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

expenditure of $600 million and an estimated total expenditure of $12 billion in Australia there was no *ex post* evaluation of the costs and benefits of the Y2K remediation program. The accounting for this massive program consisted of a 17-page report (Year 2000 (Y2K) Project Office 2000) and an accompanying press release, both self-congratulatory in tone, and lacking in any attempt at benefit–cost analysis.

The situation was similar in the United States. The President's Council On Year 2000 Conversion issued a final report in March 2000. As in the Australian case, the report (of about 30 pages, excluding appendixes) was primarily devoted to a summary of the activities of the council. However it included a brief response to criticisms that the Y2K problem had been overstated. This included a list of minor glitches that had arisen and short responses to a number of questions raised in the wake of the trouble-free rollover. It is worth quoting one of these in full (President's Council On Year 2000 Conversion 2000):

> Why weren't there more problems among small businesses? Small business was another area about which many, including the Council, had expressed concerns. While there were relatively few reports of Y2K-related failures among small businesses, for firms large and small, there is a natural inclination not to report problems that are fixed in very short time frames. This phenomenon was revealed before the rollover when surveys showed that over 70 percent of companies reported they had experienced Y2K glitches, even though the public was unaware of virtually all of them. Some said the number of failures indicated the pervasive nature of the Y2K problem. The Council believed that the experience of companies with Y2K failures before January 1, 2000 also demonstrated that most Y2K problems could be fixed without people being inconvenienced or even knowing that anything had happened.
>
> The lack of information about how small businesses were doing was an ongoing challenge for the Council and others following Y2K. The sheer number of these companies - over 23 million - and the absence of regular reporting relationships that made it difficult to gather information on the progress of small businesses prior to January 1, also made it difficult to determine how many actually experienced Y2K difficulties after the date change:

The obvious implication of this response is that most small businesses successfully implemented a 'fix on failure' strategy. Such a strategy would have been appropriate for the vast majority of systems in large businesses and government agencies, excepting a few mission-critical systems requiring continuous real-time availability.[5]

The absence of significant Y2K related problems in countries without significant compliance programs was also considered. A suggested explanation was that these countries were less technically advanced and therefore less vulnerable to Y2K related disruption. Such a claim might plausibly be made in relation to very poor countries with few computers, but it is absurd in relation to OECD countries like Italy, where computers are ubiquitous, even if less so than in the United States. Moreover, among countries with significant use of computers, the standard account of the Y2K problem implies that the problems should have been worst in the least advanced countries: those with heavy reliance on old mainframe systems and 'legacy' code from the 1970s and 1980s.

A related argument is that countries with limited efforts were able to 'piggyback' on the resources and information developed by the United States. Again this seems inconsistent with an account in which detailed checking of vast numbers of individual devices was crucial. Moreover, it raises the question of whether Australia should not have emulated the strategy adopted by Italy and other 'piggybackers'.

Why Y2K ?

It seems clear in retrospect that the response of English-speaking countries to the Y2K bug was based on gross overestimates of the seriousness of the problem and an excessively hasty dismissal of the 'fix on failure' solution normally used to deal with potential software bugs. Moreover, the evidence on which such a conclusion might be based was widely available before 2000, and was clearly decisive by mid-1999. It is necessary, then, to consider

the factors leading to adoption of such costly and unnecessary measures.

Public choice theory

A common approach to problems of this kind is based on public choice theory. The central idea of public choice theory is that lobby groups form to pursue policies which will yield large benefits for members of the group, which is assumed to be small. Although the costs of these policies typically outweigh the benefits, they are assumed to be widely dispersed, so that no individual incurs a loss sufficient to motivate resistance (Mueller 1979). The interest group model has been criticised by Quiggin (1987) and defended by Brennan and Pincus (1987).

It is true that, by the end of the 20th century, there was a substantial interest group that benefited from the promotion of aggressive Y2K remediation programs. However, this group merely amplified and took advantage of a concern that was already well-developed. They did not engage in extensive lobbying or political 'logrolling' to promote Y2K programs. Thus, the interest group approach does not seem to be particularly helpful at an aggregate level.

