Executive Order declaring a national emergency to deal with the terrorist threat and setting forth sanctions intended to hinder the pervasive and expansive financial network supporting terrorist groups around the world. The Executive Order identifies terrorists and those people or entities supporting terrorists whose property or interests in the U.S. have been blocked and with whom U.S. businesses and their affiliates are prohibited from engaging in any transaction.

List of Debarred Parties. This list is administered by the Department of State and applies only to U.S. companies or individuals dealing with products or technology that are listed on the Munitions List under the International Traffic In Arms regulations (“ITAR”) of the Arms Export Control Act. U.S. companies and

individuals subject to ITAR are prohibited from exporting products or technology to any party on this list.

Possible Sanctions For Violations of the Export Regulations

U.S. companies are held to a high legal standard for export compliance. Sanctions for violations include criminal and civil penalties including up to ten years imprisonment and fines of up to \$1 million. A company's exporting privileges can also be suspended or revoked entirely. Civil penalties for export violations may be imposed without any intentional wrongdoing, and criminal sanctions can be imposed for "knowing" export violations.¹⁴

The role of the bad parties lists in enforcing U.S. export policies is increasing in importance. These lists are updated daily, and the number of individuals and entities identified on the lists is growing quickly and in some cases, exponentially. Once changes to the lists are published in the Federal Register, U.S. companies are deemed to have knowledge of the changes. Thus, companies are faced with the increased burden of ensuring that these lists are consulted before engaging in any transaction involving the transfer of goods or technology—even transactions that are "domestic" in nature.

For example, suppose your company receives an order for products from Optical Associates, Inc., a Miami, Florida company; or suppose that your company is considering entering into a joint venture in the U.K. with Perfect Technologies, Ltd.; or suppose that your company is shipping product to a distributor in the Bahamas who has obtained a letter of credit from Bank al Taqwa, in Nassau. Proceeding with these transactions without checking the lists could result in significant penalties. Both Optical Associates and Perfect Technologies are on the Denied Persons List, and Bank al Taqwa is on the Specially Designated Nationals and Blocked Persons List. In short, checking the lists needs to be made a part of every internal control compliance policy.

Where to Find More Information

To find more information about complying with the export regulations, to check new Federal Register releases and to view on-line versions of the bad parties lists described above, visit the following websites:

Department of Commerce: www.bxa.doc.gov

Office of Foreign Assets Control:
www.treas.gov/offices/enforcement/ofac

Department of State: www.pmdtc.org

Conclusion

As the War on Terrorism persists, activity-based export controls will become the predominant mechanism to ensure that U.S. goods and technology do not fall into the wrong hands. U.S. exporters should understand their obligations under this new export control model, and should implement procedures to ensure compliance. No longer can U.S. exporters simply think of export controls as a handful of countries in which they cannot do business. Now, U.S. exporters need to be conscious not only of where they are doing business, but also with whom they are doing business.

Notes

¹ 15 C.F.R. pt. 774 (2002).

² 22 C.F.R. pt. 121 (2002).

³ 10 C.F.R. § 110.8-9 (1994).

⁴ See 15 C.F.R. § 736.2(b)(7) (2002) (General Prohibition number 7, prohibiting a U.S. person from supporting proliferation activities).

⁵ See 31 C.F.R. pt. 500-598 (1998).

⁶ See 15 C.F.R. pt. 760.1-.5. (2000).

⁷ See 15 C.F.R. pt. 764, Supp. No. 2 (2000).

⁸ *Id.*

⁹ See 31 C.F.R. pt. 744, Supp. No. 4 (2001).

¹⁰ 31 C.F.R. Ch. V (1998).

¹¹ Exec. Order No. 12,978, 3 C.F.R. 415-17 (1995).

¹² Exec. Order No. 13,224, 3 C.F.R. 786-790 (2001).

¹³ U.S. Dep't of State, *Defense Trade Controls – List of Debarred Parties*, July 1988-May 1999, available at www.pmdtc.org/debar059.htm.

¹⁴ 15 C.F.R. § 764.3 (2002); 22 U.S.C. § 2778(c) (2002).

Should You, and Can You, Monitor Your Employee Use of E-mail? A Message from the U.K. and Minnesota, U.S.A.

