

ARIZONA SUPERIOR COURT, PIMA COUNTY

JUDGE: HON. MICHAEL MILLER

CASE NO. 20072073

COURT REPORTER: NONE

DATE: December 18, 2007

DEMOCRATIC PARTY OF PIMA COUNTY,
Plaintiff,

v.

PIMA COUNTY BOARD OF SUPERVISORS, a
body politic,
Defendant.

UNDER ADVISEMENT RULING

Plaintiff Democratic Party of Pima County brings this statutory special action to compel Defendant Pima County Board of Supervisors ("Pima County") to disclose "every file stored in the Pima County's election computer that ends with the extension "gbf" or "mdb," and the password for "gbf" files." Pima County refused the request on the basis that A.R.S. § 16-445(D) prohibits their disclosure and, in any event, the government interest in secure elections outweighs Plaintiff's interest in the files. The Court conducted a four day trial beginning December 4, 2007 to address the statutory and balancing arguments. The Court also inspected *in camera* on a secure laptop computer the 2006 General Election mdb file using GEMS and Microsoft Access.

This Ruling provides the Court's findings of fact and conclusions of law.

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 2

Date: December 18, 2007

Case No: C20072073

Findings of Fact and Conclusions of Law

1. Plaintiff Democratic Party of Pima County is a political organization recognized by statute. *See* A.R.S. §§ 16-801 to 16-828. The organization includes county representatives selected pursuant to A.R.S. § 16-821. As a political party, Plaintiff is authorized to participate in the accounting and monitoring of elections. *See* A.R.S. §§ 16-602 and 16-603. Plaintiff actively exercises its right to monitor elections and it has offered a variety of recommendations to improve the integrity, transparency, and security of elections in Pima County. The records request for the election computer files arises out of its statutorily-mandated role.

2. Defendant Pima County Board of Supervisors is a body politic. Pursuant to its own regulations, day-to-day functioning is delegated to County employees. *See* Pima County Code 2.12.090. Individual supervisors are prohibited from making or interfering with the functions and decisions of County employees. *Id.* The County Administrator, Charles Huckelberry, has final authority to make individual decisions on specific record requests, such as the request made by Plaintiff. Mr. Huckelberry makes those decisions in consultation with technical advisors and with the advice of counsel.

3. The Pima County Division of Elections is charged with the responsibility of conducting most elections in Pima County. The division head is Brad Nelson. Mr. Nelson is responsible for conducting elections pursuant to state and federal law, organizing the necessary personnel and

Lynne Booth

Judicial Administrative Assistant

RULING

Page: 3

Date: December 18, 2007

Case No: C20072073

equipment to conduct the election and tally the votes, and planning for secure but transparent elections.

Mr. Nelson answers directly to Mr. Huckelberry.

4. On December 6, 2006 Plaintiff made a written, ten-item records request to Mr. Nelson and the Board chairman. Only the first item is at issue. The requested files are described as follows:

Electronic copies of the Diebold GEMS database for both the primary and general election and backup (if present) Diebold "Central Tabulator" computers. These should be produced on a CD or portable disc drive in the presence of Democratic Party observers and under their supervision. We can bring a blank factory-sealed 100 gig or more USB hard disc for simple transfer of these records.

On January 8, 2007 Mr. Huckelberry informed the Board of Supervisors in a memorandum that the request had been denied:

The County has responded to the public records request of Mr. Risner (attached) regarding Elections information. Item 1 of the request will not be provided. It is the consensus of technical opinion that providing a copy of the electronic database used to tabulate primary and general election results is ill-advised and would provide, to a knowledgeable individual, an appropriate roadmap to hack a future election in Pima County. In consultation with the Secretary of State's Office and the Maricopa County Attorney's Office, it was determined to be inappropriate to release the database. Hence, it will not be provided to Mr. Risner.

In response to the denial and intervening events, Plaintiff enlarged its request from computer files for the 2006 elections to "include every file that ends with the extension "gbf" or "mdb" . . . this request is not limited to the dates originally requested and does include all those files stored on the computer." On March 30, 2007 Deputy County Attorney Karen Friar wrote to Plaintiff's counsel to inform him that

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 4

Date: December 18, 2007

Case No: C20072073

“After much deliberation, Pima County has determined that it cannot honor the public records request would indeed be detrimental to the interest of the government in providing for a secure and honest election.” Following the denial, Plaintiff filed this statutory special action pursuant to A.R.S. § 39-121.

