Introduction and Abstract

Project Management System 2004 is a business database designed to facilitate the management of large-scale projects and their associated personnel. In particular, because of its sophisticated file-handling capabilities, it is targeted at software development projects.

The fundamental purpose of any database is to store and retrieve information on command. Our system is a flexible and practical software tool that can be adapted to suit a variety of uses, not all of which would be considered ethical by industry codes of ethics or by a reasonable person. In addition, unethical practices, such as breaches of privacy, may occur even with the storage of legal and legitimate information. It is because of such possibilities that the developers of the system have been forced to consider restrictions or other means of preventative measures, taking into account the conflicting interests of all stakeholders and technical limitations. The main argument against restriction or prevention is that this software application is a generic tool, and any such restrictions will limit its overall functionality, ease of use and adaptability.

This report examines the *unethical usage of information stored for legitimate purposes*, and *outright unethical or illegitimate usages*, and offers an evaluation of potential solutions. Where practicable, the ACS (Australian Computer Society) Code of Ethics acts as an impartial yardstick on which to base our comparisons.

"There now. We get our wish of continuing our work unimpeded, and they get their wish of being in a position of direct oversight at all times."

Figure 1 Ethics can be a barrier at times, but it should not be swept under the carpet and ignored. [http://www.nearingzero.net/screen_res/nz135.jpg]

Unethical Usage of Legitimate Information

Legitimate Data Stored in the Database

Intended uses of the database include business organisation, project scheduling, event management, personal timetabling and other business functions. These uses assume that all users are using the software collectively in a constructive and good-willed manner towards business success, and information about the business is stored in good faith in the database to facilitate the running of the business. In particular, data that may be stored in the database includes personal and business attributes of individuals, sensitive business secrets and confidential files.

Conflicts of Interest

In general, it is clear that the owners of information and computer files stored on the system would like it to be stored with integrity and confidentiality, and with a consideration to privacy; they are stakeholders whose interests must be considered. In addition, those who want access to the data must also be considered, and are also stakeholders.

This conflict is codified in the ACS Code of Ethics[1], in which there are numerous references to the ethical storage of information, highlighting its importance in today's world. These include:

- **4.5.2** – I must endeavour to preserve the integrity and security of the information of others.
- **4.5.3** – I must respect the proprietary nature of the information of others.
- **4.5.4** – I must endeavour to preserve the confidentiality of the information of others.
- **4.8.2** – I must consider and respect people's privacy which might be affected by my work.

In addition, laws such as *Privacy and Personal Information Protection Act 1998* (NSW) would need to be taken into consideration as to the lawful use of the information.

Even here, conflicting interests are codified:

- **4.6.1** – I must endeavour to provide products and services which match the operational and financial needs of my clients and employers.

Collation of Business Statistics

Conflicting interests can be seen in a scenario where the mangers and executives wish to analyse the information stored in the system, even if it would be used for an innocuous purpose to which most people would not take offence. This includes the collation of statistics on employee information, or on bottlenecks in the stages of a project.

In light of the ACS Code of Ethics, and personal views on privacy, the development team believes that such behaviour should be at least discouraged, if not prevented, unless the users of the system have given express permission for the information to be used in such a manner. However, as outlined later, due to technical limitations in our system (and any information system), complete prevention of access to information stored in the system is impossible. Indeed, to satisfy 4.6.1, it would be necessary to permit such data collection to be possible if the client so desires, but necessary safeguards will be included, such as an online authorisation form (in the future browser interface) for users to grant such permission easily.

[1] http://www.acs.org.au/national/pospaper/acs131.htm

Data Mining

Another potential use of the system is as a data-mining tool. Although it is unlikely that a business would intentionally compromise its own data, in the public arena, such care cannot always be guaranteed. For example, this software may be used by a company to allow for open source software development. Users register in good faith, but later on, the company sells the information for profit (such as to spammers). Once again, it is in the ordinary users' best interests to disallow such uses unless permission has been granted explicitly. However, this means that the interests of one stakeholder, the company, cannot be met, but this is clearly within reason. Indeed, the consequences of such an event occurring are such that it is proposed that the system contain explicit onscreen warnings to users as they log onto the system to suggest that they consider whether the data repository into which they are entering data is trustworthy. Education and proactive warnings are the keys to ensuring privacy and security.