*By: Anastasia Fowle, Dorsey & Whitney, London, England and
Rhona Schmidt, Dorsey & Whitney, Minneapolis, Minnesota*

Introduction

E-mail is everywhere. Whether a company is located only in Minnesota or has multinational branches, an employer needs to understand the “pros and cons” of monitoring employee e-mail. Here, we focus on Minnesota, because of brand new changes in state law, and the U.K., because of recently introduced regulations and the ever-increasing employee awareness of their “right to privacy.” This article provides a brief synopsis of reasons why employers in both or either locations should be interested in monitoring e-mail use, some recent statistics on the percentage of companies monitoring use in the U.K. and the U.S., and a summary of laws affecting an employer’s ability to intercept or block e-mails to or from its employees in both the U.K. and Minnesota.

Why Should Employers Monitor Employee Use of E-mail?

Why should employers care about their employees’ use of e-mail? There are several legitimate reasons why an employer may want to monitor the use of, or intercept, employee e-mails:

- illegal or offensive use of e-mail by an employee could result in potential harassment claims by another employee against the employer, such as for creating a hostile work environment;
- too much time spent by an employee e-mailing for non-business related reasons is likely to result in loss of productivity;
- increased use of an employer’s computer systems for e-mail purposes could make an employer more vulnerable to receiving e-mail viruses, which can cripple networks;
- employees may use e-mail to transmit the employer’s proprietary business information, including trade secrets;

- an employer may be liable as a publisher for defamatory statements sent out on an employer’s e-mail system in the U.S.;¹ and
- employers want to make sure that their investment in office computing is being used effectively, not siphoned off to support employees who overload the system’s communication capacity or “bandwidth”²

There are few employers to which at least one of these reasons would not apply.

Who is Currently Monitoring E-mail Use?

Statistics confirm that, both in the U.K. and in the U.S., companies are busy monitoring e-mail. A survey of employee e-mail and Internet usage among approximately 200 U.K. companies in November and December 2000 found that around 50% of companies admitted to monitoring use “infrequently,” around 20% of companies monitored on a monthly basis,³ and 11% monitored such use on a daily basis.

In the U.S., e-mail monitoring may be even more prevalent. According to a survey of 435 major U.S. firms released by the American Management Association in 2001, approximately 74% of such firms actively monitored all forms of communication and performance, and almost 47% of such firms stored and reviewed e-mail messages.⁴ The Privacy Foundation reports that fourteen million employees in the United States (just over one-third of the online workforce) have their Internet or e-mail use under continuous surveillance at work.⁵ In addition, a poll of corporate chief information officers in the U.S. conducted by CIO magazine found that 17% of the officers conduct sporadic employee e-mail checks, 16% never monitor employee e-mail, 11% check only “problem employees” and 38% check only after there’s been a complaint or productivity issue.⁶

As more employees get “hooked up” to e-mail, more and more companies will have to decide how they intend to monitor e-mail use. All such monitoring must comply with the relevant laws and regulations applicable in each location in which the company has employees.

U.K. Position

In the United Kingdom, companies have been given power to intercept e-mails sent to and by their employees under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (“Regulations”).

These Regulations came into force in October 2000 in response to criticism of the earlier-introduced Regulation of Investigatory Powers Act 2000, which had restricted interceptions to those who had the consent of both the sender and the recipient. E-mails may now be intercepted without consent (for the purpose of monitoring or keeping a record of communications) in order to monitor standards of service, to check that the company’s policies and procedures are being followed, and to help with staff training, among other things. Most importantly, employers can now (without the consent of the employee) intercept e-mails in order to prevent or detect unauthorized use or misuse.

To come within the Regulations, the interception has to be by the employer itself (using its own telecommunications system), or by some other party, with the employer’s consent.⁷ Both employers and third parties may monitor *and* record communications:

- to establish the existence of facts to ascertain compliance with regulatory or self-regulatory practices or procedures, or to ascertain or demonstrate standards that are or ought to be achieved;
- in the interests of national security;
- to prevent or detect crime; or
- to investigate or detect the unauthorised use of telecommunication systems.

The circumstances in which companies may monitor *but not* record communications are as follows:

- communications received in order to determine whether they are business or personal communications; or
- communications made to anonymous telephone help lines.

