WHY Y2K?: CHALLENGES FOR THE COMMUNICATIONS INDUSTRY

Michael K. Powell*

I. INTRODUCTION

The imminent approach of the new millennium is triggering much speculation about what our collective future holds. Much of the speculation stems from the fact that we, as a nation and a global community, have experienced a very profound change in our daily lives over a relatively short period of time. In fact, on the heels of the 1900s-a century of unparalleled growth and advancement in technology, medicine, democracy, and diplomacy, punctuated with sporadic episodes of war and decline-there is a palpable sense of heightened wonderment and anxiety about what we can expect from the next century, the benefits and forward-progress we will enjoy, the responsibilities and duties we will shoulder, and the perils we must avoid or overcome.

The twentieth century will certainly be remembered as a period of recorded history that was nearly unrivaled and was, at once, "inspiring, at times horrifying, always fascinating."[1] As we approach the conclusion of the millennium, we find ourselves standing at the leading edge of a new, wondrous and transforming economic moment (the so-called Digital Information Age), equal in its importance to that of the agricultural and industrial revolutions. In the words of Alvin Toffler, we are now riding the "Third Wave."[2] This economic revolution, similar to those that preceded it, is being fueled by dramatic advances in technology. Technology is evolving at a blinding rate and appears hell-bent to change every facet of our lives.[3] It undoubtedly will, and the potential for that is exciting.

Consider, for example, the accelerating pervasiveness and transparency of technology, from mainframes to personal computers to powerful software applications and embedded microprocessors, without which there would be none of the innovative services and products that many of us take for granted. Also consider that the typical American household now has more computer processing power than the entire Massa-

---

* Michael K. Powell is a Commissioner on the Federal Communications Commission and the agency's representative on the President's Council on Year 2000 Conversion. This article was completed with the invaluable assistance of Paul A. Jackson, Special Assistant to the Commissioner.

1 *See* Walter Isaacson, *Our Century … And The Next One*, TIME, Apr. 13, 1998, at 70.

2 *See* Alvin Toffler, THE THIRD WAVE 1 (1991).

3 Moore's Law, which holds that the maximum processing power of a microchip, at a given price, doubles roughly every

chusetts Institute of Technology (one of the U.S. educational institutions that pioneered computer and information sciences) did twenty years ago.[4]

Engineers and technologists are creating machines every day that are smarter, faster and increasingly untethered, while their software design and programming counterparts are creating more powerful and automated applications and systems. The future of computerization, as a consequence, will be characterized by powerful software applications and tiny embedded microprocessors burrowing themselves into our daily lives. These machines and systems (no longer clumsy and intrusive like personal computers) will be invisible to the human eye and will be tremendously autonomous and intelligent. They will mimic and access all of our senses, making the human-computer experience of the future radically different from today's. Ultimately, technology will allow us to evolve from using just our touch to manipulate the keyboard and our sight to interact with the monitor to the use of all our five senses.[5] The possibilities are vast, only limited by physical time (*i.e.*, the speed of light) and biological time (*i.e.*, the span of life).[6]

Through the use of advanced technology (namely telecommunications and information services), we are also shrinking the world. Technology has opened, and will continue to open, various industries-communications, data and information services, entertainment, software, electronics, and financial services-to new global consumption, trade and investment. Ultimately, technology will contribute to the complete interconnectedness of the entire global community.

But, as with all things, there is another side to progress. New technology will also unveil novel and unintended problems and adverse effects. There are many anecdotes of the "not-so-pretty" side of technology: some are technical in nature, some are economic and legal, and some are cultural and social. For example, in the technical category, it is important to remember there is probably not a single software application in use or on the market today that is without defects or "bugs." Many of these defects may never reveal their presence but assuredly many will. On the continuum of severity, there are the trivial, minor nuisances associated with a popular spreadsheet or operating system application and the potentially catastrophic effects of the impending Unix and C crises.[7]

These unintended problems and adverse effects amply highlight our growing dependence on automated and intelligent systems and components such as computers and software. They also reveal our collective vulnerability. Fewer individuals will be cognizant of the existence of these intelligent and automated systems and applications. Fewer individuals will know how to repair them, and still fewer individuals will really understand their inner-workings. The Nation and the global community would be well-advised to be vigilant in ensuring that there is increased reliability, flexibility and fault-tolerance built into future technology platforms.

II. THE FIRST GLIMPSE OF THE FUTURE: THE YEAR 2000 PROBLEM

The first taste of the anxiety and difficulty (*e.g.*, technical, economic, regulatory and legal) that we can expect from our growing dependence on technology is most assuredly the Year 2000 Problem. It is one of the most pressing issues currently facing our Nation and the world today. In recent months, public atten-

[4] *See Remarks Of President William J. Clinton Concerning The Year 2000 Conversion* (visited July 14, 1998) <http://www.y2k.gov/new/presy2k.htm>.

[5] *See* Neil Gross, *Into The Wild Frontier*, BUS. WK., June 23, 1997, at 72 (in the future, computers will "respond to our voices and extend our senses.").

[6] *See* George Gilder, *Regulating The Telecosm*, CATO Policy Report, Sept./Oct. 1997, at 1.

[7] *See* Capers Jones, *Bad Days For Software*, IEEE Spectrum, Sept. 1998, at 47 (providing examples of related imminent date change and computer programming problems).

tion has been drawn to the effects that the Year 2000 Problem will have on unprepared computers, automated and intelligent systems, and microprocessor-controlled machines that are used virtually in all industries of the global economy. There are wildly differing scenarios, ranging from "business-as-usual" to apocalyptic, that suggest that there is much about the Year 2000 Problem that is hard to predict.[8] What is known, however, is that thousands of legacy networks, systems and applications exist that were not designed to account for the millennial date change on January 1, 2000. As a consequence, the Year 2000 Problem, if not addressed properly, could affect various important sectors of the domestic and global economy, including energy, transportation, and financial and securities services.

