Risk & Sustainable Management Group

Australian Public Policy Program Working Paper: 1/P04

The Y2K scare: causes, costs and cures

John Quiggin

Schools of Economics and Political Science
University of Queensland
Brisbane, 4072
rsmg@uq.edu.au
http://www.uq.edu.au/economics/rsmg

This version:18 February 2004

The Y2K scare: causes, costs and cures

John Quiggin

Australian Research Council Federation Fellow

School of Economics and School of Political Science and International Studies

University of Queensland

Risk & Sustainable Management Group

Australian Public Policy Program Working Paper: 1/P04

This research was supported by an Australian Research Council Federation Fellowship

The Y2K scare: causes, costs and cures

Abstract

The worldwide scare over the ‘Y2K bug’ result in the expenditure of hundreds of billions of dollars on Y2K compliance and conversion policies. Most of this can be seen, in retrospect, to have been unproductive or, at least, misdirected. In this paper, 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.

The Y2K scare: causes, costs and cures

As midnight approached on 31 December 1999, the world prepared to celebrate the dawn of a new millenniun[1]. 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 and, in more apocalyptic accounts, The End of The World As We Know It (TEOTWAWKI).

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 much 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. Within circles devoted to debating Y2K issues, members of this group were often labelled 'Pollyannas'.

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, confirmed this view.

[1] A small group of pedants abstained, arguing that the new millennium would not begin until 2001.

Over time, however, it has been widely accepted that the Pollyannas had been vindicated by events. The number of Y2K-related problems was so minuscule that Y2K programs that had been planned to continue for years were wound up within months after the advent of Y2K. Moreover, 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 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 reforms that would reduce the likelihood of similar episodes in future. This paper 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 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 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 descriptions of the problem is provided by Baylor College of Medicine (1999)

> The Year 2000 (Y2K) problem results from computer systems that were designed to use years represented by two digits instead of four. When the software was designed, a two-digit year assumed the year was in the 1900s. This causes a problem when a two-digit year is meant to begin with 20 instead of 19.
>
> In the early days of programming, dates were often stored with two-digit years to conserve on computer memory. Memory used to be very expensive. The practice of storing two-digit years continued. Some applications may have been written using four-digit years but used commercial tools and compilers that were not year 2000 compliant.
>
> In addition to PCs, mainframes, and servers, the Y2K problem affects other devices that have microprocessors; for example, laboratory equipment, biomedical devices, alarm systems, heating/cooling systems, etc. Software applications and hardware devices that are not year 2000 compliant may fail or produce incorrect results.

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 crossing 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, at the height of Y2K hysteria, a wide range of date-related problems

were watched with anxious concern. For example, computer failures were widely predicted for 9 September 1999, on the basis of purely speculative arguments about coding errors that might have been made. The question of why previous 'critical' dates such as leap years had not produced problems was ignored.

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.

As the debate progressed, some of these points were taken into account by advocates of a large-scale response. Since there was nothing that could be done about embedded systems, the fact that they were basically immune from date-related failure was accepted fairly readily.

Similarly, the 'simultaneous failure' model of Y2K was discarded in favour of one in which about one-third of failures could be expected to occur during 1999. The Gartner group, a consultancy firm that played a leading role in promoting concern about Y2K and in supplying advice on Y2K compliance programs (Luening 1998), estimated that only about 10 per cent of Y2K problems would occur on 1 January 2000, with 55 per cent occurring during 2000 and 35 per cent during 1999 (Lei 2000).

However, the implications of these adjustments to the Y2K story were never considered. Once large-scale failure of embedded systems was discounted as a possibiity, there was little need to ensure perfect reliability. A 'fix on failure' approach was therefore worthy of consideration for most systems.

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 estimate that 35 per cent of failures would occur during 1999 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.

The response

Although the story of the Y2K bug had circulated as folklore among those interested in computers since the 1980s, 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 organizations.

