B 1/1/4

The Y2K scare: Causes, Costs and Cures

John Quiggin*
Australian Research Council Federation Fellow
University of Queensland

The worldwide scare over the 'Y2K bug' resulted in the expenditure of hundreds of billions of dollars on Y2K compliance and conversion policies. Most of this expenditure can be seen, in retrospect, to have been unproductive or, at least, misdirected. In this article, the technological and institutional factors leading to the adoption of these policies are considered, along with suggestions as to how such policy failures could be avoided in future.

As midnight approached on 31 December 1999, the world prepared to celebrate the dawn of a new millennium. The celebration was tinged with an element of apprehension, however. It had been widely predicted that the advent of the year 2000 (hereafter Y2K) would bring about widespread failures in computer systems leading to severe economic damage (Yardeni 1997) and, in more apocalyptic accounts, The End of The World As We Know It (TEOTWAWKI)[1]

As Y2K approached, governments and other authorities issued reassuring bulletins saying that thanks to a massive remediation program costing many billions of dollars, the problem had largely been solved, and only minor disruptions were to be expected. These reassurances failed to convince a significant minority of the population, who stored bottled water and canned food as a precaution against possible disaster.

A smaller minority dissented for the opposite reason, claiming that the whole problem had been grossly overstated, and most of the money spent on remediation had been wasted. Australian Y2K sceptics included Fist (1998a; 1998b and Quiggin (1999a;1999b).

Within an hour of the arrival of Y2K in New Zealand and Australia, it became apparent that the advocates of TEOTWAWKI had been proved wrong. No computer failure more serious than a bus ticket machine with an erroneous date stamp was reported from either country. The agencies responsible for co-ordinating the remediation effort reported that their efforts had been even more successful than expected, but warned that a state of alert would be necessary for some time to come. Official reports released early in 2001, restated this view.

Over time, however, it has been widely accepted that the sceptics had been vindicated by events. The number of Y2K-related problems was so small as to cast doubt on the claimed magnitude of the original problem. Y2K programs that had been planned to continue for years were wound up within months after the advent of Y2K. Most importantly, it became apparent that Y2K-related problems had been insignificant even where little or no remediation effort had been undertaken.

Despite an expenditure estimated at $A12 billion in Australia (Campbell 2000) and as much as $US 500 billion for the world as a whole, no serious *ex post* evaluation of Y2K policy has been undertaken. In this paper, it will be argued that, although some relatively minor problems were prevented, and some collateral benefits were realised, most money spent specifically on Y2K compliance exercises was wasted. Moreover, it will be argued, evidence available early in 1999, should have been sufficient to justify the adoption of a less costly strategy of 'fix on failure'.

The Y2K process is also of interest in the analysis of policy processes and in suggesting policy improvements. The fact that government agencies and private corporations were willing to undertake such a large expenditure on a little-understood problem requires explanation. If, as will be argued here, this expenditure was largely wasted, it is desirable to consider institutional

Australian Journal of Public Administration • 64(3):46-55, September 2005

reforms that would reduce the likelihood of similar episodes in future. This article offers some suggestions for possible reforms. However, analysis of the Y2K problem suggests that its characteristics were such as to elicit an excessive response from large institutions and governments, even in the presence of general procedures designed to avoid wasteful investments.

The Y2K bug

The story of the Y2K bug[2] became known to almost every inhabitant of the developed world during 1998 and 1999. During the early days of computing, the story went, programmers sought to economise on then-scarce computer storage space by writing dates with two digits for the year instead of four. These programmers either failed to consider the implications of the end of the 20th century or assumed that their systems would have been scrapped long before then.

By the time the problem was taken seriously in the mid-1990s, code with two-digit dates was said to be ubiquitous, occurring not only in conventional computer systems but in 'embedded systems' such as those in automatic lifts, air navigation systems and so on. While the exact consequences of these problems were beyond anyone's imagination, widespread system failures could be anticipated on 1 January 2000, and the cascading effect of these failures was expected to cause, at a minimum, severe economic dislocation.