Elections Computer System

5. The Pima County Division of Elections uses Diebold System Inc.’s Global Election Management System (“GEMS”) to process elections. GEMS has been certified by the Arizona Secretary of State for use in Arizona. The parties agree that the GEMS program is not subject to disclosure.

6. The GEMS program has several primary functions. First, it is used to print the ballots. This is a more complicated process than first appears because most general elections have races that do not apply to all county voters. Additionally, ballots are rotated from precinct to precinct. There can be as many as sixteen hundred ballot styles.

Second, GEMS writes the memory cards used to program optical ballot scanners and touch screen displays (hereinafter “voting machines”). These memory cards are integral parts of a ballot scanning process.

Third, GEMS tallies the votes from the voting machines. This process involves processing many different digital inputs, sometimes on a concurrent basis.

Finally, GEMS prints a variety of reports from the race results to management and audit functions.

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 5

Date: December 18, 2007

Case No: C20072073

7. GEMS is a stand-alone program designed to run on computers with a Microsoft Windows operating system. The current version used by Pima County is 1.18.24.0. The GEMS software is an executable file. The program is derived from human-readable source code that is then compiled into object (machine-readable) code. The source code is copyrighted and only available through a license agreement with the manufacturer. A copy of the source code is held in escrow with the Arizona Secretary of State.

8. GEMS creates a relational database. The database consists of tables of information (*e.g.*, race, candidate, precinct) and queries (pre-formed requests for particular information).

9. GEMS creates one database file for each election. The format is based on the format used by Microsoft Access, a general database program. Each database file ends with the letters "mdb," which stands for "Microsoft DataBase." The filename extension nomenclature follows a system used with other applications in the Microsoft Office Suite, such as Microsoft Word (.doc), Microsoft Excel (.xls), and Microsoft Powerpoint (.ppt). That is, the application creates a file with a specific three-letter extension to identify its relationship to that application.

10. A "gbf" file is a password-protected, compressed, and encrypted version of the mdb file. A gbf file can only be created and opened by the GEMS program. For the purpose of this case, the distinctions between a gbf and mbd file are irrelevant. The remainder of the Order refers only to the mdb file, although it applies equally to the gbf counterpart.

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 6

Date: December 18, 2007

Case No: C20072073

11. The GEMS-created mdb file can be opened using Microsoft Access. Data in the file can be manipulated. Password protection can be overwritten. The full functionality of the GEMS program, however, cannot be utilized if the mdb file is opened in Microsoft Access. GEMS is necessary to utilize all of the election-related functions.

12. Although the Microsoft-sponsored mdb format is widely used, it has size and input limitations. Specifically, file integrity becomes less robust (*i.e.*, prone to crashing) when the database becomes too large. The data may also become corrupted if it receives too many inputs, too quickly, at one time (concurrency problems). These limitations are well known. Microsoft has warned against using the mdb format for some critical applications, such as election management software.

13. The parties agree that “[t]here are significant security flaws with the architecture of the GEMS software.” Each of the expert witnesses endorsed that statement to one degree or another.

Is An MDB File A “Computer Program?”

14. A.R.S. § 16-445 requires Pima County to file with the Secretary of State “a copy of each computer program for each election.” The filing must be made at least ten days before the election. Any revisions to the computer program must be filed within 48 hours after the revision. A.R.S. § 16-445(B).

Electronic medium used to operate the vote tabulating devices must be kept under lock and seal. A.R.S. § 16-445(C). If there is a retally of the votes, the election officer must submit an affidavit vouching for the authenticity of the electronic medium and that there has been no alteration since the

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 7

Date: December 18, 2007

Case No: C20072073

election. *Id.* There is no requirement that the mdb file be sent to the Secretary of State after the election. *See generally* Arizona Secretary of State Election Procedures Manual, pgs. 79-80 (Aug. 2006).

Pima County argues that A.R.S. § 16-445(D) prohibits disclosure under the public records law. It provides that “[a]ll materials submitted to the secretary of state shall be used by the secretary of state or attorney general to preclude fraud or any unlawful act under the laws of this title and title 19 and shall not be disclosed or used for any other purpose.” The issue is whether a “computer program” ordered to be filed with the Secretary ten days before the election includes the mdb file created by GEMS during the election process, but which is not finalized until after the votes are counted.