In response to survey data that indicated 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. With the help of SBA, the Commerce Department, the U.S. Department of Agriculture (USDA), and other Council agencies, the Council led two special "Y2K Action Weeks" in October 1998 and March/April 1999. (President's Council on Year 2000 Conversion, 2000)

Australia and other English-speaking countries adopted similar programs. The Australian response is described in 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 1998).[2] Remediation efforts were confined to critical systems, and, even in these systems, efforts were viewed as inadequate

[2] That is, 80 per cent were correct in their evaluation.

by most advocates of a serious Y2K effort. On 8 November, 1999, Taskforce 2000, a UK-based business group, advised travellers to avoid Italy, Germany and a number of other countries for a five-week period around 1 January 2000 (Hoffman 1999).

In Eastern Europe and less developed countries, the problem was almost entirely ignored in view of the more pressing concerns facing these countries. Warnings against travel to these countries were also issued by a number of official and private bodies concerned with the Y2K problem.

The sceptics

As has already been observed, the standard account of the Y2K problem was not universally accepted in the period before the problem became a major policy issue. As large-scale Y2K remediation programs were implemented throughout the English-speaking world in 1998 and 1999, criticism grew correspondingly more vigorous. Nevertheless, the volume of criticism from Y2K sceptics was tiny in comparison with the output of those who either endorsed the official position or criticized the official effort as being inadequate.

In Australia, for example, most daily newspapers incorporated regular (mostly weekly) columns with titles such as BugWatch which provided news on the progress of official Y2K effort, links to international news items and so forth. The only regular commentators to express skepticism were Fist (1998a,b) and Quiggin (1998, 1999 a,b). Graeme Bond, a Melbourne computer analyst, with responsbility for a major Y2K program, also contributed skeptical comments to the media. These contributions were almost completely ignored.

Internationally, the picture was similar. Although there was vigorous debate on Internet newsgroups such as comp.software.year-2000.tech and the self-explanatory alt.y2k.end-of-the-world, skeptical views were slow to emerge and had little, if any, effect in promoting a more measured, and less costly, response to the problem.

Nevertheless 1 January 2000 approached, the tone of commentary became marginally

more skeptical. For example the lead article in a survey presented by CNET news.com (Leuning, Ricciuti and Yamamoto 1999) opened with the observation that "

> just weeks away from the red-letter date, much of the initial hype has subsided. Although some problems have appeared, many experts believe that serious damage from the most celebrated bug in high-tech history will be minimal. Which raises an irresistible question: Was all the money spent to trumpet Y2K crises really necessary?

Policy responses were also modified in ways that implied a downgrading of the threat. For example, a number of Western countries had made, and partially implemented, plans to evacuate diplomatic staff from countries in Eastern Europe considered vulnerable to failure. Although these countries made little or no additional remediation effort in the second half of 1999, evacuation policies were quietly abandoned in a number of instances.

The millennium and the aftermath

As 1 January 2000 began in New Zealand, it rapidly became apparent that the Y2K bug was a non-event. By the time the date change was approaching in New York, the countries of Eastern Europe, which had done little or nothing to mitigate the effects of the Y2K problem, were evidently unaffected by computer failure.[3]

With the exception of the TEOTWAKI advocates, many of whom disappeared from view, few commentators on Y2K changed their position in the immediate aftermath of the uneventful turnover. The officials in charge of Y2K preparedness declared their satisfaction that their programs had been so successful, and suggested that there had been a beneficial effect extending to those who had failed to prepare (Co-Intelligence Institute 2000).

In addition, defenders of the program predicted the emergence of further problems as 2000 progressed. Goodwin (2000) adjusted the earlier Gartner group estimates, cited

[3] an Australian government reported later noted the appearance of a Slovenian weekly magazine with an incorrect publication debate, but this event passed without notice amid the revelry of New Year's Eve.

above, and suggested that only 5 per cent of problems had emerged. He listed sixteen critical dates during 2000. Particular attention was paid to February 29, 2000 on the grounds that computer programs might fail to recognise that 2000 was a leap year[4].

The sceptics pointed out the confirmation of their predictions, not only with respect to the absence of Y2K problems throughout the world, but with respect to the reactions of those responsible for Y2K compliance programs who had claimed that it was only their precautions that had prevented disaster.

