McGREGOR STILLMAN'S

LegalEye

PRO POSSE SUO

VOL 3, No.1

SPRING 1999
SPECIAL EDITION

Presenting Legal News, Views and Updates from
McGregor Stillman - Avocats
Barristers & Solicitors

HEADS UP

Heads Up is a column which appears in each issue of the McGregor Stillman Legaleye, highlighting new or proposed legislation in the Province of Alberta.

Y2K: SOME LEGAL ISSUES

The following paper was originally presented at the Legal Education Society of Alberta seminar "Year 2000: The Legal Issues" in December, 1998. It is merely an overview and is not intended to be a definitive legal opinion on any of the topics included. The excerpted article is reprinted here with permission from L.E.S.A. and by the kind permission of its author, James A.T. Swanson.

It would do no good to describe the Y2K problem, as it has been defined, discussed, and debated at nauseam. This article will discuss some of the various problems which may arise from the Y2K problem only, rather than attempting to trace its history.

1. Where is the Bug?

In some cases the problem is not at the software level. Hardware may be incapable of using or updating a date in the year 2000 or beyond. Many computers still in use today will be affected by this. With any particular system the problem may originate at any level. It can be in the hardware, or at the operating system level, with the programming or language tool that a program was written in, or with what is know as *middleware*, designed to handle data and programs for other purposes, or within a specific application. A system that is affected at any level by difficulties with the date can be rendered useless since the date is something that is used by all levels.

Common examples include:

a) Hardware
Computers, monitors, scanners, printers and other accessories which contain one or more date-dependent chips, primarily either a chip called the BIOS (Basic Input/Output System) and another called the RTC (Real Time Clock).

This also includes mainframes, mini and personal computers, network servers, application servers, file servers, print servers, web servers, lap-tops and notebooks, etc.

b) Software
Programs, applications and computer codes that process date.

c) Automated systems
Examples include embedded chips (also known as firmware) and programmable controllers in buildings, factories, trains, airplanes, power and other utility plants, including such things and devices as:

elevators
pacemakers
satellites
telephone systems
fax machines
automated tellers
fire-protect systems
valve operators
security systems and bank vaults
point-of-sales equipment
equipment maintenance systems
programmable logic controllers
air traffic control systems
global positioning systems
some automobiles
oil rigs
heating/ventilation/air-conditioning systems
all sorts of programmable controllers, which have replaced mechanical relays in virtually all electricity generating plants and control rooms.

d) Data Files
Many of these currently in existence will have problems, even if they are on compliant systems. The difficulties can result from their origin on earlier software which was not compliant.

207, 10335 - 172 Street, Edmonton, Alberta, Canada T5S 1K9 Telephone: (780) 484-4445 Fax: (780) 484-4184 E-mail: mcgregor@mcgregorstillman.com

If imported or communicated from outside your business or organization through floppy disks, modem, network or Internet connections, these can play havoc with otherwise compliant systems. Inventory can have a dynamic nature: new macros, files off the internet, etc. - all of these can take a system back out of compliance.

All four of the above may freeze up, crash, behave badly or give out erroneous data if they are not Y2K ready and compliant. Erroneous data may appear on the surface to be accurate, and may be relied on for months or years before the errors are noticed.

2. What can be done?

Older chips may not have available replacements. The technology to reprogram the chips by rewriting the proprietary language used may be obsolete and no longer available. Programmers who have the knowledge and skills to do so are rare.

It is also estimated that for every 6 lines of code written, Y2K programmers will make one new mistake. Therefore, the real deadline may be earlier.

There are only five options as to how to deal with the problem:

a) Repair
b) Replace
c) Retire
d) Re-engineer, so it doesn't have date sensitive functions
e) Do nothing

Only the first two are preferable and the fifth one is not viable in most cases at all.

3. Year 2000 Compliant?

There is no one definition of Year 2000 compliant.

"Year 2000 compliant" is used in this paper to mean systems that will continue to function normally, accurately and dependably after January 1, 2000, with no issues that they did not have before that date.

Compliance has to include the fact that the year 2000 is a leap year.

In all cases with existing systems, it is necessary to check out the fine print. Many programs will function after the year 2000, but only up to 2020 or 2038. There may also be issues with date format: d/m/y, y/m/d, etc.

Computers and other systems use dates in a great many ways - for financial transactions, billing and paying, to process claims, to operate utilities and telecommunications, scheduling and process control systems, reservation systems on airlines and hotels, and so on. Failure can lead to miscalculations, crashes, rejection of valid transactions and claims, overpayments, underpayments, non-payments, premature expiration of things like credit cards, prescriptions, licenses, permits, etc., and the list is endless.