15. “Computer program” is described as “all programs and documentation adequate to process the ballots at an equivalent counting center.” A.R.S. § 16-444(A)(4). “Database” is not defined in the election statutes or other Arizona law.

16. Federal copyright law defines “computer program” as “a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.” 17 USCA § 101. Even such a simple definition made within the context of a specialized area of law is subject to problems of context and nuance. *See* William F. Patry, *Copyright and Computer Programs: It's All In The Definition*, 14 *Cardoza Arts & Ent. L.J.*, 1, 39 (1996). Nonetheless, there is a fundamental distinction between a computer program and a database. *Compare* Copyright Office Circular 61 *Copyright Registration for Computer Programs* (a “computer program” is a set of statements or instructions to be

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 8

Date: December 18, 2007

Case No: C20072073

used directly or indirectly in a computer in order to bring about a certain result”) with Circular 65 *Copyright Registration for Automated Databases* (“database is a body of facts, data, or other information assembled into an organized format suitable for use in a computer and comprising one or more files”).¹

17. The expert witnesses also agreed that an mdb file is fundamentally different from the GEMS executable file. The latter is not readable by a human. It contains the majority of the instructions to operate the computer. The only disagreement is whether the addition of queries, which are in the form of “SQL” statements, transform the mdb file into a computer program.

18. The Arizona Secretary of State creates and distributes the Elections Procedures Manual that provides additional details to election officials regarding the conduct of elections and the filing of mandated materials. The Elections Procedures Manual does not provide explicit instruction on whether the mdb file may be disclosed. Gila County Election Director, Dixie Mundy, testified that the Secretary of State provides training materials and seminars. She does not recall any instruction from the Secretary of State prohibiting the disclosure of mdb files. Finally, the Secretary of State’s Election Director, Joseph Kanefield, testified pursuant to a Rule 30(b)(6) designation about the Secretary’s policies and procedures regarding election software. He did not indicate that the Secretary of State opines that A.R.S. § 16-445 prohibits disclosure. Similarly, the Arizona Attorney General, which represented the Secretary

¹ Copyright protection specifically extends to “computer programs” whereas databases may be copyrightable as a form of original compilation. *Id.* The point is not whether GEMS versus the mdb file is subject to copyright; rather, the importance lies in the recognized legal distinction between the software program that creates a database and the database itself.

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 9

Date: December 18, 2007

Case No: C20072073

of State in this case and conducted an investigation relating to the computer files, did not seek intervention in this case to oppose disclosure of the mdb files.

19. The final mdb files (which are the principal files requested by the Plaintiff), are not required to be sent to the Secretary of State. Unofficial results that are released to the public must be transmitted to the Secretary by telephone, fax, or “other electronic means.” A.R.S. § 16-622(B). The official canvas for all elections must be provided to the Secretary “on paper and also electronically in a ‘readable’ format prescribed by the secretary of state.” Elections Procedures Manual at 158 (2006); *see also* A.R.S. §§ 16-646(B) and (C). Nothing in the vote tallying statutes or the Elections Procedures Manual indicates that Pima County is required to provide to the Secretary the final mdb file.

20. The Court finds that the mdb file is not a computer program as defined under A.R.S. § 16-444(A)(4) for three reasons. First, the legal distinction between a computer program and database is well recognized in other contexts and applies equally here. *See e.g.*, Raymond T. Nimmer, 1 Information Law § 3:33 (2007); Amy Sullivan, *When The Creative Is The Enemy Of The True: Database Protection In The U.S. And Abroad*, 29 AIPLA Quarterly J. 317, 323 (2001). Second, computer experts recognize the distinction between a computer program and a database. Finally, the prohibition against disclosure, when read in the context of all elections statutes, does not include the final mdb files because they are not required to be provided to the Secretary in that form.

21. The Court concludes that A.R.S. § 16-445(D) does not prohibit disclosure of mdb files.

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 10

Date: December 18, 2007

Case No: C20072073

Balancing Plaintiff's Right To Public Records Versus Defendant's Interest In Conducting Secure Elections.