Intentional Disruption to the Business

A user, especially one with Administrator privileges, may wish to intentionally compromise the system for selfish purposes, such as the sale of corporate secrets, unauthorised rescheduling of critical dates and project deadlines, deletion of records or the access of colleagues' personal data. Clearly, the interests of the other users on the system outweigh an obnoxious user's desire to gain access to the system. Consequently, as outlined in further detail below, there are deterrence and safety mechanisms built into the system to prevent such attacks.

Possible Solutions and Remedies

Access Control

Many of the above activities, if they were allowed to go unchecked would be inconsistent with the ACS Code of Ethics. To prevent such uses, the development team has equipped the database with access control security; many of these ideas are common practice in the industry, such as operating system and web site security.

Access control measures include:

- **Login with password:** Any user of the database software must login to execute any queries. This is to ensure that only appropriate users may perform particular actions in the system. New users may only be created by a user with Administrator privileges.
- **Random password generator:** This service, available at the user interface level, provides a random password to users that have difficulty creating a secure password. This service attempts to minimize the potential for an intruder cracking an easily guessed password. This ensures that unethical and unauthorised uses of the database are minimised to the extent that they can be regarded as remote.
- **"Read", "write", and "modify permissions" lists** are stored as instance fields in each object in the database. These allow or disallow methods called by a certain user to read, write, or modify the permissions for a particular database object. This separation of access levels ensures that the system is flexible enough to allow users to perform their duties in their business, while ensuring data integrity.
- **Administrator only functions:** With regards to ethical use of the information, only Administrators have access to change Access Control Lists (which group users together, such as "Administrators" group) and add or remove users. This is because these two items are fundamental to the access control in this system.

Technical Limitations on Total Prevention of Access

As mentioned above, there are technical limitations to any information system that makes complete prevention of access to information stored in the system impossible. This is because super-user (or in our system, "Administrator") privileges must be conferred on at least one user so that the system can be maintained, new users added and so on. Indeed, in our system, all users in the Administrators group automatically have unfettered access to the entire system. The ramifications of a user abusing such a privilege are a concern (especially since the system administrator is unlikely to be electronically monitored by those higher up in the organisation's hierarchy). Thus, education is a way of preventing such breaches as before, by encouraging system administrators to grant managers full access to only certain sections of the database. In addition, a more-limited, but still powerful, "Power Users" group will be created by default, in order to encourage Administrators to subscribe to this list for day-to-day activities.

Logging

A transaction log would increase security by acting as deterrence to unauthorised activity, as it records all queries executed by all users (without exceptions) during each session. Any attempts to undermine the security of the system will be easily detectable.

Data Security and Integrity

Due to the nature of the client/server system, in which users can connect to the server from any part of the world using a public Internet connection, it is important to ensure that the data arrives at its destination intact and that the packets are not sniffed out and read by hackers. To ensure this, we have decided to utilise Java's built-in encryption, including the practically unbreakable 512-bit RSA and checksums to ensure security and integrity as it is transferred. By ensuring its security and integrity, users of the system can rest assured that their data is not being captured for inappropriate use in transit. Furthermore, to deter hackers, accounts are locked after three failed login attempts in a row, and IP addresses may be blacklisted by the server.

Locally, the data must be stored on disk to ensure persistence. Because fundamentally, the data is stored in XML format, which is human readable, users with super-user access to the host system should not be able to read the data in the file. This also applies to the transaction log. Once again, strong encryption will be used to prevent access to the information in such a manner.

However, there is a competing interest in terms of data integrity. If the data is corrupted, it is far more difficult for the data to be recovered than if it were human readable. The developers have elected to make encryption of the files on disk optional, but turned on by default. This conforms with the ACS Code of Ethics, as there is a strong regard for privacy and security of information, while allowing the end user to use the software as he or she pleases.