The implications of the millennial date change problem are especially significant for the communications industry. Hundreds of millions of users of communications services throughout the country transmit voice, data and video information through a communications infrastructure composed of the wireline telephone networks, cellular and personal communications system ("PCS") networks, satellite constellations, broadcasting and cable television systems, and the Internet. Many critical programs, such as Defense Department command and control, Federal Reserve electronic fund transfers, and Medicare benefit payments, also depend upon this ubiquitous infrastructure and, consequently, could be seriously affected if the Year 2000 Problem interrupts telephone and data networking services. Senator Robert F. Bennett, Chairman of the Senate Special Committee on the Year 2000 Technology Problem, was right on the mark when he labeled the "global []communications infrastructure . . . the central nervous system of modern society."[9]

III. OVERVIEW OF THE YEAR 2000 PROBLEM

Simply stated, the Year 2000 Problem[10] is the inability of unprepared computers and other related automated and intelligent systems to process the millennial date change that will occur on January 1, 2000. In the 1950s and 1960s, computer designers and programmers, in order to reduce the need for expensive computer memory and data storage,[11] developed the convention of storing calendar year dates using only the

[8] The on-going dialogue about the Year 2000 Problem and its potential impact, and the sizable collection of written commentary on the issue, suggest that no one-layman and technologist alike-truly knows what will happen when the calendar advances to January 1, 2000 from December 31, 1999. *See, e.g.*, Frances Cairncross, *Survey: The Millennium Bug*, ECONOMIST, Sept. 19, 1998, at 1; Steven Levy & Katie Hafner, *The Day The World Shuts Down*, NEWSWEEK, June 2, 1997, at 53; Neil Munro, *The Big Glitch*, NATIONAL JOURNAL, June 20, 1998, at 1422; Douglas Stanglin & Shaheena Ahmad, *Year 2000 Time Bomb*, U.S. NEWS & WORLD REPORT, June 8, 1998, at 45; Rajiv Chandrasekaran, *Double-Zero Hour Looms For Historic Repair Job*, WASH. POST, Aug. 2, 1998, at A1. *Compare* Chris O'Malley, *Apocalypse Not*, TIME, June 15, 1998, at 62 ("while there are more than a few fatalists … most of the folks responsible for fixing the nation's electronic infrastructure actually think we're going to make it into the next millennium with only minor, if any, disruptions of vital services") (emphasis added) with Edward Yardeni, *Year 2000 Recession?* (visited Nov. 11, 1998) <http://www.yardeni.com/y2kbook.htm> (self-described "alarmist" predicts "[i]f the disruptions are significant and widespread, then a global recession is possible").

[9] *See Hearing Before The Senate Special Committee On The Year 2000 Technology Problem*, 105th Cong., 2d Sess. (July 31, 1998) (opening remarks of Senator Robert F. Bennett, Chairman, Senate Special Committee on the Year 2000 Technology Problem).

[10] Other terms used are the "Millennium Bug" and the "Y2K Problem." Moreover, the millennial date change issue is often referred to as the "Century Date Change Problem" because several other important dates, prior to and following the rollover to January 1, 2000, can potentially affect the unprepared electronic infrastructure. For example, September 9, 1999—or 9/9/99—is important date because the string of four 9s is often used by computer designers and programmers as a termination code to close or shut down applications. Another important example is February 2000, which contains a leap year day (*i.e.*, one additional day that February 1900 did not possess) that automated and intelligent systems may not be able to process correctly. There are over 12 different computer date change issues that are implicated by the millennial date rollover.

[11] The genesis of the Year 2000 Problem can be attributed to the legitimate concerns and deliberations about the costs and space requirements associated with computer memory. *See, e.g.*, Richard Comerford & Tekla S. Perry, *Brooding On The Year 2000*, IEEE Spectrum, June 1998, at 71-72; Cairncross, *supra* note 8. Corporate executives, information technologists, and

last two digits for the date year. Thus, the calendar year 1967 was represented as "67." As a consequence, computerized systems and networks may erroneously assume "00" to be "1900," not "2000," and thereby not function properly in the year 2000. In some cases, the hardware and software will continue to work, but they will generate and process spurious data that may not be detected for months or even years.

If you are curious how the truncating of calendar dates from four digits to two could potentially lead to unintended and unpredictable consequences on January 1, 2000, think of the problem in practical terms. The ability to process employee benefits, calculate financial interest, monitor bank loans, and many other important activities depend upon the ability of computers and software applications to determine elapsed time by taking a "start date" and subtracting it from an "end date." For example, a typical corporate human resources department has relatively sophisticated computer hardware and software to record and calculate a variety of date-sensitive data, including length of company service, as well as period-in-time to accession, promotion, or termination. On January 1, 1999, when the computer calculates the company service of an employee who started with Company X on January 1, 1967, the computer subtracts "67" from "99" and outputs "32" years of company service (*e.g.*, 99 - 67 = 32). On January 1, 2000, when the recalculates the employee's company service it outputs incorrectly "-67" years (*e.g.*, 00 - 67 = -67).[12] This erroneous output might crash the computer system or merely result in inaccurate data.

While many designers and programmers realized thirty or forty years ago that the two-digit calendar year convention would not work for years after 1999, they assumed that the computer applications they were developing would be obsolete and replaced long before the Year 2000 Problem became apparent or serious.[13] Unfortunately much of the mission-critical software that companies and individuals rely upon still uses this convention.

Another area of concern-and one that most government departments and agencies and private industry recognize as equally problematic and dangerous-is the microprocessor problem. The Year 2000 Problem may affect thousands of microprocessor-controlled systems and machines (which make use of billions of microprocessors, or so-called computer "microchips").[14] These microchips, which are the hardware equivalent of unprepared computer software, are hardwired into all types of machines and equipment that are used daily throughout the world. From a consumer's perspective, microchips are used in the toaster oven, the video cassette recorder, the car engine, and many other appliances. Relatedly, in critical industry sectors and infrastructures, microchips are used in environmental and climate systems, command and control systems, power distribution systems and communications systems.