The Regulations have given companies wide scope for intercepting e-mails, but interceptions will be legitimate only if the controller of the telecommunications system on which they occur has made all reasonable efforts to inform potential users that interceptions may be made. “Reasonable efforts” could be made by employers notifying employees in advance that there is a filtering system in place. This notice may take the form of clauses in employment contracts, company wide e-mail policies, reminders on notice boards, stickers on computers and telephones, and appropriate standard wording on all e-mails sent that such monitoring may take place. The more an employer does in the way of notifying its employees, the more “reasonable” its efforts will likely be deemed.

While the Regulations give companies the broad ability to intercept e-mail, companies must ensure that any intercepting they perform pursuant to the Regulations does not conflict with the relevant employee’s privacy rights under the Data Protection Act 1998. For example, any interception that involves obtaining, recording or otherwise processing personal data by means of automated equipment such as recording of telephone calls or filtering e-mails, will fall within the scope of the Data Protection Act 1998, as will the holding or processing of the personal data after the interception has taken place.

In addition to the Data Protection Act 1998, employers must be aware of the draft code of practice released by the Data Protection Commissioner in October 2000. The draft code governs the use of personal data in employer/employee relationships. It is more favorable to employees than the Regulations because it puts stricter controls on the employer’s ability to monitor employee e-mails. But the draft code has not been finalized or implemented, was drafted before the Regulations came into effect (so the Commissioner may change her stance in light of the Regulations) and is not strictly legally binding, so the Regulations are the rules that govern. However, the code is a suggested code of practice and cannot be ignored by employers.

The draft code suggests that an employer does the following:

- establish the specific business purpose for which the monitoring is to be introduced;
- assess the impact of the monitoring on the privacy, autonomy and other legitimate rights of staff. Do not introduce monitoring in which any adverse impact is out of proportion to the benefits;

- in making this assessment, consult relevant trade unions or other employee representatives;
- record both the business purpose for which the monitoring is to be introduced and the impact assessment behind it;
- if comparable benefits can reasonably be achieved by another method with less adverse impact, adopt the other method;
- focus any monitoring on those areas where it is actually necessary and proportionate to achieving the business purpose. Monitoring of all staff will not be justified if the purpose of the monitoring is to address a risk that is posed only by a few;
- make all staff subject to the monitoring aware that it is taking place and the purpose for which personal information is being collected, unless in exceptional circumstances, such as: (a) the monitoring is behavioral; (b) it is carried out for the purpose of preventing or detecting crime, or for the apprehension or prosecution of offenders; (c) informing staff would likely prejudice this purpose; and (d) the standards outlined by the Commissioner relating to covert monitoring are complied with;
- do not use personal information collected through monitoring for purposes other than those for which the monitoring was introduced and staff were told, unless the information is such that no reasonable employer could ignore it, i.e. it reveals criminal activity or gross misconduct; and
- remember that information collected through monitoring can be misleading, misinterpreted or even deliberately falsified as well as being inaccurate because of equipment malfunction. If the information is to be used in a way that might have an adverse impact on employees, present them with the information and give them an opportunity to challenge or explain it before it is used.

It is assumed that the draft code, once implemented, will no longer conflict with the Regulations. However, this may not be the case. If there are still differences between the code and Regulations after implementation, it will be up to employers to try and interpret the interplay between the code and Regulations until these grey areas are decided by the courts.

MN Position

Companies in Minnesota are subject to both federal and state limitations on intercepting and monitoring e-mails. At the federal level, the Electronic Communications Privacy Act (“ECPA”)⁸ makes intercepting, disclosing

and using electronic communications illegal. At the state level, the Minnesota Privacy of Communications Act (“MPCA”)⁹ also prohibits the interception, disclosure and use of electronic communications under certain circumstances.¹⁰ The MPCA protects communications whether or not they are interstate, foreign or intra-workplace e-mails, whereas the ECPA only protects communications in or affecting interstate or foreign commerce.¹¹ At least one commentator has argued that the effect of this difference in coverage is based upon where the “signal” travels, and how the governing law relates to those travels.¹² For example, a fully internal e-mail system will not be protected under the ECPA, since the “signal” never leaves the employer’s workplace to go through a system “affecting” interstate or foreign commerce, but e-mails received over public networks would likely be protected under the ECPA since that “signal” would have passed through a system that affects interstate or foreign commerce.¹ However, both a fully internal and an external system will be protected under the MPCA since there are no interstate or foreign commerce requirements.¹⁴