Information asymmetry and organisational structure

It is more useful to focus on the incentives facing individuals and groups within organisations in considering the formation of a social consensus on the need for Y2K mitigation. An obvious feature of those incentives was their asymmetrical nature.

Individuals and groups who argued for a 'fix on failure' approach stood to benefit only modestly if this approach avoided unnecessary costs, but faced the risk of blame in the event of significant system failures attributable (accurately or otherwise) to Y2K related problems. Conversely, it was evident in advance that there was little risk of loss to individuals who advocated comprehensive remediation. The absence of any serious Y2K problems could always be attributed to the success of the remediation program.

The asymmetry of incentives was amplified by the possibility of litigation, particularly in the United States and, to a lesser extent, in other English-speaking countries. The reliance of the United States on tort litigation as a method of compensating those experiencing adverse outcomes of various kinds produces a strong bias in favour of 'defensive' expenditures. In particular, jurors have been highly unsympathetic to individuals and organisations that have chosen to disregard known low-probability risks.

The special characteristics of the Y2K problem were ideally suited to produce this kind of reaction. On the one hand, the problem was both widespread and comprehensible to non-experts, such as potential jurors. On the other hand, if 'embedded systems' are disregarded, the Y2K problem differed from most other computer 'bugs' in that a complete solution was feasible, though very expensive.

In these circumstances, litigation against organisations that had failed to undertake comprehensive Y2K remediation, and experienced any form of system breakdown in early 2000, was virtually guaranteed of success. By contrast, the risk of blame being allocated to organisations that overspent on Y2K remediation was perceived to be minimal. The absence of litigation or other processes for the allocation of blame in the aftermath of the Y2K non-event shows that this perception was accurate.

Thus, the Y2K problem has both similarities and differences with the lobbying problems considered in public choice theory. The outcome can be understood in terms of incentives, as in rational choice theory. However, the problem is not so much one of concentrated interests as of the public-good nature of information. Society as a whole would have benefited if more people had been willing to take a sceptical viewpoint. However, the potential costs of unjustified scepticism would be borne, in large measure, by the sceptics themselves, while the benefits of justified scepticism accrued to society as a whole.

Moral panic

The panic over Y2K shared some, but not all, of the characteristics of the 'moral panics' first analysed by Cohen (1972). Cohen (1972:9) defines a moral panic as 'a condition, episode, person or group of persons [who] become defined as a threat to societal values and interests.' With the Y2K bug, as with the panic over Mods and Rockers studied by Cohen, a problem of which the general public had been largely unaware and that those directly involved

had regarded as relatively minor suddenly became a concern of the media and political actors, and was represented as a serious threat to society.

On the other hand, unlike moral panics focused on social deviance, there was no obvious folk devil. The bug itself was an abstraction. The programmers whose drive for efficient coding led them to use two-digit dates were not, in most popular accounts of the Y2K problem, presented as culpable for failing to foresee that their code would still be in use in the 21st century. The absence of any obvious folk devil suggests that deviance may not be an essential component of moral panics.

An important point raised by the debate between Waddington (1986) and Hall *et al.* (1978) regarding moral panics over youth gangs and street crimes is whether the term 'moral panic' involves a prejudgement that the problem in question has been overstated. Waddington observed that there had in fact been an increase in street crime in the period in question, and suggest that the use of the 'moral panic' category by Hall *et al.* was an attempt to downplay the resulting concern.

The claim underlying moral panic theory is that there is a systematic tendency, arising from the nature of the mass media and political processes, to overstate some kinds of threats, particularly those involving new and unfamiliar dangers. The experience of the Y2K problem supports this view. Although sceptics had sound arguments, they were not such as to command significant media coverage. By contrast both the alarmist advocates of TEOTWAWKI and the officials committed to a large-scale remediation program received extensive coverage.

