8. The Year 2000 Bug

Congress should

- be forthright in making the public aware of the scope of the problem;
- amend federal court rules to keep class action suits out of state courts;
- allow private companies to carry first-class mail in competition with the U.S. Postal Service; and
- impose strict time limits on any emergency measures, particularly those that strain constitutional limits.

The year 2000 ''bug'' (Y2K) stems from the inability of some computers, software, and embedded chips to process dates after December 31, 1999. In addition to raising difficult technical and business-planning issues, Y2K also raises some larger policy issues. What should government do as the final date approaches, and afterwards? Clearly, the Y2K problem cannot be legislated away. The best that lawmakers can do may be to avoid making the situation worse.

To Prevent Panic, Tell the Truth

Because of the complexity of the economic and technical issues involved, it will remain unclear whether Y2K is anything to panic about until the millennium. Experts have gathered considerable evidence that Y2K could disrupt banking, transportation, electric power generation, manufacturing, and health care. Skeptics can show very little evidence to rebut the claim that Y2K disruptions will be widespread, serious, and expensive. The view that the concern about Y2K has been cooked up by consultants and lawyers to make money is not evidence; it is speculation.

Some recent news is encouraging. Wall Street's test of financial transactions in August 1998 showed that more than 90 percent of securities trades

could be made (provided that the power stays on). But problems remain at the interfaces between different companies' systems. And for every item of good news, there is bad news—a recent report that electric utilities lag behind in their preparations, and reports of noncompliant dialysis machines, diabetic testing devices, and security systems, among many other examples. Lawmakers should review and consider the available evidence on Y2K. No one should rely on hopes, speculation, intuitions, or uninformed guesses.

Alerting the public to the issue early is the key to preventing last-minute public panic. U.S. citizens are not sheep; they are adults with the right to make decisions affecting the well-being of their families. Government officials and lawmakers can serve the public best by sharing their best estimates of the overall impact of Y2K early on. No one is likely to panic if he knows what to expect.

At least one pundit has suggested that public panic will be more disruptive than the actual Y2K problem itself. On this theory, one might downplay the need to plan for Y2K. But note the underlying premise: that Y2K problems in themselves will not be especially disruptive. There is substantial evidence that this view is wrong. One would not silence weather broadcasts in the face of an oncoming storm, ''because they might cause a panic.''

A Run on Banks?

One harmful public reaction would be a run on banks due to the belief that checks and credit card transactions will not be processed after 1999. That is possible but unlikely, as there should be no reason that many individuals will form this belief all at the same time. The best way to prevent a potential liquidity crisis is contingency planning. For example, if the Internal Revenue Service will not be able to process refund checks, can taxpayers use an alternative method to receive payment? If the power is out in some regions, how will banks maintain communications? How can banks that fear running short of cash amend their contracts with customers to reduce the risk of runs?

A Bad Idea: Guaranteeing Loans to Small Business (S. 2372)

Many small and midsized businesses lack the time or resources to complete Y2K testing before 2000. Extending federal loan guarantees to businesses, as proposed by S. 2372, would be a disaster. The World Bank and the Inter-American Development Bank have also considered loans to

help some small countries address Y2K. Such loan programs are a bad idea. The likelihood of the loans' never being repaid is extraordinarily high.

If a small business cannot satisfy private-sector financiers that it is a good credit risk, taxpayers should not be asked to bear the risk that it will not be Y2K compliant. In many cases, the best decision that businesses can make will be to simply go out of business. Accepting that painful reality is the right thing to do; business risk should be borne by proprietors, not by taxpayers. Every business closure will create an opportunity for a new business.

Dealing with the Flood of Lawsuits

Y2K will become the occasion for many lawsuits to be played out in an already distorted and wasteful tort system. Types of Y2K litigation might include (1) consumer vs. business, (2) business vs. supplier, (3) business vs. insurance company, and (4) shareholders vs. management, among others.

General tort reform measures addressing the abuse of punitive damages, contingency fees, and joint and several liability and adoption of the ''loser pays'' rule would have forestalled much of the current alarm over Y2K lawsuits. But tort reform is the responsibility of state governments, not Congress. And it is too late to undertake a general program of tort reform.

Lawmakers should not be overprotective of negligence. People should have a right to sue when they have been injured by another's breach of contract or carelessness. Depriving people of that right, under some circumstances, might constitute an unconstitutional ''taking'' under the Fifth Amendment. Lawmakers will be tempted to grease the most squeaky wheels—that is, to pass legislation protecting the loudest complainants from litigation. But that will often be a mistake.