---

others found it necessary to think of their nascent automated and intelligent systems-very often, huge assemblies of cabinets filled with vacuum tubes, and later magnetic cores, for main memory-in the practical terms of computer-storage requirements, financial costs and limitation of physical space. *Id.* The two-digit calendar year convention has been lambasted as "penny-wise and pound-foolish" but in reality the solution allowed designers and programmers to save valuable money and space. In its September 19, 1998 survey of the Year 2000 Problem, the *Economist* magazine noted the "cost of one megabyte of magnetic disk storage (enough for a solid novel) in 1965 was $762, compared with 75 cents today and perhaps 34 cents in 2000." Cairncross, *supra* note 8.

[12] The foregoing is only a hypothetical example of the potential unintended effect of the Year 2000 Problem and is in no way a definitive example.

[13] *See* Comerford & Perry, *supra* note 11, at 72.

[14] According to the Gartner Group, Inc., a private consulting firm, there are approximately four billion microprocessors currently used in everything from the average modern automobile, to transoceanic supertankers, to automated industrial process machines, to any variety of computational and medical equipment. *See* Munro, *supra* note 8, at 1424-25. Some of the four billion microchips-roughly 160 million, or 4 percent-performed some date-related function. *Id.* at 1425. Using Gartner's estimate of 160 million potentially affected microprocessors, "industry would have to find and fix about 288,000 defective chips every days between now and the end of 1999." *Id.*

IV. WHAT IS THE IMPACT OF THE YEAR 2000 PROBLEM?

Fixing embedded networks, systems and applications requires computer designers and programmers to go line-by-line through billions of lines of code to correct the way the software calculates dates. In many cases, microprocessors need to be replaced. Both types of remediation efforts require the dedication of a tremendous number of knowledgeable expert personnel[15] and the allocation of significant financial resources.[16] The technical solutions are without a doubt available or, at a minimum, implementable. However, the time-consuming, resource-intensive nature of the domestic and global Year 2000-readiness effort demands, in light of the immovable deadline, a flexible, efficient and effective solution comparable in some respects only to a nation preparing for war.

The Year 2000 Problem thus begs the question, "What might happen on January 1, 2000, if there is not a concerted, effective and comprehensive attack directed to remediate various embedded legacy networks, systems and applications?" Technologists and computer experts reveal that it is impossible to predict with any level of confidence what types of disruptions and failures that Year 2000-incidents would precipitate. However, this problem has already cropped up resulting in telling serious malfunctions and disruptions.[17]

Consider the following situations that have recently occurred. Banks have had to correct loan processing software that could not calculate ten-year loans because it could not tell the difference between 2003 and 1903. A corned beef manufacturer destroyed new inventory because its legacy computer system believed that the fresh product was almost 100 years old. In 1998, when Chrysler Corporation conducted a Year 2000 test at one of its assembly plants, the simulated millennial date change affected the facility's security system and prevented any people from leaving the building.[18] A merchant sued a computer hardware company for selling point-of-sale credit card readers that purportedly could not process authorizations of credit cards with expiration dates in 2000.[19]

The risks, however, are not confined to the direct effects of a Year 2000 failure. There may also arise secondary, or "echo," effects stemming from the Year 2000 Problem.[20] For example, some companies may

---

[15] *See* Chandrasekaran, *supra* note 8, at A1 ("[Y2K] is one of the most expensive, labor-intensive, time-consuming problems mankind has ever faced.") (remarks of Ann K. Coffou, Analyst, Giga Information Group, Inc.).

[16] It is still unclear, at this juncture, what will be the financial impact of the Year 2000 Problem. The Gartner Group's frequently cited estimate puts the total price tag at approximately $300 billion to $600 billion. *See* Steve Prentice, *Telecomms And The Year 2000-IT Problem, Or Global Crisis?*, Gartner Group, Inc., at 2 (1998). J.P. Morgan Securities, Inc., and Merrill Lynch, Inc., respectively, have forecasted $200 billion and $1 trillion. *See* William D. Rabin, *Industry Analysis: The Year 2000 Problem*

experience problems associated with billing and accounting processes. The delay in collections and the resulting shortfall in revenue could theoretically lead to a company's inability to pay salaries and retain personnel who are essential for the uninterrupted provision of services. These problems are not directly attributable to the Year 2000 Problem (*i.e.*, a technical manifestation), but they can affect a company's ability to provide commercial services impacting employees and consumers. Relatedly, there is also a need to consider public or crowd psychology (*i.e.*, the perceptions and responses of consumers) when dealing with the millennial date change issue. If consumers are overly sensitized to the doomsday and alarmist reports that are so widely reported and they encounter a disruption in an essential service, even if the failure arises from a non-Year 2000 incident, then unintended (and equally catastrophic) consequences could unfold.

For example, the Federal Communications Commission is worried about the possibility that on the fateful day, millions of telecommunications users will pick up their phones to find out if there is dialtone. The public switched telephone network is not engineered to have millions of users pick up the telephone at the same time and dial; rather the network is optimized for a certain number of users (albeit a high number of users), dialing and talking for a certain number of minutes. If millions of users pick up the telephone at or near the same time then it is theoretically possible that certain parts of the network could experience a disruption, but not because of the Year 2000 issue. In the banking context, customers may attempt to withdraw money from their bank's ATM and discover that the ATM will not disperse money. Perhaps the ATM is experiencing a Year 2000 glitch, but equally plausible is the possibility that the money machine is out-of-cash or out-of-service, common reasons for such machines to be disabled.

What will be the consequence of a large number of users that discover there is no dialtone or ATM service, not because of a Year 2000 failure, but because of the constant alarmist reports that have convinced those telecommunications users and bank customers that it is nothing other than a Year 2000 incident? Will the public psyche be so consumed with fear and doubt that a non-Year 2000 incident will manifest itself in panic and runs on food stores and money supply? Of course, no one knows, but we should be mindful of the attending psychology impacts.