A typical description of the problem is provided by the House of Commons Library (1998:8):

> Since the early days of electronic computing, almost universally, only 2 digits have been used in computer systems to denote the year in date fields. For example, 1998 is denoted as 98. This practice was adopted to save expensive computer memory storage space and programming time. In the 60s and 70s, adding two century digits to a date field would have required storage space probably five times more expensive than that required for two - a cost difficult to justify when the general opinion was that most systems would be obsolete before the end of the century. As a result, in many applications the Year 2000 could be interpreted as 1900 because the computer is unable to distinguish between these years which would be both be denoted as 00.

Examples of the type of machines that could be affected include:

- Personal computers
- Surveillance equipment
- Lighting systems
- Entry systems
- Barcode systems
- Clock-in machines
- Vending machines
- Dating equipment
- Switchboards
- Safes and time locks
- Lifts
- Faxes
- Vehicles
- Process monitoring systems
- Production line equipment.

A notable feature of the standard account, illustrated by the House of Commons Library description presented above was the way in which a plausible claim about mainframe computer systems, particularly those programmed using the COBOL[3] language that was dominant in the 1960s and 1970s, was extended to personal computers and then to electronic devices of all kinds.

The standard conclusion was that, although the problem was huge in its scope, it could be addressed by a large-scale systematic program designed to ensure, by 1 January 2000, that all computer systems, including microprocessor-dependent equipment items, were compliant. This program could and did, involve the checking and rewriting of millions of lines of computer code and the scrapping and replacement of equipment worth billions of dollars.

A number of objections could be, and were, made to this standard account. First, bugs in computer software are, and always have been, ubiquitous. Social and economic systems have been designed, formally or informally, to deal with, and in some cases to exploit, the unreliability of computer systems. The excuses that 'the computer made a mistake' or 'the computer is down' have become standard elements of the repertoire of strategies designed to deflect blame and unwelcome inquiries in organisations of all kinds.

In systems where failure could not be tolerated, the standard practice has been to build redundant systems of control using independent mechanisms to avoid the possibility of simultaneous failure. Because of their unreliability, solutions based on complex software have been avoided wherever possible. Typical failsafe mechanisms go into the safest possible state when faced with system failure. For example, boomgates at level crossings are designed to drop shut when power is disconnected, preventing access to the railway in the event of a system failure.

Second, calculations involving dates have long been notorious for their complexity and proneness to error. For that reason a competent system design would not be critically reliant on the correctness of date-related calculations.

Of course, not all systems were competently designed and implemented. The kind of simple design that would use a two-digit date to save space would be unlikely to include additional code to handle leap years. Undoubtedly in the years between the first uses of computers in business in the early 1960s and the advent of the Y2K scare in the late 1990s, every leap year had produced numerous incorrect calculations of dates, requiring *ad hoc* repairs to systems or a temporary return to manual systems. The absence of any publicity about problems suggested that all such problems were too minor to be worth reporting.

By contrast, during the Y2K panic, a wide range of date-related problems were watched with anxious concern. For example, computer failures were widely predicted for 1 January 1999 and 9 September 1999, on the basis of purely speculative arguments about coding errors that might have been made (House of Commons Library 1998). The question of why previous 'critical' dates such as leap years had not produced serious problems was ignored. Moreover the fact that these dates passed without incident in the course of 1999 did not influence judgements about the seriousness of the Y2K problem (Quiggin 1999a; 1999b).

A further difficulty with the standard account related to the notion of a cascade of failure occurring on 1 January 2000. Date calculations are most significant in financial systems such as payroll and accounting. Such systems typically include both forward-looking and backward-looking components. Moreover, many systems involve financial year calculations, for which the 2000 fiscal year began in calendar 1999. Thus, it was reasonable to expect Y2K-related failures to be spread over time, rather than occurring simultaneously on 1 January 2000.

Embedded systems played a crucial role in the arguments of those who predicted TEOTWAWKI. By their nature, such systems could not be repaired without scrapping much of the physical infrastructure of modern society. But this very characteristic made it exceedingly unlikely that systems of this kind could be critically dependent on accurate dates. A momentary loss of power such as that associated with the replacement of a battery would reset the date, causing immediate failure in a date-dependent system.

More importantly, experience during 1999 provided a guide to the likely severity of problems in 2000. The absence of any significant Y2K problems, despite the transition to fiscal 2000 for many organisations, some of them poorly-prepared, suggested that severe Y2K problems were unlikely to emerge in 2000. The widely-publicised estimate by Y2K consultants the Gartner Group that 35 per cent of failures would occur during 1999 (Lei 2000) implied that there would be about twice as many failures during 2000 as during 1999. Since there were no failures of critical systems reported during 1999, the best estimate of the number of such failures in 2000, even in the absence of additional remediation, was zero.