22. The parties agree the mdb files are public records.

23. The public records law creates a strong presumption in favor of disclosure. *Griffis v. Pinal County*, 215 Ariz. 1, 4, ¶¶ 12-13, 156 P.3d 418 (2007). If a public record falls within the scope of the statute, the Court can perform a balancing test to determine whether privacy, confidentiality, or the best interests of the state outweigh the policy in favor of disclosure. *Id.*; see also *Carlson v. Pima County*, 141 Ariz. 487, 490-491, 687 P.2d 1242 (1984).²

24. Pima County is concerned that each of the primary functions of the GEMS software could be compromised if the database is released to Plaintiff. The concerns are based on several assumptions, which the Democratic Party does not deny. First, release of the computer file to Plaintiff will likely result in wide disclosure. Second, although Plaintiff does not seek disclosure of the GEMS software, the program is available on the Internet; persons who have not obtained an official license to operate the program can download it. The Court finds that disclosure of the mdb files will not be limited to Plaintiff.

² The balancing test generally focuses on "the public's right to openness in government" rather than the specific interest of the petitioner in the requested records. *Carlson v. Pima County, supra*, 141 Ariz. at 491. Although Plaintiff stresses its particular standing as a political party with specific rights and responsibilities in the elections process, the Court applies the *Carlson* standard.

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 11

Date: December 18, 2007

Case No: C20072073

25. Pima County identifies four types of security compromises that could occur if the mdb files were released and there were lapses in physical security:

- a. Counterfeit ballots could be generated from GEMS.
- b. Counterfeit memory cards could be generated from GEMS.
- c. Electronic transfer information could be obtained from the mdb file to launch a “man-in-the-middle” attack during transmittal of election results.
- d. Counterfeit election results could be generated to confuse or call into question official election results.

26. Each of the concerns raised by Pima County represents a valid, significant security risk if physical security of the cast ballots, voting machines, memory cards, electronic input devices, and counting computer is not strictly maintained. For instance, the substitution of ballots or memory cards would require a lapse in existing security measures or the complicity of elections personnel to overcome lock-boxes and anti-tamper seals. Pima County acknowledges that its security measures would generally prevent insertion of counterfeit materials, but it wishes to maintain an additional layer of security in the event that those measures are not effective or are breached.

27. Interception of electronic transmissions and substitution of invalid voter results is an on-going concern. Specifically, the extant procedures involve modem transmission of voting machine results to the central counting computer. Interception of the electronic transmission would be made

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 12

Date: December 18, 2007

Case No: C20072073

easier if the transmission information contained within the mdb file was widely known. This is known as the “man-in-the-middle” ruse. There is a pending recommendation from Mr. Huckelberry to eliminate all modem transmission of voting machine results and to use a hardwire method within a secure-room environment. If Mr. Huckelberry’s recommendation is accepted, the interception and substitution of voting machine results by remote electronic means is virtually eliminated.

28. The risk of interference with the counting computer has been significantly reduced by recent measures to control and monitor persons with access to the computer, to eliminate remote connections, and to create a special room that allows physical monitoring of the security measures. As with the counterfeit materials, it would be very unlikely that a contaminated mdb file could be substituted for the valid, working mdb file.

29. Use of the mdb file from past elections to create false election results in future elections does not appear to be a significant risk for several reasons. First, the printout of election results produced by GEMS has no security artwork (unlike the “timing marks” on ballots) and could be easily duplicated with any word processor. This possibility exists independent of disclosure of the mdb file. Second, persons not designated as elections personnel could not credibly claim that the election results they proffer are more valid than the results prepared from the secure, elections computer. Moreover, even such an attempt would likely result in a criminal investigation regarding fraud. *See* A.R.S. §§ 16-1012 to 16-1021 (penal provisions for interference, counterfeiting, intimidation, and corruption of the

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 13

Date: December 18, 2007

Case No: C20072073

election process). Finally, Plaintiff concedes that the release of mdb files immediately after the polls close is neither practical or appropriate. Release of the mdb file days or even weeks after the election significantly reduces the concern that valid election results could be challenged with an altered mdb file.

30. Pima County also alleges that future mdb files would have to be “built from scratch” if past-election mdb files were released as public records. Bryan Crane, the master programmer for the Election Division since GEMS first came into use, explained how he builds the mdb file for each new election based upon prior files from previous elections. Use of prior mdb files is important because although the candidates and initiatives/referendums frequently change, the races and most precincts remain the same. Upon closer examination, however, his concern is a factual assumption for the more general concern about counterfeit ballots and memory cards.