Common sense will check some Y2K litigation. Software Productivity Research, Inc., estimates potential global Y2K litigation expenses at $300 billion, but other estimates put the figure for non-litigation-related Y2K fixes at $600 billion worldwide. Resources will be scarce; businesses with a right to litigate will not necessarily do so. Their first priority for scarce resources will be to continue serving customers and fix the infrastructure, not pay expensive lawyers. Businesses value long-term relationships with suppliers, retailers, and customers. Most lawsuits between businesses never see the inside of a courtroom. Because of distortions in the tort system, however, some problems remain. Some proposals for addressing potential lawyer meltdown are discussed next.

Limit Class Action Suits

One positive step would be to amend Federal Rule of Civil Procedure no. 23 to confine class action suits to federal courts. As of this writing, many of the 18 Y2K lawsuits filed thus far are class action suits of large classes of customers against businesses, almost all filed in state courts.

In many state courts, judges certify large classes of individuals with little regard to whether the plaintiffs are indeed similarly situated. Defendants then settle the actions by offering trivial benefits to the members of the class and millions in fees for participating attorneys. Reforming Rule 23 would stop such wasteful litigation from going forward in Y2K cases and others.

That would greatly help to sort justified from unjustified Y2K lawsuits. An International Data Corporation survey of 500 executives in 1996 found that most anticipate more Y2K litigation from consumers than from other businesses. Consumers have as much right to sue as anybody—but there is no need to support class actions that use consumers as token representatives and are nothing more than a money mill for lawyers (see Chapter 29).

Reject Safe Harbors for Information Disclosure

The thesis behind bills such as the Year 2000 Information Disclosure Act (see H.R. 4455, H.R. 4355, and S. 2392) is that Y2K compliance efforts are stymied by

1. companies' reluctance to disclose Y2K problems with specific products, or with company systems, for fear the disclosure will become evidence in lawsuits;
2. consumers' reluctance to name specific noncompliant products uncovered in testing, for fear of defamation suits by the products' makers; and
3. fears that consumers, Web site hosts, or sponsors of other forums will be liable for statements about the Y2K problem on which others choose to rely.

The Year 2000 Information Disclosure Act raises the bar to litigation in such cases by allowing the suits to go forward against grossly negligent statements (or, in the case of H.R. 4455, against fraudulent statements), but not against simple negligence. On its face, that is a simple and conservative measure, but it bears a closer look. First, is it right to shield vendors or anyone else from liability for negligent statements?

Second, in case 1, are the companies that support the measure mistaken about the nature of the danger of the liability they face? Either their products are Y2K compliant, or they are not. If they are not, the companies will face litigation from aggrieved customers, and the facts will come to light one way or another. Indeed, failure to disclose may in itself be grounds for liability. Many companies have been forthright with their customers, suppliers, and others about the Y2K status of their products and operations. Evidently, the fear of disclosure is not universal, and it may be unfounded.

Second, in situation 2, it seems unlikely that consumers or Web sites would be liable for defamation if they truthfully reported their experience with a certain product. Situation 3 is more problematic. If tort law were consistent with common sense, speakers would not be held liable if others choose to rely on a stranger's anecdotes in a public forum. The Y2K situation is so complex that such reliance would rarely be anything but reckless stupidity. But our distorted tort system might conceivably allow an award in this case, under rules of contributory negligence.

But this is not an argument for legislation shielding negligence to encourage more disclosures. More information sharing might be helpful in addressing Y2K—but it may not be of substantial help and may cause harm in some cases. Complex information technology systems are more than a bunch of different products hooked together; Company A may use many of the same products as Company B, but if the systems are configured or used differently, Company B may meet with a disaster if it chooses to rely on Company A's testing experience. Test reports from hospitals indicate that even stand-alone products, produced by the same manufacturer and apparently identical, may differ: some products may be compliant and others not. The hospitals must record equipment as compliant or noncompliant serial number by serial number. Manufacturers are often not the best source of information about a given product used in a particular way. Perhaps the most important tenet of Y2K compliance is that companies must test every component of their own systems and conduct joint testing with key suppliers. Reliance on third-party anecdotes or letters of compliance should not necessarily be encouraged.