Both the ECPA and the MPCA contain exceptions from liability for employers who monitor their employees’ e-mail. The primary exceptions¹⁵ under both statutes are:

- an officer, employee or agent of a provider of a wire or electronic communications service, whose facilities are used in the transmission of a wire or electronic communication¹⁶ may intercept, disclose or use that communication in the normal course of employment while engaged in any activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service.¹⁷ A provider of an “electronic communications service” is a provider of “any service which provides users thereof the ability to send or receive wire or electronic communications . . .”¹⁸ Arguably, an employer that operates its own e-mail service that allows employees to send or receive e-mails would fall within this “provider” exception. Such an employer would have the right to monitor its employees’ use of such e-mail service to engage in quality control checks and perhaps also to prevent excessive use of the e-mail service for personal or non-work related activities.¹⁹ However, if an employer hires an “external” service provider to provide e-mail service to the company and its employees, then such employer may not fall within the “provider” exception (since this is arguably not use of its own facilities), and consequently would have to rely on another exception to intercept, use, or disclose employee e-mails. The precise breadth of the

“provider” exception remains to be tested in the courts.

- a person may intercept an electronic communication where one of the parties to the communication has given prior consent to such interception.²⁰ The statute does not specify whether consent must be express or may be implied. Presumably, consent could be achieved by an employer drafting an e-mail policy and having an employee sign an acknowledgement to such policy.

In addition to the MPCA in Minnesota, the new Internet Consumer Privacy Act (“MICPA”), signed by Minnesota Governor Jesse Ventura on May 22, 2002,²¹ affects e-mails transmitted or received by employees. The less publicized portion of the MICPA, which like the rest of the MICPA is effective on March 1, 2003, gives businesses the right to block certain e-mail messages received or transmitted through such businesses’ service without liability.

MICPA regulates commercial electronic mail messages by prohibiting messages that (a) use a third party’s domain name without permission, (b) contain false routing information, or (c) have a misleading subject line.²² A “commercial electronic mail message” means an e-mail sent through an Internet service provider’s facilities in Minnesota to a resident of Minnesota for promoting the sale or lease of real property, goods or services.²³ Such e-mail messages must contain opt-out instructions and contact information,²⁴ and unsolicited e-mail messages must contain an appropriate label at the beginning of the subject line (either “ADV” or “ADV-ADULT”).²⁵

Under the new law,

[n]o electronic mail service provider may be held liable in an action by a recipient for any act voluntarily taken in good faith to block the receipt or transmission through its service of any commercial electronic mail message that the electronic mail service provider reasonably believes is, or will be, sent in violation of²⁶

the statutory requirements set forth in the preceding paragraph. An “electronic mail service provider” means a business, nonprofit organization, educational institution, library or government entity that enables a set of users to send or receive electronic mail messages via the Internet.²⁷ Thus, under MICPA, any business may block the transmission of commercial e-mail messages sent to a Minnesota resident through facilities in Minnesota, if such business reasonably believes the e-mail has been or will be sent in violation of the new statutory requirements, without being liable to the party that would have

been a recipient. This new ability for companies to block commercial e-mail messages is not subject to any requirement to obtain consent from the employees who would be affected.

While the new MICPA is effectively a spam law, employers can use the blocking rules to stop commercial e-mails from being received or transmitted by employees at least to the extent permitted by the statute. MICPA does not permit “monitoring” as such, but for employers to “block” commercial e-mails that do not comply with the statute, presumably they would have to be monitoring the commercial e-mails in some sense. How MICPA works with MPCA and ECPA in this respect remains to be seen.²⁸

Conclusion

Firms with employees and locations in both, or either, the U.K. and MN should be aware of the permissible and prohibited activities in each country with respect to e-mail use and monitoring. The best practice for employers who wish to monitor employee e-mail is to have an explicit e-mail policy in place covering what will be monitored, and to what extent, so that employees have a “reasonable expectation” as to what is private and what is not. All employees who use e-mail should be aware of their employer’s policy and know that they are expected to follow it. Finally, an employer should also abide by the policy (for instance the scope of monitoring e-mails, if any), and uniformly enforce the policy to ensure its validity. These steps may not immunize the company from any possible action, but by taking them, a company can show that it has made every effort to prevent offending communications from being sent by its employees.