Pima County’s expert witness, Professor Merrill King, testified that starting over with a new mdb file for each election should not result in a new architectural structure for the mdb file or the formatting of ballots and memory cards. In fact, he emphasized that the primary risk of starting from scratch with each election is the increased likelihood of clerical errors because creating a ballot involves manual input of voluminous numerical and formatting data. Using the analogy of building a house, Professor King explained that the mdb structure for races and precincts (*i.e.*, equivalent to walls, number of rooms, etc.), must remain the same to comply with state and federal law, and only the contents (*i.e.*, furniture) must change to reflect the new candidates and questions. Using a prior, valid structure

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 14

Date: December 18, 2007

Case No: C20072073

eliminates the likelihood of significant errors. The rationale for using prior mdb files as a template for future elections is valid and well-established.

Mr. Crane and Professor King suggested that by starting from scratch with each new election it would be possible to detect or prove counterfeit mdb files if public disclosure of the mdb file increased the risk that someone would do so to compromise an election. This potential problem ultimately returns to the concerns noted above regarding counterfeit ballots, memory cards, and substituted mdb files.

Plaintiff correctly points out that the risk of counterfeit items or reverse-engineering is primarily a concern if a perpetrator can physically substitute ballots, memory cards, or electronic transmissions with contaminated copies. These types of counterfeits are fundamentally different from counterfeiting in other areas where there is no attempt to eliminate or invalidate the real item (*e.g.*, counterfeit money, pirated DVD's, and unlicensed software have independent value separate from original items produced by the U.S. Treasury, movie companies, and software manufacturers).

31. In addition to the specific, identified concerns listed by Pima County, the witnesses also identified the threat of new attacks on electronic election systems that no one has anticipated. For instance, Plaintiff's expert, Mickey Duniho, is a retired master programmer with many decades of experience at the National Security Agency. He confirmed that the risk of novel attacks on computer systems is an ever-present threat. Defendant's witnesses opined that disclosure of a mdb file was the

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 15

Date: December 18, 2007

Case No: C20072073

equivalent of making public the architectural drawings of a building. Whatever the merits of the security system that might be in place, unlimited access to the drawings increases the likelihood that a potential intruder could find and exploit a security flaw not known by those responsible for security.

Although it is difficult to quantify an unknown —but plausible— threat, this consideration must be weighed against Plaintiff's interest in the mdb files.

32. Plaintiff does not identify specific reasons why it needs possession of the mdb files. (It previously had asserted the need for audit logs contained within the mdb file that would show alterations and printing of vote tallies prior to the polls closing, but those audit logs have been separately disclosed.) Plaintiff premises its request on two general arguments. The first is based on the presumption in favor of disclosure, which also requires that an official who wishes to withhold public documents must prove specifically how the public interest outweighs this presumption. Citing *Phoenix Newspapers, Inc. v. Keegan*, 201 Ariz. 344, 349 (App. 2001). Second, Plaintiff argues that it cannot perform its statutorily-mandated role of elections monitor unless it can inspect the mdb files.

These general arguments arose from its internal research and informational meetings with Pima County election officials. Plaintiff identified a variety of administrative personnel and physical security issues that could compromise an election or call into question the election results. (Plaintiff is careful to note that it is not alleging or even suggesting that prior elections were compromised or fraudulent.) It now wishes to determine if there are weak spots in the elections management software.

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 16

Date: December 18, 2007

Case No: C20072073

33. The risk of a novel attack based on the public disclosure of an mdb file can be assessed in a limited context. Various witnesses testified about the public disclosure of an mdb file from an Alaska election. The witnesses did not know the context of the disclosure and this Court's own legal research does not disclose it; however, newspaper reports from the Anchorage Daily News describe a suit to release the raw election results. *See e.g.*, www.adn.com/news/politics/elections/story/8218154p-8115104c.html (last visited December 13, 2007). Expert and lay witnesses for both parties testified that they had obtained the mdb file on the Internet, and examined it using various methods.