Risk society

In many ways, the standard account of the Y2K bug would appear to be an ideal illustration of the model of the 'risk society' put forward by Beck (1992). Conversely, the extent to which risks were overestimated in this case must raise questions as to whether Beck's model involves a similar bias towards overestimation of risks.

Although Beck (1999) does not discuss the Y2K bug, the analysis put forward by some writers on Y2K, particularly the partisans of TEOTWAWKI, has similarities with Beck's discussion of the risk society. In much of the TEOTWAWKI analysis, the Y2K bug was seen as a scourge that would sweep this society away, allowing the emergence of a better and simpler alternative. In some cases, this was supplemented by apocalyptic millenarianism, as in the writing of Christian fundamentalist Gary North (North 2000).

Few policymakers paid serious attention to the claims of North and similar writers. On the other hand, the very existence of such writers permitted the advocates of large-scale, comprehensive remediation programs to present, and view, themselves as the sensible centre, and to dismiss the advocates of 'fix on failure' as extremists on one wing of the debate, comparable to the apocalyptic school on the oth*er.*

The precautionary principle

The adoption of a large-scale response to the putative problem of Y2K might be justified in terms of the precautionary principle, commonly advocated in relation to environmental risks. Although there is no generally agreed definition (VanderZwaag (1999) identifies fourteen different definitions) the central idea is that where there is doubt about the reality or severity of an environmental threat, the burden of proof should be on those arguing against a risk-mitigating response. A range of issues in relation to the precautionary principle are discussed by Quiggin (2004).

Although the precautionary principle was not formally invoked in most discussions of the Y2K bug, similar reasoning seems to have applied. The observation that most of the Y2K remediation effort was wasted or misdirect therefore suggests some issues that may be relevant in environmental and other applications of the precautionary principle.

Most importantly, application of the precautionary principle should not be used to justify a comprehensive attempt to reduce risk to zero. In cases where the reality of the risk is in doubt, it is important to consider the severity of the possible outcomes. In the case of Y2K, careful consideration would have revealed the possibility of combining a vigorous remediation effort for mission-critical systems with a general policy of watchfulness and 'fix on failure'.

Why was the Y2K panic confined to English-speaking countries?

As has been discussed above, only in English-

speaking countries did the Y2K bug produce widespread public concern and elicit a systematic official response on a large scale. Two factors help to explain this observation.

First, because of common language and historical ties, ideas tend to flow more rapidly between English-speaking countries than between English-speaking and non-English-speaking countries. Reports from the United States promoting concern about Y2K were typically reproduced in the Australian press within a matter of days, especially in the latter phase of the crisis when most newspapers had special 'Bug Watch' columns, devoted specifically to this topic.

Second, similar causes operated similarly. Although the United States relies more on tort litigation as a method of social regulation than any other country, tort law also plays a prominent role in other English-speaking countries, and there is some degree of mutual recognition of precedent. Thus, Australian enterprises considering a 'fix on failure' strategy faced similar risks to those of their American counterparts. By contrast, this risk was considerably smaller in countries without a common law tradition of tort litigation.

Could we do better ?

In retrospect, it is possible to see why collective judgements regarding the Y2K problem were so badly wrong and so resistant to the accumulation of contrary evidence. It is more difficult to see how such poor collective judgements can be avoided in the future. Nevertheless, some positive suggestions can be made.

First, the Y2K episode is an illustration of the dangers of relying on a blame-allocation system such as tort litigation as a method of social regulation. The knowledge that any decision that knowingly involves taking a risk will be the subject of blame if the risk turns out badly leads in some cases to deliberate obscurity in decision-making processes, allowing for denial of responsibility and in other cases, such as Y2K, to a bias towards 'defensive' policies. The best-known case of this process is the practice of 'defensive medicine' in response to malpractice suits. The limited success of tort law reforms in this and other areas is indicative of the depth of reliance placed by English-speaking countries on litigation as a process for allocating both blame and compensation for decisions with adverse outcomes.

Second, the Y2K failure suggests that, in situations where there is strong pressure to conform with a consensus, some form of institutionally sanctioned scepticism is necessary.