4. What's at risk?

Smaller businesses are likely safer internally than large - they use OTC software and fewer custom applications, but they still are only links in a supply chain.

5. The Legal Consequences

Y2K litigation is not a 21st Century phenomenon; it has already started.

For example:

The Edmonton Journal edition for September 9, 1998 reported that at least 16 suits had already been filed in the U.S., six of which name Intuit, known for its Quicken financial product, as a defendant.

Arthur Andersen, the global accounting and consulting giant, is in litigation in Massachusetts seeking a declaratory judgment on threats to sue over a system purchased in 1990 and 1991.

6. Specific Areas of Legal Concern and Potential Liability

Primary areas of potential liability that need to be considered by any organization or business include (note that these categories overlap):

a) Contract

Are current suppliers going to be able to deliver what you need or will they fail to do so because their systems fail? *Remember that suppliers can include those as fundamental as the electricity or water supply and the phone company.*

If suppliers are hardware or software providers, are their products and services Year 2000 complaint?

If customers suffer systems failure or breach of contract from other suppliers so that their businesses falter or fail, will accounts receivable with such customers be collected?

Are there sufficient contractual representations, indemnities, warranties and obligations in agreements with suppliers to provide a remedy should they fail? *Have those agreements and contracts even been reviewed?*

Will the organization be able to deliver what it has promised to deliver? Will failure to do so, whether due to system failure within the organization or within a supplier, lead to being sued?

Will systems and operations be functioning after January 1, 2000? If so, will they be functioning so that they are accurate and dependable?

Do contracts and agreements with customers leave you open to lawsuits should you fail to deliver, whether or not it is your fault? Note that many companies in the US are reportedly invoking the rule in *Hadley v. Baxendale* by giving notice of particular and specific damages that will result from any breach of contract.

If the organization is a Y2K solution provider or consultant, is it doing so in a proper, cautious and complete manner? *Re-writing code can be dangerous - bugs are inevitable, particularly where done in a hurry. The cure may be worse than the disease.*

If managing other peoples' money, has the organization invested prudently in organizations that are Year 2000 compliant or otherwise less exposed to the possible costs and liabilities. Will the systems of the organization fail and cause financial loss to investors?

Has there been a breach of warranty, including the warranties of fitness for the purpose and merchantable quality in the Sale of Goods Act?

What representations have been made in advertising or manuals?

Express and Implied warranties, as well as limitations on liability will have to be considered.

b) **Tort (Civil Wrongs) Analysis**
Was it known, or will it be held that it ought to have been known, that suppliers or the organization's own systems were going to fail?

Will either non-performance by suppliers or systems failure cause the organization to cause harm to others?

Will machinery fail or polluting substances escape into the environment, and will the organization be found at fault?

Will failure of systems or those of a supplier cause harm to members of the public in general?

Will someone be injured or be killed due to a failure, or suffer some sort of financial loss?

If little or nothing has been done about the problem, why not? *Have you acted reasonably? Can you show diligence where required?*

If a plan to remedy the problem has been implemented, was the plan sufficient? *Was it executed properly and in a timely fashion?*

Were good management practices followed?

Were the right suppliers and advisors chosen and did you get the right advice?

Was it decided that it was too late to act, and nothing was done, and will it be shown that something could still have been done?

Have all reasonable steps been taken to remedy or avoid any problems that may occur, including but not limited to re-programming or replacing your systems?

Have there been negligent or intentional misstatements?

Were appropriate steps taken to keep remediated systems clean from re-infection?

c) **Employment**
If systems fail, or the organization is shut down by the failure of a supplier, will it still be able to meet the payroll and pay the withholdings to Revenue Canada required by law?

Will the organization be sued for wrongful dismissal if it can't give a reasonable notice of work no longer being available?

d) **Fiduciary Duties - Liability of Officers and Directors:**
Has full disclosure of all material facts and any potential problems been made to business partners, particularly "silent" partners?

Has full disclosure been made to shareholders, lenders and investors in the organization of all material facts and any potential Year 2000 Problems?

Have sufficiently skilled people been hired and has proper advice been sought out to assist the organization in dealing with Y2K? *Has it done so in a timely fashion?*

Has the organization taken all reasonable steps to have appropriate indemnities, warranties, representations and agreements with suppliers?

Has the organization taken all reasonable steps to avoid as much as possible exposure to claims by customers and others outside the business that may be affected by failure of its systems or those of suppliers?