Once large-scale failure of embedded systems and the risk of a cascade of failures on 1 January 2000 were discounted as possibilities, there was little need to ensure perfect reliability. A 'fix on failure' approach was therefore worthy of consideration for most systems.

The response

Although the story of the Y2K bug had circulated, since the 1980s, as folklore among those interested in computers, and had been the subject of some serious discussion since then, political attention was not attracted until the late 1990s, by which time the possibility of a low-cost approach to full Y2K compliance had already passed. The leading nation in responding to Y2K, and in promoting international action, was the United States.

At a cabinet meeting in January 1998, President Clinton and Vice President Gore discussed with the cabinet the importance of Federal agencies being prepared for the transition to the Year 2000 and noted the responsibility of each agency head for the achievement of that goal. On February 4, 1998, by Executive Order 13073, President Clinton created the President's Council on Year 2000 Conversion to address the broader picture of how the Y2K challenge could affect information systems in the United States and around the world. The council's formal charge was to coordinate the Federal Government's overall Year 2000 activities. The Council further bolstered its outreach efforts to key infrastructure sectors with the January 1999 formation of its Senior Advisors Group (SAG), which was made up of more than 20 Fortune 500 company CEOs and heads of major national public sector organisations.

In response to survey data that indicated that many small businesses were not ready for the date change, the council worked closely with the Small Business Administration (SBA) and others to encourage greater Y2K activity among the nation's more than 23 million small businesses. The council led two special 'Y2K action weeks' in October 1998 and March/April 1999 (President's Council on Year 2000 Conversion 2000).

The United Kingdom and Australia adopted similar programs. The UK program involved the establishment of a government agency, Action 2000 and an associated private sector body, Taskforce 2000. In 1997, Action 2000 received funding of 70 million pounds (about $A200 million) for one of its initiatives, a training program for small and medium-sized businesses (House of Commons Library 1998).

The Australian response is described in Year 2000 (Y2K) Project Office (2000). The estimated cost of the Commonwealth Y2K program was $544 million of which $530 million was allocated to remediation within the Commonwealth and the remainder to programs promoting Y2K compliance in the community at large. Considering the size of the Commonwealth government relative to the economy, and the fact that compliance efforts were more systematic in the Commonwealth than elsewhere, this suggests that the official estimate of expenditure of $12 billion for the Australian economy as a whole may have been overstated.

The response to Y2K problems in non-English speaking countries was slower and less enthusiastic. Italy was generally considered the least well prepared, and attracted considerable criticism. The official body created to deal with Y2K met for the first time only in February 1999. Its head, Enrico Bettinelli, estimated that with months to go before the end of the year only 15 per cent of Italians knew what the millennium bug was and only 20 per cent thought it a serious problem (BBC News 1999). Remediation efforts were confined to critical systems, and, even in these systems, efforts were viewed as inadequate by most advocates of a serious Y2K effort. In Eastern Europe and less developed countries, the Y2K problem was almost entirely ignored in view of the more pressing concerns facing these countries.

The reaction of the English-speaking countries to the perceived neglect of the Y2K problem in the rest of the world was twofold. First, increasing pressure was applied, with modest success, to accelerate work on Y2K compliance. Second, warnings against travel to these countries were also issued by a number of official and private bodies concerned with the Y2K problem. On 8 November 1999, the quasi-official private sector body Taskforce 2000 advised travellers to avoid Italy, Germany and a number of other countries for a five-week period around 1 January 2000 (Hoffman 1999). In addition, the US and Australian governments announced, and partially implemented, plans to evacuate all but essential embassy staff in some non-compliant countries, as well as issuing travel advisories for their citizens (United States Embassy to Australia 1999).

As 1 January 2000 began, it rapidly became apparent that these warnings were unnecessary. By the time the date change was approaching in New York, the countries of Europe, which had done little or nothing to mitigate the effects of the Y2K problem, were evidently unaffected by computer failure.[4] Non-compliant small businesses, schools and other organisations experienced few, if any, problems when they reopened early in the New Year.

Evaluation

Despite Commonwealth government