The generic term for someone willing to argue against a consensus position is 'devil's advocate', and the history of this term reflects the fact that the canonisation process in the Catholic church is one which naturally generates enthusiastic support. The office of the Promotor Fidei, popularly referred to as the 'Devil's Advocate', was instituted to provide a sceptical check on such enthusiasm by collecting and presenting evidence against candidates for canonisation[6]. In the criminal legal system, scepticism is institutionalised through rules that ensure legal representation, even for criminal defendants who are viewed by the community as 'obviously guilty'.

Third, the Y2K program illustrates the general problem of inadequ*ate ex* post project evaluation. Official estimates suggest that the Australian Y2K program involved expenditure of $12 billion. Yet the only official report published in Australia would have been rejected as grossly inadequate if it had been published as an account of the annual operations of a minor local council or small company. The need for ex post evaluation is particularly evident in the case of preventative programs such as Y2K.

It seems unlikely that, even if such measures had been in place, excessive expenditure on Y2K preparedness would have been avoided. However, it is possible that, if greater scepticism were embedded in the policy processes, total expenditure would have been reduced and the proportion of that expenditure that was devoted to general disaster preparedness, rather than to specific policies of Y2K compliance, would have increased.

Conclusion

The Y2K scare has been interpreted in many different ways. Some have seen it as a cautionary example of the vulnerability of modern civilisation, while others have treated as a simple scam perpetrated by consultants hustling for business.

From the perspective of public administration, the two most compelling observations relate to conformity and collective amnesia. The response to Y2K shows how relatively subtle characteristics of a policy problem may produce a conformist response in which no policy actors have any incentive to oppose, or even to critically assess, the dominant view. Moreover, in a situation where a policy has been adopted and implemented with unanimous support, or at least without any opposition, there is likely to be little interest in critical evaluation when it appears that the costs of the policy have outweighed the benefits.

There are no simple organisational responses that would have a high probability of producing a radically different response to a future problem similar to the Y2K scare. Nevertheless, innovations designed to enhance organisational scepticism might achieve a better balance between costs and benefits in cases of this kind**.**

References

BBC News 1999, Italy: Tourists and Flights, read on 18 December 2003 at http://news.bbc.co.uk/hi/english/static/millennium_bug/countries/italy.stm/

Beck, U 1992 *Risk Society: Towards a New Moder*nity, Trans. M. Ritter, Sage Publications, London.

Beck, U 1999 *World Risk Soci*ety, Polity Press, Cambridge.

Cohen, S 19*72, Folk Devils and Moral Pan*ics, MacGibbon and Kee, London.

Brennan, G and J Pincus 1987 'Rational actor theory in economics: A critical review of John Quiggi*n', Economic Re*cord ,63 (180), 22-30.

Campbell, I 2000 'Putting The Bug To Bed: Under Budget', Media Release, Parliamentary Secretary to the Minister for Communications, Information Technology and the Arts, Canberra.

Co-Intelligence Institute 2000 What Happened to Y2K? Koskinen Speaks Out, transcript of interview with John Koskinen, read on 18 December 2003 at http://www.co-intelligence.org/y2k_KoskinenJan2000.html.

Fist, S 1998a 'BBC Time Bomb', *The Australian,* September , read on 18 December 2003 at http://www.abc.net.au/http/sfist/cxy2k1.htm

Fist, S 1998b 'Apocalyptic Visions', *The Australian,* 20 January, read on 18 December 2003 at http://www.abc.net.au/http/sfist/y2k.htm.

Hall, S *et al.* 1978 *Policing the Crisis: Mugging, the State, Law and O*rder, Holmes & Meier, New York.

Goodwin, B 2000 'Was Y2K a costly non-event?', computerweekly.com, 13 January, read on 18 December 2003 at http://www.computerweekly.com/Article22154.htm.