V. COMMUNICATIONS AND THE YEAR 2000 PROBLEM

Luckily the Year 2000 Problem has not adversely affected the normal day-to-day operations of the ubiquitous communications infrastructure over which the Federal Communications Commission (the "Commission" or "FCC")[21] has express statutory oversight. Nevertheless, there is a tremendous amount of public concern about the pace and extent of remediation activities in the communications industry. There have been illustrative examples of network disruptions in the non-Year 2000 context, including America Online's system failure in 1996,[22] and the AT&T frame relay network incident[23] and PanAmSat's Galaxy IV

[21] The Federal Communications Commission is an independent United States government agency, charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers interstate and foreign wireline communications among the 50 states, the District of Columbia, and U.S. possessions and the use of the electromagnetic spectrum for communications purposes. In addition to addressing those issues that are directly within its jurisdiction, the Commission-as a principal member on the President's Council on Year 2000 Conversion-is directly responsible for coordinating the federal government's Year 2000 effort in the communications industry.

[22] On August 6, 1996, America Online experienced a 19-hour outage when new host software, essential to the on-line service provider's operating system, went off-line. *See* David S. Hilzenrath, *American Online Goes Off-Line*, THE WASHINGTON POST, Aug. 8, 1996, at A1. Approximately 6.3 million AOL users worldwide were temporarily unable to access electronic mail or otherwise use on-line services and functions (*e.g.*, electronic news, World Wide Web). *See id.*

[23] Thousands of AT&T customers were affected by the disruption of an advanced frame relay network in April 1998. For nearly 20 hours, widespread problems impaired the ability of frame relay customers to utilize the high-speed, packet-switched

satellite failure[24] in 1998, that have been prominently featured in the general media. These events have only hastened public concern about the communications industry's readiness and capacity to implement Year 2000 compliance remedies. Hundreds of millions of communications users in the United States transmit voice, data and video information upon the ubiquitous communications infrastructure, and each depends on the network for its near unfailing reliability, continuity, and usability.

A. Challenges For Making Communications Year 2000-Compliant

Of course, there are several challenges associated with making the communications infrastructure Year 2000-compliant that will squarely confront the communications industry. First and foremost, there is the obvious challenge of making all mission-critical systems and components Year 2000-ready before January 1, 2000. As we approach the immovable deadline of the Millennium, companies and organizations will have to engage in the prioritization of implementing solutions. C. Michael Armstrong, Chairman and Chief Executive Officer of AT&T Corporation and Chairman of the Network Reliability and Interoperability Council, punctuated this fact when he noted at the Council's first meeting that an AT&T analysis found that testing every potentially vulnerable system in the AT&T network would require 60,000 test years to complete.[25]

Second, as described in Section IV, remedying the Year 2000 Problem in the communications industry will demand the commitment of tremendous personnel and capital resources.[26] For example, GTE Telephone Operations has dedicated 1,200 employees to the company's preparedness effort. Other companies are committing similar levels of personnel resources and spending in excess of $400-$500 million.

Third, there appears to be a lack of clear guidance on the question "What does it mean to be Year 2000-compliant?" A striking absence of common definitions related to the Year 2000 Problem presently exists. Firms and companies often resort to the ambiguous terms "compliant," "ready," "functional" and "capable." If one were to survey the different definitions proffered by governmental and private entities, one would be surprised to learn that they are vague and varying.

For example, the Federal government defines Year 2000 compliance in section 39.002 of the Federal Acquisition Regulations:

> Year 2000 compliant means, with respect to information technology, that the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.[27]

A "compliant" product, according to the Hewlett-Packard Company, "accurately processes date data (including, but not limited to: calculating, comparing and sequencing dates), from, into and between the

---

data network technology to transmit and exchange large amounts of computer information. *See* TR DAILY, *AT&T Says Most Customers' Frame Relay Service Restored, Acknowledges 'Root' Cause Of Network Failure Unknown*, Apr. 14, 1998.

[24] In May 1998, PanAmSat's Galaxy IV satellite malfunctioned and spun out of control, interrupting the transmission of radio and television broadcasts and disrupting paging services to 80-90 percent of Nation's approximately 40 million pager users. *See* Mike Mills, *Errant Communications Satellite Cause Pager, TV Disruptions*, THE WASHINGTON POST, May 20, 1998, at C14.

[25] GTE Telephone Operations estimates that the number of tests that would be required to test all combinations of its equipment and operating systems would be exceptionally high—10^{29}. Attempting to perform that number of tests in the time remaining, *i.e.*, less than 13 months, is simply impossible even if adequate test beds and other facilities were available to facilitate such testing.

[26] *See, e.g., supra* section IV & note 17 (describing the breadth of the costs and liabilities facing corporations).

[27] Federal Acquisition Regulations, 48 C.F.R. § 39.002 (1996).

twentieth and twenty-first centuries, the years 1999 and 2000, and leap year calculations, when used in accordance with its product documentation, and provided all other products used in combination with the product properly exchange data with it."[28]

SBC Communications, Inc. prefers "Year 2000 ready" and provides the following definition: "the system or service must successfully pass the inventory, assessment, testing and implementation phases and, to the extent applicable, be able to read, compute, store, process, display and print calendar dates falling after December 31, 1999, without interruption or degradation to service."[29]

So does the question "What does it mean to be Year 2000 compliant?" mean that every individual mission-critical element and component in a system is certified, and, if so, what is the consequence when all of the Year 2000-compliant elements are re-connected and the process or function does not work? What happens if Firm X uses a definition, standard and process methodology which is wholly different from Firm Y, and, when the two firms interconnect, there is not continuity of service and errors and failures arise? Unfortunately, the truth is that individual critical elements and components that alone are "Year 2000 compliant" may not be capable of performing their specific functions because of the various methods for reaching compliance.

At some level, the definitional problem may prove unimportant. What really matters is that systems and services remain functional through critical date rollovers. The assurance of that is dependent on the exhaustive testing of a remediated system irrespective of what definitions are adopted. In short, if the mission-critical processes, services and functions continue to work then it should not matter that the components might not meet a given definition of Year 2000 compliance.