Notes

¹ Mary E. Stumo, et al., *An Employer’s Guide to Controlling Employee’s E-mail and Internet Use*, 19th Annual Upper Midwest Employment Law Seminar MSBA CLE, May 2002.

² *E-mail Privacy*, at <http://www.nolo.com/lawcenter/ency/article.cfm/objectID/286D456E-73C7-414A-B174343E0225C4C8/catID/96A3E6BC-22BC-43EE-BDE2D470B0972A47> (June 10, 2002).

³ *The Uneasy World of E – KLegal Internet Survey*, at <http://www.kpmg.co.uk/kpmg/uk/press/detail.cfm?pr=837> (June 11, 2002)

⁴ 2001 AMA Survey, *Workplace Monitoring & Surveillance: Policies and Practices*, Summary of Key Findings, at http://www.amanet.org/research/pdfs/emsfu_short.pdf (June 11, 2002).

⁵ Andrew Schulman, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use*, at <http://www.sonic.net/~undoc/extent.htm> (May 24, 2002).

⁶ *Id.*.

⁷ Article 3(1) Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000) SI 2000/2699

⁸ Electronic Communications Privacy Act, 18 U.S.C. § 2510 (2000).

⁹ Minn. Stat. §§ 626A.01 – 626A.41 (2000) (Privacy of Communications Act).

¹⁰ There are also other statutory provisions dealing with protection of stored e-mail messages. *See* 18 U.S.C. §§ 2701 (2000); Minn. Stat. §§ 626A.26 (2000).

¹¹ Linda L. Holstein & Karen E. Reilly, *Electronic Communications in the Workplace: New Limits on Employer Surveillance*, *The Hennepin Lawyer*, Jan.-Feb. 1996, at 4, 6.

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.* at 7.

¹⁵ There is another exception for “ordinary course of business,” which will not be discussed in this article.

¹⁶ The ECPA states: “Whose facilities are used in the transmission of a wire *or electronic* communication,” whereas the MPCA states: “Whose facilities are used in the transmission of a wire communication.” The effect of the difference is not clarified in the annotations to the MPCA, and will not be discussed in this article.

¹⁷ 18 U.S.C. § 2511(2)(a)(i) (2000); Minn. Stat. § 626A.02, subd. 2(a) (2000).

¹⁸ 18 U.S.C. § 2510(15) (2000); Minn. Stat. § 626A.01, subd. 17 (2000).

¹⁹ Mark S. Dichter & Michael S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age*, at <http://www.morganlewis.com/art61499.htm> (May 24, 2002).

²⁰ 18 U.S.C. § 2511(2)(d) (2000); Minn. Stat. § 626A.02 subd. 2(d) (2000). But note that even if consent is given, the communication may not be intercepted for the purposes of committing any criminal or tortious act in violation of the constitution or law of the United States or of any state.

²¹ 2002 Minn. Laws ch. 395.

²² *Id.* *See also* <http://www.spamlaws.com/state/mn.html> (June 13, 2002).

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ When monitoring employee e-mails, employers must not forget the employee’s right of privacy. *See Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998) (establishing legal grounds for three types of invasion of privacy torts: intrusion upon seclusion, publication of private facts, and appropriation of name and likeness; declining to recognize a “false light publicity” invasion of privacy tort).

Practicelaw.org — MSBA’s New Online Service. FREE And For Members

MSBA’s newest service, *practicelaw.org* helps members deliver high-quality legal services more efficiently. It uses online technology to deliver the practice tools that lawyers use every day. Those tools include official court forms and rules, templates for legal documents, sample pleadings and discovery, and checklists and reminders, as well as articles, practice tips and advice from experienced practitioners. Because it is online, *practicelaw.org* can hyperlink directly to outside sources, such as cases and statutes — something impossible to do in traditional publications. And being online means that members

do not have to download or install anything; any member with Internet access has instant access to all of *practicelaw.org*. The material in *practicelaw.org* is organized into “FILES,” each covering a specific practice area. Currently there are four files: **family law, employment law, appellate practice, and marketing**. A fifth file contains miscellaneous material that is of value but not comprehensive enough to justify its own file (for example, the **Uniform Conveyancing Blanks**.) Each file is organized into “tabs,” which cover a specific topic in that practice area. Visit the site at www.practicelaw.org and register today!