Hoffman, T 1999' Germany, Italy get Y2K 'red light' travel warnings,' *Computerworld,* Nov 8, 1999 read on 18 December 2003 at http://www.cnn.com/TECH/computing/9911/08/redlight.y2k.idg/

House of Commons Library (1998), 30 June 1998, The millennium bug', Research Paper 98/72.

Lei, T 2000 'Caution reigns as Y2K bug remains silen*t', Computerwo*rld 6(11), 14 - 20 January 2000,, read on 18 December 2003 at http://www.computerworld.com.sg/.

Mueller, D 1979 *Public Choice*, Cambridge University Press, Cambridge.

North, G 2000 'Gary North's Y2K Links and Forums', http://www.garynorth.com/y2k/.

President's Council on Year 2000 conversion 2000'The Journey to Y2K: Final Report of the President's Council on Year 2000 Conversion', read on 18 February 2004at http://www.y2k.gov/docs/LASTREP3.htm.

Quiggin, J 1987'Egoistic rationality and public choice: a critical review of theory and evidence', *Economic Record* 63(180), 10–21.

Quiggin, J 1999a 'Y2K bug may never bite', *Australian Financial Review,* 2 September.

Quiggin, J 1999b 'Panic merchants owe us a bottle', *Australian Financial Review*, 30 December.

Quiggin, J 2004 'The precautionary principle and the theory of choice under uncertainty, Working Paper 10/R04, Risk and Sustainable Management Group. University of Queensland

United States Embassy to Australia 1999 'Transcript: State Department Briefing on Y2K Preparations', read on 18 December 2003 at http://usembassy-australia.state.gov/hyper/WF991221/epf202.htm).

Waddington, P 1986'Mugging as a moral panic: a question of proportio*n', British Journal of Socio*logy, 37(2), 245–259.

VanderZwaag, D 1999 'The precautionary principle in environmental law and policy: elusive rhetoric and first embraces', *Journal of Environmental Law and Practice*, 8, 355–75.

Wikipedia 2004 Computer Bug, http://en.wikipedia.org/wiki/Computer_bug, read on 22 September 2004.

Yardeni 1997 Testimony to Senate Banking, Housing and Urban Affairs Committee, http://banking.senate.gov/97_11hrg/110497/witness/yardeni.htm

Year 2000 (Y2K) Project Office (2000), 'Year 2000 Round-up Report Year 2000 Round-up Report - final report', Department of Communications, Information Technology and the Arts< Canberra.

Notes

[1] This terminology was popularised by Jobn Koskinen, the US Administration's Y2K Co-ordinator. Speaking shortly after 1 Jan 2000 he restated a position he had consistently espoused It was clear two years ago to me after talking with a lot of experts, if nobody did anything else beyond what they had already done up until two years ago, that the world as we knew it would end. (Koskinen 2000).

[2] Wikipedia (2004) describes a computer bug as follows:
A computer bug is an error, flaw, mistake or fault in a computer program which prevents it from working correctly ... Usage of the term "bug" to describe inexplicable defects has been a part of engineering jargon for many decades.
As with popular accounts of the Y2K bug, the widely-known account of the general term 'bug' that traces the use of the term to the discovery of an actual insect in a malfunctioning computer is inaccurate.

[3] The popularity of COBOL had declined greatly by the 1990s, but there were still many 'legacy' systems programmed in COBOL and running on mainframe computers, notably in financial applications, which could be expected to be vulnerable to date errors.

[4] An Australian government report later noted the appearance of a Slovenian weekly magazine with an incorrect publication date .

[5] A mission-critical application is one that is critical to the proper running of a business. Real-time availability means that the program must respond continuously to new data rather than being run in 'batch' mode, at regular intervals. An example of a mission-critical real-time system is an aeroplane's onboard navigation system.

[6] Pope John Paul II abolished this office in 1983 and subsequently consecrated more saints than the combined total of his predecessors since the 16th century. This suggests that the work of the Promotor Fidei represented a significant obstacle to canonisation.

*I thank Nancy Wallace and an anonymous referee for helpful comments and criticism.
This research was supported by an Australian Research Council Federation Fellowship