1. Legal And Regulatory Liability Concerns

Without a doubt, in the Year 2000 Problem context, legal and regulatory liability issues are the most significant barriers to the dissemination of timely and candid information about the Year 2000 readiness efforts of carriers, service providers, and manufacturers that are critical to remediating the problem.[30] The legal concerns proffered by industry-some that appear to be overstated and some that appear to be legitimate-are associated in part with issues of product disparagement, antitrust violations, third-party liability, and carrier-vendor contractual relations, just to name a few. As a consequence, some companies have been reluctant to divulge information pertaining to their Year 2000 vulnerabilities and have been largely unwilling to guarantee or certify Year 2000-readiness due to concerns about liability.

With respect to the Year 2000 Problem, the reasons for the concern and uneasiness expressed about legal

---

[28] Hewlett-Packard Company's Year 2000 Compliance Definition <http://www.hp.com/year2000/compliance.htm> (visited Nov. 11, 1998).

[29] SBC Communications, Inc.'s Year 2000 Readiness Definition <http://www.sbc.com/News/y2k.htm> (visited Nov. 11, 1998).

[30] There has been no shortage of commentary and discourse on the potential legal consequences arising from the Year 2000 Problem and the possibility of significant legal litigation before and after January 1, 2000. *See, e.g.*, Kathy Barrett Carter, *Lawyers Boot Up For Y2K Crashes*, THE STAR-LEDGER, Aug. 4, 1998, at 1; Mark E. Konrad, *Countdown To 1/1/00: Solving The "Year 2000 Problem"*, NEVADA LAWYER, at 14 (June 1998); J. Travis Laster, *The Year 2000 Problem In Delaware: Preparing To Defend Shareholder Derivative Law Suits*, INSIGHTS, at 12 (June 1998); James K. Lehman & Kevin A. Hall, *Year 2000 For Lawyers: A Legal Primer On The Millennium Bug*, SOUTH CAROLINA LAWYER, at 15 (July/Aug. 1998); Linda A. Monica, *Year 2000: The Gathering Storm Of Litigation Over The "Millennium Bug*, MAINE BAR JOURNAL, at 184-85 (July 1998) ; Dean A. Morehous, Jr., *Liability Issues And The Year 2000*, Practising Law Institute, 18th Annual Institute on Computer Law (Feb. 1998); Ronald Rosenberg, *Lawyers Cashing In On Y2K Liability Problems*, THE JOURNAL RECORD, Feb. 5, 1998; Anna Snider, *The Millennium Has Arrived For Y2K Practice Groups*, NEW YORK LAW JOURNAL, May 11, 1998, at 1.

liability are apparent. Certain gloom-and-doom reports suggest that on January 1, 2000, 50% of companies may experience a Year 2000-incident affecting part or all of their systems.[31] If the forecasts are even marginally accurate, on January 1, 2000, many affected companies could be subject to a wide-range of potential liability. In fact, it is interesting to note that the cost to eradicate the Millennium Bug ($300 billion to $600 billion) pales in comparison to provocative estimates of legal costs in the range of $1 trillion.[32]

A small number of class action suits already have been filed in both state and federal courts. Most pending actions deal with "goods" (*e.g.*, computer software and intelligent systems) purchased between calendar years 1994 and 1997. Plaintiffs seek relief under several different causes of action, including a federal Magnuson-Moss Act claim and state law claims such as breach of warranty, breach of contract, consumer fraud, misrepresentation, and negligence.[33]

The *Produce Palace International v. TEC-America Corp.* lawsuit was the first Year 2000 litigation action, brought in the Circuit Court for the County of Macomb, State of Michigan.[34] Plaintiff Produce Palace bought a computer system to network their cash registers, process credit cards and expedite accounting. The Plaintiff alleged that the system was installed in 1995 without the ability to process credit cards expiring on or after January 1, 2000. The Plaintiff alleged breach of warranty under Michigan law,[35] violation of the Magnuson-Moss Warranty Act,[36] breach of warranty of fitness under Michigan law,[37] breach of duty of good faith,[38] negligent repair, misrepresentation, breach of contract, and violation of the Michigan Consumer Protection Act.[39] The Plaintiff also alleged a right under Michigan law to revoke the transaction due to a lengthy repair history and continuing defects, and sought a refund of the purchase price along with incidental and consequential costs. The instant action was settled, subject to an arrangement reached among the parties for $260,000.[40]

Firms may also be fearful of the prospect of not complying with the myriad of Year 2000 readiness and disclosure rules that are promulgated by the various U.S. regulatory agencies and the potential adverse consequences of non-compliance. Making affirmative representations of Year 2000 compliance or disclosing information about a firm's readiness activities and potential Year 2000 trouble spots would provide legal ammunition that could be used against the firm by a regulatory agency-like the Commission-or another litigant or class of plaintiffs.

The regulatory landscape is filled with numerous examples of voluntary and mandatory disclosure requirements. The Securities and Exchange Commission ("SEC") has been perhaps the most visible regulatory agency when it comes to the promulgation of information disclosure guidelines. In January 1998, the SEC issued a notice-the so-called "Bulletin no. 5"-regarding the disclosures to be made by public compa-

---

[31] *See* Monica, *supra* note 30, at 185.

[32] *See, e.g.*, Carter, *supra* note 30, at 1 ("[L]egal costs could reach $1 trillion, substantially more than…businesses will spend to fix Y2K problems, and more than all the money spent on Superfund environmental litigation, asbestos, breast implant and tobacco litigation combined"); Larry Smith & Lori Tripoli, *More Billables Than Superfund!…Law Firms Position for the Billion-Dollar Y2K Boom*, OF COUNSEL, May 18, 1998, at 10.

[33] *See, e.g., Atlaz Int'l, Ltd. v. Software Bus. Technologies Inc.*, No. 172539 (Cal. Super. Ct.) (Dec. 2, 1997) <http://www.2000law.com/my_html/atlaz.htm>; *Issokson v. Intuit, Inc.*, No. CV-773646 (Cal. Super. Ct.) (Apr. 28, 1998) <http://www.2000law.com/pdf/issokson.pdf>; *H. Levenbaum Ins. Agency, Inc. v. Active Voice Corp.*, No. 98-3864 (Mass. Super. Ct.) (July 2, 1998) <http://www.2000law.com/pdf/levenbaum.pdf>.