Has the organization chosen compliant suppliers? *Has it taken reasonable steps to find alternates where suppliers cannot make the necessary assurances of compliance?*

If the company is a public company, has proper disclosure of the potential effects of the Year 2000 problem been made?

Has the extent of the problem been underestimated or misrepresented?

Will lenders terminate arrangements or call loans because the organization has not properly dealt with the problem?

Has senior management done enough to remediate the organization's systems and to avoid liability to third parties by selecting compliant suppliers and protecting the organization with sufficient warranties, etc.?

Senior management may actually be under a duty to bring litigation for any damages suffered due to the fault of others. There may be pressure on them to litigate.

e) **Insurance**
Is there insurance coverage for the Year 2000 problem or its consequences? **(This cannot be taken for granted and there may well be no coverage since this is a man-made problem).**

Is special coverage required, and is it available at any reasonable cost? If such coverage, if available, is not obtained, will management or the organization be sued and found liable? If such a suit causes an organization to fail will shareholders, investors, etc. then sue the organization and its management?

f) **Infringement:**
If suppliers of systems software and hardware are re-programming or changing systems to make them Year 2000 compliant, are they doing so with proper legal authority from the original supplier, or are they infringing copyright in the computer code?

g) **Criminal Liability:**
Will there be found to be criminal fraud in the representations made by systems vendors?

Will there be criminal negligence found where suppliers of technology products have delivered a non-compliant product which causes injury or death?

h) **Regulatory Liability:**
What should be disclosed with respect to compliance?

Do financial costs associated with Year 2000 problems create regulatory compliance issues in the preparation of audited financial statements?

Have regulations been breached?

i) **Mergers and Acquisitions:**
What due diligence and other measures should be taken in current and contemplated M&A transactions to protect against inheriting Year 2000 problems or compounding existing ones?

j) **Protection of Trade Secrets and Intellectual Property:**
Year 2000 compliance may require inter-company access to information that is sensitive and proprietary. How will intellectual property be protected and how will needed access to the information of others be obtained?

Trade secrets may be discovered improperly while trying to repair or rewrite code and programs.

k) **Litigation:**
How will internal documentation being generated now affect the chances in court in the future?

What steps need to be taken to head off litigation and at the same time prepare for it?

l) **Finance:**
If an organization is financing on the security of its accounts receivable, will the failure of its customers have a domino effect, leading to lenders calling in loans and financing?

Can the organization safely provide representations as to Y2K compliance to lenders and investors?

m) **Legislative:**
Is there applicable legislation (e.g. the Sale of Goods Act, mentioned above?)

n) **Jurisdiction:**
Which jurisdiction's law will apply? For example, there will be situations where software licences expressly require attornment to the law of California, but the supplier is incorporated in Delaware, the retailer or value-added reseller in British Columbia, and the end user in Alberta.

There will likely be many class actions filed in favourable jurisdictions.

o) **Choice of Parties to Sue:**
Many situations will involve several parties along the supply chain. If a supplier, partner or customer has a Y2K problem, it's likely that lawsuits will move like dominos up or down to others on the chain.

Possible plaintiffs include any business with losses or business interruptions, any business which is sued (third party notices or counterclaims), Directors and Officers of a company sued, Insurers (including subrogated claims) and injured members of the public.

7. Conclusion

We hope that this brief overview will have assisted you in understanding the technological basis for the Year 2000's potential legal problems, and the main legal issues that arise out of them, both presently and into the future.

For more a more in depth discussion of the issues, and possible ways of planning, please contact any of the lawyers at McGregor Stillman.

McGREGOR STILLMAN

Barristers and Solicitors

#207, 10335 - 172 Street
Edmonton, Alberta, Canada
T5S 1K9

Telephone: (780) 484-4445
Facsimile: (780) 484-4184
E-mail: mcgregor@mcgregorstillman.com

The law firm of McGregor Stillman is a four lawyer general law firm, with emphasis on Civil Litigation, Corporate and Commercial matters, Real Estate, and Wills and Estates. The firm has represented clients throughout Alberta, and has also represented clients from British Columbia, Saskatchewan, Manitoba, Yukon, Northwest Territories and Ontario. The firm has a well established network of agent connections in Canada, including Vancouver, Calgary, Regina, Saskatoon, Winnipeg, and Toronto and environs. The firm has an affiliation with Goodman, Lister & Peters of Detroit, Michigan. McGregor Stillman also has established contacts with various other law firms throughout the United States and Great Britain.

The firm's partners are
TERRY M. McGREGOR
and I. MARK STILLMAN
The firm's associates are
JOHN P. POIRIER and
TERRY J. THOMAS