Bisnes¹ Commercial Overview- Russia and Siberia²

*By: Elena Ovsianikova, attorney and professor of law,
Novosibirsk State University, Russia*

Last year was a relatively good year for Russia's business environment. Russia has now passed through the first phase of the economic transformation process, as a basic market environment has been created and macroeconomic stability has been achieved. These achievements have been made because the main institutions required in a market economy are now established in Russia, and most business entities operate on the basis of business drivers and signals that are typical of a market environment.

Russia

Last year, substantial progress was made in improving legislation governing economic, business, and investment activity. New laws have been introduced with regard to the taxation of corporate income, and new Labor and Land Codes have been adopted, with special attention being made to legislating the private business sector.

The adoption of the Land Code in 2001 was a major political achievement for Russia, and provided a significant step to a market economy. The Land Code represents a significant reform in Russian law, specifically because of the encouragement that the Code gives to the creation of private ownership rights to land. Rights to land may now be held by the state, municipalities, private individuals, or legal entities. Foreign individuals and legal entities are treated equally to Russian individuals and legal entities under the new Code. The adoption of the new Labor Code in 2002 represents a departure from old Russian law in the regulation of labor relations, because the Code creates a legal basis for balancing the interests of all parties in labor relations.

Other notable adoptions in business/commercial law in 2001 include the adoption of laws governing investment funds, joint stock companies, and digital electronic signatures. The adoption of these laws is important to Russia's business climate, for the reasons described below. Finally, although it has not yet been adopted, it

should be noted that the Russian government has recently given its broad approval to the new text of the law governing insolvency (bankruptcy).

Russian legislation saw a number of substantial, liberal changes over the last few years. These new laws are creating the conditions needed to consolidate and develop a market economy that business institutions need to improve the investment and business climate in Russia. The Russian government is aiding Russia's emergence into the global market by striving to harmonize federal law with international law.

Siberia

Siberia, which is actually three-quarters of Russia's total territory, is playing an important role in creating a comfortable business environment for foreign investors. Siberia is in a unique location in Russia: the region creates a "bridge" between the East and West, as well as the North and South. It is now the main supplier of Russian oil, both domestically and abroad. In addition to its vast mineral holdings, Siberia is one of the most important forest zones on the planet: more than 40 million cubic meters of industrial and carving wood are produced from Siberia annually.

Novosibirsk, the capital of Siberia and the sister-city of Minneapolis/St. Paul, is Russia's third largest city. It represents one of the most important commercial centers outside of European Russia, as it is a major scientific, business, and industrial city. The desirability of the marketplace is perhaps best demonstrated by the presence of so many foreign companies' sales and representative offices. International business partnerships connect the capital of Siberia with 85 countries, including the United States, France, Italy, Germany, and Japan.

Novosibirsk State University in Akademgorodok, with 5,000 students and a workforce of 15,000 scientists and researchers, is called Siberia's "Silicon Valley" because

of its high concentration of intelligence and software companies: many talented programmers and software companies are based in this area. The programmers and companies are involved in the offshore programming business that has been developing in Russia. This high concentration of high-quality programmers, mathematicians, economists, and lawyers fostered by the University, as well as low labor costs, have created lucrative opportunities for foreign companies. For example, huge Novosibirsk corporations, such as Unipro, Intech, and Compania de Ventyra have been very successful doing international business in Novosibirsk.

With the changes in the law and the attraction of many large businesses to the area, Russia is standing at a new crossroads in her destiny.

Notes

¹ There are two Russian translations of the English word “Business”: the first is the word “delo,” which means business in the social sense of the word. The second translation, and the one used here, is the word “bisnis,” which is used in the context of commerce.