Illegitimate Uses

File Sharing

Although Project Management system 2004 does not store files themselves, it facilitates their sharing, as the File Manager table acts similar to a library catalogue that aids borrowers to share books. In this manner, our database software could conceivably be used to break copyright laws by unlawfully sharing and obtaining copyright material, such as music and video files, works of literature, and software. The efficient searching in the system, which includes indexing, makes our software even more attractive to use as a file sharing server.

On the other hand, the file sharing industry is currently experiencing a worldwide boom due to sluggish industry response to consumer demand for new media technologies. Our database software could act as an efficient file server, able to return media details and locations to legitimate paying users over a network.

Conflicts of Interests

In this regard, the law dictates that the copyright holders' rights take precedence over what users may want to do with the system, and prima facie, it would appear that we should prevent such activities from occurring. This is because a database is supposed to allow users to share files efficiently, helping organise computer-related logistical tasks. It is extremely difficult to censor copyright material within the database without dramatically reducing speed and functionality. It would also be contrary to the ACS code of ethics to censor data retrieval, as an automated system that scans the database without the users' notice would potentially be contrary to the following clauses (as well as being abhorrent ethically):

- **4.6.1** – I must endeavour to provide products and services which match the operational and financial needs of my clients and employers
- **4.5.2** – I must endeavour to preserve the integrity and security of the information of others.
- **4.8.2** – I must consider and respect people's privacy which might be affected by my work

Prevention of unethical file sharing with the software

Although the software was never intended to aid illegal activities, it is inevitable that some copyrighted material will be illegally shared. To discourage users from file sharing, when the system boots (both client and server), it displays a warning recommendation discouraging this activity. The development team hopes that potential users may see the message and choose not to do business with any organisations that offer file sharing services.

Unethical software development

Project Management System 2004 has an extensive calendar and event scheduling system that allows software development teams to reach their full potential. While most users of the system would use it for legitimate purposes, there are those with unethical interests. For these users, the system could be used to manage the development of unethical software, such as data miners, spy-ware, and spammers, or even run a reverse-engineering company, contrary to copyright law and licence agreements.

Conflicts of Interest

In accord with the ACS Code of Ethics, Project Management System 2004 attempts to protect intellectual property and the privacy of individuals. The prevention of organised crime lies more within the domain of law enforcement forces. Nevertheless, the programmers recognise that the ramifications of such activities affect all global citizens, but not all countries have an adequate legal system to prevent unethical business practice. From the ACS code of ethics:

- **4.8.2** – I must consider and respect people's privacy which might be affected by my work.

This has effect in that any monitoring of the use of the software may be in breach of this clause.

Prevention of unethical software development with the software

It is difficult (and arguably unethical) to prevent organised crime by decreasing the functionality of the software and censoring the data; keyword filters would simply annoy legitimate users and cause our software to gain a bad reputation as being heavy-handed (for it is uncommon practice to do so). Instead, it is suggested product registration is used as a means for police to track the software use of known criminal organisations when legally permitted. However, criminals may forge an application form, and legitimate business may be forced to reveal business secrets, breaching confidentiality and privacy. Furthermore, the police may become a stakeholder, in that they may demand the information such business provide for countering terrorism and other criminal activities, by analysing their use of software. Such a thing cannot be allowed.

Conclusion

In conclusion, ethics is an important part of designs of computer systems, as all stakeholders' interests must be evaluated and balanced against each other to achieve a fair and equitable balance between those who have information stored in the system, and those who would like to access or change that data. Even though there may be a legitimate justification for gaining access to such data, it is important that users have the right to say who and access their data and what they can do with it – education, express permissions and access control play important roles. In addition, the developers' ability to counteract blatantly illegal and unethical uses is hampered by the need to ensure that the software is generic and does not perform unethical activities itself by acting in an overbearing 'Big Brother' manner. The ACS Code of Ethics was found to be useful in providing insight into industry standards.