[34] *See Produce Palace Internat'l v. TEC-America Corp.*, No. 97-3330-CK (Mich. Cir. Ct.) (June 12, 1997) <http://www.2000law.com/my_html/Produce.htm> (visited Nov. 11, 1998).

[35] *See* Mich. Comp. Laws Ann. § 440.2314 (West 1998).

[36] *See* 15 U.S.C. § 2301.

[37] *See* Mich. Comp. Laws Ann. § 440.2315 (West 1998).

[38] *See* Mich. Comp. Laws Ann. § 440.1203 (West 1998).

[39] *See* Mich. Comp. Laws Ann. § 445.901 (West 1998).

[40] *See* Erich Luening, *First Y2K Lawsuit Filed Is Settled*, CNET NEWS.COM, Sept. 14, 1998 <http://www.news.com/news/>.

nies and by investment firms and advisors.[41] The SEC's Bulletin no. 5 was subsequently superseded by an August 4, 1998 interpretative statement regarding the disclosure of Year 2000 issues and consequences for public companies, investment advisors, investment firms and municipal securities issuers.[42]

The SEC noted, in relevant part, that:

> [c]ompanies already disclose in their [Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A")] their assessment of known trends, demands, commitments, events or uncertainties that are likely to have a material impact. MD&A is designed to allow investors to see the company through the eyes of management. Investors deserve no less with respect to management's assessment of their company's Year 2000 problems.[43]

The palpable anxiety and concern of legal and regulatory liability has thus contributed to an environment where companies are fearful of disclosing timely and candid information about their products or services, or how far they have advanced toward compliance. To address this significant problem, President Clinton signed the *Year 2000 Information and Readiness Disclosure Act*, a bi-partisan legislative initiative to which the telecommunications industry and many others substantially contributed and that was enacted by the Congress, on October 19, 1998. This legislation is an important part of the country's efforts to prepare for the Year 2000 Problem. It promotes and encourages the sharing of Year 2000 information by limiting the liability exposure those statements might cause.

The *Year 2000 Information and Readiness Disclosure Act* will surely advance the information exchange effort. However, additional measures may be needed on a forward-going basis. There will be a significant and continuing role to be played by the Congress, the Administration, and industry with regard to the legal liability issues and other barriers to the information flow.

2. Competitive and Marketplace Concerns

Competitive and marketplace concerns are also significant hindrances to addressing the Year 2000 Problem. A considerable amount of anxiety exists in the private sector about the attending competitive consequences if companies openly reveal to customers that they are experiencing difficulties in remediating their embedded electronics infrastructure. Some firms are legitimately concerned about the manner in which they will be treated by the capital markets. In both instances, companies could lose the confidence of both their customers and investors. Even a temporary wavering of confidence might have a tremendous impact on the financial bottom-line.

There is also a growing chorus of concern in the private sector about the accounting implications of the Year 2000 Problem. As noted above, most U.S. communications carriers, manufacturers, and providers will spend on average $400-$500 million to attack the Year 2000 issue. In many cases, there will be substantial spikes in capital expenditures in a given year. Because such spikes are often unanticipated and cannot be depreciated, the market may react by de-valuing the company's stock. Many companies are concerned about how such a single or repeated spike of a multi-million dollar expenditure will be accounted for in any forward-going quarterly or annual reports, and more importantly how the financial markets will respond.

---

[41] *See* Securities and Exchange Commission Staff Legal Bulletin No. 5 (Divisions of Corporation Finance and Investment Management), Jan. 12, 1998, at 1 <http://www.sec.gov/rules/othern/slbcf5.htm> (visited Nov. 11, 1998).

[42] *See* Securities and Exchange Commission Statement Regarding Disclosure of Year 2000 Issues and Consequences By Public Companies, Investment Advisers, Investment Companies, and Municipal Securities Issuers, Release No. 33-7558, Aug. 4, 1998, at 1 <http://www.sec.gov/rules/concept/33-7558.htm> (visited Nov. 11, 1998).

[43] *Id.*

3. The Criticality, Interdependency and Uniqueness of Communications Services

Few events in the Digital Information Age (before the Year 2000 Problem) have so clearly demonstrated the interconnectivity and interdependency of the communications industry. The communications infrastructure is one of a handful of basic building blocks-including energy and transportation-upon which all other industries and programs rest. It is also disproportionately dependent on the coupling of various disparate networks.

If one is particularly interested or concerned about the public switched telephone network-as are most critical end-users-then it is important to remember that no single entity owns or controls the public switched telephone network. The major telecommunications carriers, such as the Bell Operating Companies, GTE, AT&T, MCI WorldCom and Sprint, provide service to the majority of the country. But 1,300 small to mid-size independent telephone companies serve many rural and insular parts of the country as well as the U.S. territories and possessions. Moreover, the total global network depends as well on different international carriers, in different countries around the world. And these companies are only one in a long chain of vertically and horizontally-interrelated companies required for the network to operate.

For example, in order to fix the Year 2000 Problem, carriers rely on manufacturers of central office switches and other network equipment, like Northern Telecom, Lucent and Siemens. Private networks and end users must make sure their equipment-such as their telephones, voice mail systems, Private Branch Exchanges ("PBXs"), and local area computer networks-is Year 2000-ready; otherwise, they may be unable to send or receive voice and data traffic. These groups are, in turn, dependent upon other manufacturers for their equipment, who are, in turn, dependent yet again on other providers for parts and services such as power. And on it goes.

Without a doubt, the telecommunications network is a tremendously complex and interdependent thing. It consists of millions of interconnected parts and hundreds of millions of lines of computer code. The public switched telephone network processes millions of calls per minute. To transit each and every call, automated and intelligent machines and systems (in the possession of the thousands of telecommunications carriers and users described above) make calculations for the most efficient multi-path, real-time interaction of all points along the established circuit between the call's origination and destination.[44] In microseconds, a phone call from Washington, D.C. to New York travels from your telephone, to the Private Branch Exchange (*i.e.*, switchboard) in your building, to the local exchange carrier's central office switch, through the carrier's network components and systems that route your call to an inter-exchange carrier (or carriers), through long-distance trunk lines (or other telecommunications facilities like microwave, satellite, fiber optic), to another local exchange carrier's central switch, and ultimately to the telephone on the other end. Make the same call two minutes later and the call may be routed in a completely different manner as calculated by the network.