² Ms. Ovsianikova’s article is based on her presentation to the International Business Law section on April 5, 2002.

www.probono.net/mn/civil

Minnesota Lawyers Serving the Public Good

Join a virtual legal community of advocates serving the public interest. This site provides Minnesota volunteers with instant desktop access to an up-to-date online library of training materials, model pleadings, forms and links that can be downloaded and printed easily; interactive news and calendar pages with informative articles, important events, CLE courses; and postings of new volunteer opportunities for lawyers and law students. Minnesota lawyers volunteering with Minnesota Advocates for Human Rights or handling death penalty cases are also eligible for the Asylum and Death Penalty practice areas respectively. Find pro bono cases that need immediate volunteers in family law, housing, benefits, and other areas.

Jolie Lahlum, an MSBA member, says: “I was delighted to find the resources in the [probono.net/mn Civil Law](http://www.probono.net/mn/CivilLaw) library. The sample divorce documents were extremely valuable and enabled me to provide competent legal services on my first pro bono case. Probono.net is a wonderful resource.”

Go to www.probono.net/mn/civil today and join.

2002-2003 International Business Law Section Council



Paula R. Johnson, *Chair*
Jostens, Inc.
5501 Norman Center Drive
Minneapolis, MN 55437
(952) 830-3309
(952) 830-3293 Fax
paula.johnson@jostens.com

Diane C. Miller Esch, *Vice-Chair*
The Pillsbury Company
200 S. 6th Street, MS 3726
Minneapolis, MN 55402
(612) 317-1447
(612) 330-8893 Fax
dmiller@pillsbury.com

Susanne I. Haas, *Secretary*
Honeywell International, Inc.
MN10-2480
1985 Douglas Drive N.
Golden Valley, MN 55422
(763) 954-5387
(763) 954-5390 Fax
susanne.i.haas@honeywell.com

Mark S. McNeil, *Treasurer*
Lindquist & Vennum, PLLP
80 S. Eighth Street, #4200
(612) 371-2473
(612) 371-3207
mmcneil@lindquist.com

Patrick J. Kelly, *Past Chair*
Fredrikson & Byron
200 S. Sixth Street, #4000
Minneapolis MN 55402-1425
(612) 492-7040
(612) 492-7077 Fax
pkelly@fredlaw.com

Charles B. Barry
Artesyn North America Inc.
7575 Market Place Drive
Eden Prairie, MN 55344
(952) 392-6597
(952) 392-6677 Fax
charles.barry@artesyn.com

Scott M. Borene
Borene Law Firm, PA
Immigration Law group
80 S. Eighth Street, #4602
Minneapolis, MN 55402
sborene@borene.com

Edward J. Hayward
Oppenheimer Wolff & Donnelly
45 S. Seventh St. #3300
Minneapolis MN 55402-1609
(612) 607-7280
(612) 607-7100 Fax
ehayward@owdlaw.com

David F. Fisher
5047 Gladstone Ave. S.
Minneapolis MN 55419
(651) 296-1424
(651) 297-7909 Fax
david.fisher@state.mn.us

Alain Frecon
Frecon Law Office
150 S. Fifth St. #2300
Minneapolis MN 55402-4223
(612) 338-6868
(612) 338-6878 Fax
afrecon@aol.com

Mary K. McCormick
McCormick International
10808 Glen Wilding Lane
Bloomington, MN 55431
(952) 884-6408
(952) 948-0658 Fax
marymcc@pclink.com

James F. Pedersen
Dorsey & Whitney
220 S. 6th Street, #1700
Minneapolis, MN 55402
(612) 340-7894
(612) 340-8827 Fax
pedersen.james@dorseylaw.com

Richard Y. Sako
5501 River Bluff Drive
Bloomington, MN 55437
(612) 766-7915
(612) 766-1600 Fax
RSako@faegre.com

Prof. Anthony S. Winer
Wm. Mitchell College of Law
875 Summit Ave.
St. Paul MN 55105-3076
(651) 290-6365
(651) 290-6414 Fax
awiner@wmitchell.edu

From the Editor

By: Jennifer Kalvestran, Meagher & Geer, PLLP

I would like to express my gratitude and appreciation to those who contributed to this edition of *International Business Law News*. I am interested in working with other members of the section. Please contact me if you would like to contribute an article to a future edition of the newsletter, or if you have any comments about this edition of the newsletter. I can be reached at:

Jennifer Kalvestran
Meagher & Geer, PLLP
33 S. 6th Street, #4200
Minneapolis, MN 55402
612/371-1315
jkalvestran@meagher.com

Thank you!

Jennifer Kalvestran