As 2000 progressed with Y2K and other date-related problems still notable only for their absence, the tenor of public discussion began to change. Y2K programs that had been planned to continue for several years were closed down within months. A survey by CMP Media of 1,750 IT professionals and consumers showed that 63 percent believed that Y2K was mostly hype (Berkowitx 2000).

By 2003, the proposition that Y2K fears were overblown was fairly generally accepted. A sample of 160 news stories referring to Y2K in October 2003 (Google news) shows that the majority of stories (over 100) either refer to the "Y2K scare" as an instance of unfounded concern or to the "Y2K boom" in equipment spending, and the subsequent downturn. A smaller number of articles point to the benefits of Y2K preparations as a training run for actual emergencies such as the terrorist attacks of September 11, 2001.

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

[4]In the Gregorian calendar, which replaced the earlier Julian system, every fourth year is a leap year with the exception that years which are multiples of 100, but not of 400 are not leap years. Programmers who wrote their own date program, rather than calling on standard system routines, and used neither the Gregorian nor the Julian system, but a hybrid excluding all multiples of 100 would produce the stated error. The fact that such a remote possibility, producing an error of a kind that occurs routinely from all manner of causes would be taken seriously is an indication of the mania that surrounded the Y2K problem.

and benefits of the program. The accounting for this massive program consisted 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 overhyped. 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.

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 third 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 adopted to 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.

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 criticized 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 amplifed 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. 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 skeptical viewpoint. However, the potential costs of unjustified skepticism would be borne by the skeptics themselves, while the benefits of justified skepticism accrued to society as a whole.

International comparisons and impacts

These tendencies were most evident in English-speaking countries, for a number of reasons. 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 ligitation.

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. In the leadup to January 1, 2000, 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).

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 arises, some form of institutionally sanctioned skepticism is necessary. The generic term for somone willing to argue against such a 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 skeptical check on such enthusiasm by collecting and presenting evidence against candidates for canonisation[5]. In the criminal legal system, skepticism 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 inadequate *ex post* project evaluation. Official estimates suggest that the 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 skepticism 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.

Concluding comments

The Y2K scare has been interpreted in many different ways. Some have seen it as a

[5] Pope John Paul II abolished this office in 1983 and has now 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.

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 skepticism might achieve a better balance between costs and benefits in cases of this kind.

References

Baylor College of Medicine (1999), Description of Y2K Problem, read at http://www.bcm.tmc.edu/it/y2k/y2kdesc.html, June 15, 2003 (available in Google cache, 18 December 2003).

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/

Berkowitz, B. (2000), Post-Mortem: The Bug Appears to Be Beaten, USC Annenberg Online Journalism Review, read on 18 Feb 2004 at <a href="http://www.ojr.org/ojr/technology/1017966298.php">:

Brennan, G. and Pincus, J. (1987), 'Rational actor theory in economics: A critical review of John Quiggin', *Economic Record* ,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. (1998), 'BBC Time Bomb', *The Australian,* September , read on 18 December 2003 at http://www.abc.net.au/http/sfist/cxy2k1.htm

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

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/

Lei, T. (2000), Caution reigns as Y2K bug remains silent, *Computerworld* 6(11), 14 - 20, January 2000, read on 18 December 2003 at http://www.computerworld.com.sg/pcwsg.nsf/0/8FBCDBF1B69513BB48256B-4F002AE3BC?OpenDocument,

Luening, E. (1998), Y2K study paints grim picture, CNET News, 5 August, read on 18 December 2003 at http://news.com.com/2100-1001-214132.html?legacy=cnet

Leuning, E., Ricciuti, M. and Yamamoto, T. (1999), Everyone pays a price for Y2K hype, CNET News, 9 November, read on 18 December 2003 at http://news.com.com/2009-1091-232056.html?legacy=cnet

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

President's Council on Y2K 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. (1998), Y2Ks nasty legal side effects, *Australian Financial Review*, November 5.

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.

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)

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