The foregoing description points to the mathematical difficulty (*i.e.*, the infinite number of permutations and combinations of routing possibilities and service events to transit a voice or data call) of testing the entire public telephone network for Year 2000-readiness.[45] If any one of those components/systems (*e.g.*, central office switch), network elements (*e.g.*, advance intelligent network, Signaling System 7), or network interconnectors (*e.g.*, local exchange carrier, interexchange carrier, Internet Service Provider, private telecommunications network user) is affected by the Year 2000 Problem, a call might be disrupted.

[44] *See generally Hearing Before The House Committee On Ways And Means, Subcommittee On Oversight*, 105th Cong., 2d Sess. (June 16, 1998) (testimony of A. Gerard Roth, Vice President, Technology Programs, GTE Corporation) <http://www.house.gov/ways_means/oversite/testmony/6-16-98/6-16roth.htm> (visited Nov. 11, 1998).

[45] *See, e.g.*, *supra* Part V.A; *supra* note 26.

B. Unique Advantages For Remediation in Communications

It is important to note, however, that as daunting as the challenges and complexity may appear, the communications industry is probably better equipped and positioned to address this issue than most. As Frances Cairncross of the *Economist* noted in her September 19, 1998 survey on the Year 2000 Problem, critical industry sectors like communications "*depend disproportionately on networks* and therefore *tend to emphasize reliability and continuity*."[46] In support of Ms. Cairncross's observation, there are five very important points.

First, the industry is dependent upon a highly complex, technical network that is engineered for near unfailing reliability.[47] Communications is not an industry that contemplates periods of downtime (*e.g.*, evenings, weekends, holidays, or re-tooling cycles). Communications, quite apart from other industries, is both a "live" network running 24 hours a day, 365 days a year, and a industry sector "based on operating a ubiquitous, shared physical infrastructure."[48] The success of the industry "is measured *by the number of customers mutually connected* by the infrastructure, and *by the reliability and usability of these interconnections*."[49]

Success is also measured in terms of revenues, subscribership, dividends, and profits. The major telecommunications carriers and providers understand well that they potentially face diminished goodwill, regulatory trouble,[50] and legal liability[51] if they do not satisfactorily address the Year 2000 problem. Let us not forget that the industry is also susceptible to financial ruin.[52] For example, in the case of PanAmSat's Galaxy IV, the satellite failure foreclosed any possibility of the company (a publicly traded subsidiary of Hughes Electronics) collecting an estimated $78 million in revenues for 1998, and reportedly could lead to a $20 million revenue shortfall in both 1998 and 1999 from the loss of all pre-empted users of the newer Galaxy VI satellite.[53]

---

[46] *See* Cairncross, *supra* note 8, at 11 (emphasis added).

[47] The Bellcore standard is 99.9999 percent up time, translating into a switch reliability standard of less than 3 minutes downtime per year. That is 3 minutes of 525,650 minutes in a year.

[48] *See* Ross M. Richardson, *Letters To The Editor: Who Will Win The Telco Wars?*, WALL STREET JOURNAL, Jan. 8, 1998, at A9. Even though the most prominent examples of telecommunications disruptions—AT&T frame relay and PanAmSat Galaxy IV—highlight the vulnerability that users may experience in the event of a serious failure of a single piece of hardware, it is important to note that communications networks and components are designed to be fault-tolerant, adaptable and quickly remedied. For example, AT&T was able to implement technical solutions and substantially restore frame relay service within 20 hours after the initial outage reports. Moreover, communications failures of this magnitude are rare. Wayne A. Whiyte, Chief of Spectrum Management at NASA's Lewis research facility, commenting on Galaxy IV noted "[s]atellite communications has been in existence for 30 to 40 years now and you can probably count the number of satellite failures on one hand." *See* Frank D. Roylance, *Orbiting Switchboard Pulls Plug On U.S.*, THE BALTIMORE SUN. May 21, 1998, at 1A.

[49] *See* Richardson, *supra* note 48, at A9 (emphases added).

[50] *See supra* Part V.A.1.

[51] *See, e.g.*, *id.*; *supra* Notes 34-35.

[52] Concerned users of communications service are often quick to point to the AOL service interruption and the AT&T data relay outage, but they forget about the devastating effect on the financial bottom-lines of two of the largest firms in the communications industry. *See, e.g.*, Jeff Jinnett, Legal Issues Confronting the Federal Government and State Governments Due to the Year 2000 "Millennium Bug" (1996) ("[when AOL] went off-line for less than one day…its stock dropped approximately three points…the market value of the outstanding AOL stock was reduced by approximately $273 million") <http://www.comlinks.com/links/jjin2.htm> (visited Nov. 11, 1998); Gavin Souter & Michael Prince, *AT&T Fails To Connect: Failure Of Frame Relay Network Highlights Risks In Telecommunications*, BUSINESS INSURANCE, Apr. 20, 1998, at 1 (AT&T CEO Michael Armstrong "would not say how much AT&T would lose in revenue…however, he said the frame relay business generates $1 billion annually for AT&T").

[53] *See, e.g.*, Diane Mermigas, *Satellite Risk Is Out There*, ELECTRONIC MEDIA, June 1, 1998, at 18; Anthony L. Velocci, Jr., Market Focus, AVIATION WEEK & SPACE

In this new competitive landscape of telecommunications, profit-maximizing actors will act in their own self-interest, namely to survive and prosper.[54] The captains of industry that are most susceptible to the risks and fears of competition, wake to and work through each day thinking about the negative consequences of not providing quality, reliability, and increasingly innovative services and products. The corresponding impact can be felt in the anxiety they feel about satisfying regulators, shareholders and customers.