Reject Safe Harbors for ''Good Faith'' Compliance Efforts (H.R. 4240 and similar proposals)

Most ''safe harbor'' legislation proposed so far would protect the software industry from punitive damages or pain and suffering awards (allow-

ing recovery of economic damages only) if the company (a) discloses noncompliant products to known buyers and (b) offers a free repair. H.R. 4240 also offers businesses generally a safe harbor for making ''reasonable efforts'' and completing testing and notification by a certain date. A financial industry representative testified before Congress that a bank should be able to win a safe harbor from punitive damages by passing a year 2000 compliance audit conducted by the Comptroller of the Currency. Congress should reject such proposals.

Strange as our rules of tort law sometimes are, they and the precedents associated with them are familiar to a wide body of lawyers and judges. Federal statutory liability limits drafted in haste will cause more problems than they resolve. Instead of litigation and proposals for settlement centering on familiar determinations of negligence, the litigation would instead focus on unfamiliar new questions of whether and how the safe harbor applies. For example, what efforts are ''reasonable''?

Here is a sampling of other issues:

- Is the liability limit an unconstitutional ''taking'' of private property (most likely if the limit bars recovery for economic losses as well as punitive damages)?
- If testing by a certain date is satisfactory, how should the date be chosen? Perhaps any date in 1999 is already too late.
- Do ''good faith'' measures demand that a software company offer a free patch to software? What does this do to companies' profit incentive to develop and promote a successful patch?
- Suppose ''good faith'' measures demand that a company participate in a government-sponsored Y2K certification plan. Is the government competent to conduct such a plan?

The difficulty of answering those questions suggests that piecemeal liability limits and safe harbors are not a satisfactory solution.

Government Systems' Compliance

As of this writing, many government departments and agencies lag behind the private sector in reaching Y2K compliance. Those lagging behind include the Department of Defense and the Department of the Treasury.

For many agencies, it is too late; testing for and fixing Y2K take time, money, and careful, quality programming. Those resources are now very scarce. The federal government should focus its resources on bringing the

systems of departments that perform *core constitutional functions*, such as the Department of Defense, into compliance and on developing contingency plans *even for those core agencies that may be ready in time*. It makes little sense, however, to give scarce resources to agencies of suspect constitutional status or dubious importance, such as the Department of Commerce or the Department of Agriculture.

In considering the progress of core agencies toward compliance, be aware of reporting gimmicks that convey a false sense of security. For example, while an agency may report that 30 percent of its ''mission-critical'' systems have been fixed, that is meaningless unless one knows how the agency has determined that a system is ''mission critical.''

One measure can easily be taken quickly to ensure that mail delivery continues after 2000. The statutes granting the U.S. Postal Service a monopoly on nonurgent mail delivery should immediately be repealed. As of this writing, little reliable information is available about the Y2K compliance status of the USPS. However, the complexity of the task it faces is enormous, given the size of its operations; in addition, it got a late start. Continuation of the USPS's monopoly might be devastating, preventing the private sector from helping itself.

Emergency Measures

Contingency plans for Y2K being formulated in the United States, Canada, and other countries include an active role for the military. Soldiers may be called upon to help local police keep order or to maintain other key services. A survey in the summer of 1998 of government and industry managers working on Y2K compliance issues reports that 10 percent are preparing for martial law. Current Y2K hearings have repeatedly invoked the possible need for martial law.

The Constitution of the United States does not grant a power to the federal government to claim emergency powers or to declare martial law. In thinking about contingency planning for Y2K, lawmakers should remember the importance of preserving a free society. While the military may be called in to perform public functions in a true emergency, Y2K does not justify the suspension of the right to due process or private property rights.

Any emergency measures that call for the military to perform functions normally reserved for civil and elected authorities should be strictly limited in time and scope. Such measures should be drafted so that they cease to

be effective as of a certain date, a date that cannot be extended by a mere rubber stamp.

Recommended Reading

McCullagh, Declan. ''Don't Sue Me! Corporations Lobby for Y2K Liability.'' http://cgi.pathfinder.com/netly/article/0,2334,14414,00.hmtl.

_____. ''Y2K Is Showcasing the Government's Worst Instincts.'' http://cgi.pathfinder.com/netly/article/10,2234,14396,00.html.

Munro, Neil. ''The Big Glitch.'' *National Journal*, June 20, 1998.

Schonbrun, Lawrence W. ''The Class Action Con Game.'' *Regulation* 20, no. 4 (1997).

Zerega, Blaise. ''The Big Blackout.'' *InfoWorld*, September 7, 1998.

—Prepared by Solveig Singleton