Second, the aforementioned legacy of reliability and continuity evidences that companies have a strong stable of trained, reliable experts in network reliability issues. They have experience with identifying threats to network reliability, planning corrections and executing those corrections. In the past, they pulled the entire network apart during the AT&T divestiture and implemented toll-free 800 number portability and local number portability. Perhaps the most analogous example of the industry reconfiguring the live network to remedy a "number" issue was when, due to the depletion of the country's telephone number pool, the industry added the three-digit area code. In essence, the domestic telecommunications industry implemented a *three-digit* technical solution, as opposed to the *two-digit* solution required for the Year 2000 Problem.

Third, because of the importance of network reliability, continuity, interconnectivity and interoperability, there are a number of first class technical consortiums and prominent trade organizations that have a long history of developing standards and addressing network issues and then sharing those findings with all its members. Bellcore has served in this role for the phone system since days of old. The Telco Year 2000 Forum, the Alliance for Telecommunications Industry Solutions ("ATIS"), and other industry groups are providing valuable assistance in facilitating information sharing, building private partnerships, and coordinating testing and contingency planning.

The Network Reliability and Interoperability Council ("NRIC") is another important tool the Commission and the industry will use to assist them in their effort to address the Year 2000 Problem. The newly constituted NRIC-which includes representatives from all the communications industries, including broadcast and cable, as well as equipment manufacturers and On-line Service Providers ("OSP")-will play an important oversight role with respect to interoperability and end-to-end testing. We believe that this organization will be invaluable in coordinating the overall testing, collection and dissemination of information, in addition to advising the Federal Communications Commission on the status of industry readiness and facilitating the development of contingency plans.

The states are also important assets in the Commission's effort to ensure that the integrity and continued operations of the nation's critical communications infrastructure is maintained. As a consequence, the Commission has engaged the support of the National Association of Regulatory Utility Commissioners ("NARUC") and is specifically working with its Communications Subcommittee to ensure that telecommunications companies are aware of the seriousness and consequences of the Year 2000 Problem, to provide information and guidance about the problem, to provide remedial actions and solutions, and to assess the extent and pace with which the telecommunications industry is addressing the problem.

In totality, the Telco Year 2000 Forum, ATIS, Bellcore, NRIC, the States, and other industry groups are providing valuable assistance in facilitating information sharing, building private partnerships, and coordinating testing and contingency planning.

Fourth, most communications firms have contingency plans and continuity of operations procedures for potential non-Year 2000 related disruption scenarios. The industry has also established mutual assistance procedures in the event of a particularly debilitating failure where competitors will assist by carrying the

[54] *See* Alfred E. Kahn, THE ECONOMICS OF REGULATION: PRINCIPLES AND INSTITUTIONS 1 (1970) (citing I Adam Smith, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 421 (Edwin Canaan ed., 4th ed. 1925) (1776)); *see also* Ernest Gellhorn & William E. Kovacic, ANTITRUST LAW AND ECONOMICS 48-50 (1994).

affected carrier's or provider's voice, data or video traffic on their excess capacity. These plans and procedures can be coopted and specifically modified for the Year 2000 Problem. Given the ultimate importance of contingency preparedness, the fact that such plans and procedures exist in some form or another will greatly contribute to the industry's ability to react to any potential Year 2000 incident.

Fifth, the great bulk of the communications infrastructure is largely controlled by a relatively few carriers, providers, and manufacturers. For example, in the United States, the top 20 local exchange and interexchange carriers control more than 97 percent of the total number of U.S. access lines. In the manufacturing context, the majority of the domestic and international telecommunications industry's equipment comes from Lucent, Alcatel, Siemens, Northern Telecom, Fujitsu, and a handful of others.

VI. READINESS EFFORTS BY THE FEDERAL GOVERNMENT AND INDUSTRY

The Commission has taken its responsibility to monitor the pace and extent of the communications industry's Year 2000 readiness efforts seriously since first becoming aware of the problem several years ago and has been working to ensure that the Year 2000 challenge is properly addressed. We have developed and continue to develop outreach and advocacy strategies to raise industry awareness of the issue, as well as methods for assessing and monitoring the industries' efforts to address the problem. Moreover, we have been looking into ways to facilitate the development of effective contingency plans in the event that a major disruption to any segment of the communications industry-including wireline telephony, terrestrial wireless, radio and television broadcasting, cable television, satellites, and international telecommunications-should occur.

Inasmuch as the Commission can play an important role by providing information and guidance to companies, encouraging companies to share information with each other and with their customers, and facilitating the development of readiness and contingency plans, the Commission's ability to address the Year 2000 Problem is *limited*. Only private communications firms themselves have the ability to address properly the Year 2000 Problem. As a consequence, we have been working to promote a flexible (but effective) public-private, "mission-oriented" partnership to ensure that users of communications services enjoy as close to the same level of quality and reliability on and after January 1, 2000, as they do today.

In the time we have remaining, we will have to marshal efficiently the unique skills and resources of the public and private sector to fix the networks and systems that we absolutely need to have and to minimize Year 2000-related disruptions in this country and around the world. With the help of the President's Council on Year 2000 Conversion, the Administration, the U.S. Congress, the Federal Communications Commission, the industry and others, we will substantially meet the Year 2000 challenge, but it will take the contribution and commitment of each of us to achieve it. As Henry Stimson noted, "I know the withering effect of limited commitments and I know the regenerative effort of full action."

VII. CONCLUSION

In the midst of one of the most difficult and dire periods in the 20th century, Winston Churchill once remarked, "Victory at all costs, victory in spite of all terror, victory however long and hard the road may be." At the Federal Communications Commission, Sir Churchill's words resonate fully, for we are optimists and believe that we are participating in one of the greatest undertakings of the day.

Of course, as we move closer to the Millennium, all of our concerns become more acute. Because our collective well-being is dependent upon the reliability of all the nation's and world's telecommunications

networks, government and industry must work together to ensure that whatever disruptions occur do not lead to widespread outages and failures. In this regard, the Commission is fully committed to taking whatever actions it can to facilitate information sharing and industry compliance efforts. Time is of the essence. We cannot move this deadline of January 1, 2000.