Professor King also knew of the Alaska mdb file, but only recently. The context and implications of how he learned about this development are revealing. Professor King is the Executive Director of the Center For Election Systems at Kennesaw State University in Georgia. He consults nation-wide with state and federal elections officials about election software. He has a particular interest in security issues. He also oversees a staff of persons at his Center that regularly search for emerging issues in elections management software.

Professor King was not aware of the public disclosure of the Alaska mdb file until his recent involvement with this case. He asked his staff to research the security implications arising from the disclosure of the file. Apparently, despite public disclosure of the Alaska mdb file more than a year ago, it had not registered as a security issue with him or his staff. He testified that there is no indication

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 17

Date: December 18, 2007

Case No: C20072073

that the release of the mdb file compromised a subsequent election in Alaska or in any other place in the country.

Professor King opined, however, that the release of a single mdb file may not be sufficient to allow computer hackers to obtain enough information about the architecture of the mdb database to compromise elections in other jurisdictions. He explained that multiple mdb files from various jurisdictions might be necessary to provide confirming data that would enable a computer hacker to map the structure of the GEMS-created mdb file. Essentially, unless multiple copies of mdb files are released it will not be possible to know the actual risk from computer hackers.

Plaintiff's expert witnesses opined that there is nothing in multiple copies of the mdb files that would be of such incremental value that there would be an increased risk if Pima County disclosed all its mdb files. Plaintiff's experts are extremely knowledgeable in computer security and computer programming, but none of them have the hands-on experience with the GEMS program possessed by Defendant's witnesses.

33. The Court finds that the risk of releasing multiple, but not identical, versions of a database file with a similar structure poses a known risk that hackers could use the files to contaminate valid mdb files. The risk arising from the release of mdb files has not been quantified or assessed with any precision. This known-but-unquantified risk, coupled with the possibility of failure in the physical security of elections equipment, cautions against unlimited release of mdb files. The Court concludes

Lynne Booth
Judicial Administrative Assistant

RULING

Page: 18

Date: December 18, 2007

Case No: C20072073

that releasing a large number of mdb files at this time does not protect the interest of the State in valid elections.

The absence of negative consequences from the release of the Alaska mdb file indicates that a limited release of mdb files may not harm the State's interest, or that the reduced risk from disclosure is outweighed by the benefit to the public.

Plaintiff has demonstrated that its participation in monitoring computer-based elections has resulted in increased elections security. Mr. Huckelberry has praised and adopted a number of the physical and personnel recommendations made by the Democratic Party. The continuing interest of the Democratic Party in this area has spurred election officials to conduct internal reviews that have resulted in improvements that are independent from the recommendations made by Plaintiff.

The Court concludes that the public interest will benefit from the continued involvement of Plaintiff in reviewing election management software. Without access to at least some of the mdb files, Plaintiff will be constrained in its ability to fulfill its statutorily-mandated role. The positive benefit to the public by Plaintiff's ability to analyze mdb files for two elections in 2006 outweighs the much smaller risk posed by the disclosure to the public.

Lynne Booth

Judicial Administrative Assistant

RULING

Page: 19

Date: December 18, 2007

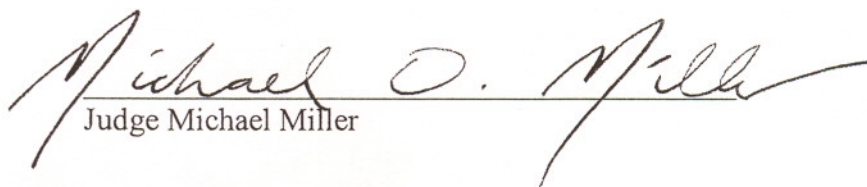
Case No: C20072073

ORDER

IT IS ORDERED that the public records request identified in Plaintiff's December 6, 2006 letter, Item no. 1, is **granted**. Specifically, Pima County shall disclose pursuant to A.R.S. § 39-121.02 the final mdb and gbf files for the 2006 General and Primary Elections.

IT IS FURTHER ORDERED **denying** Plaintiff's March 6, 2007 letter request for "every file that ends with the extension gbf or mdb." Such denial is without prejudice to Plaintiff to re-urge the record request after it has had the opportunity to study the mdb files for the 2006 elections and to address the current (and any future) security concerns raised by Pima County arising from the disclosure of many mdb and gbf files.

Dated this 18th day of December 2007



Judge Michael Miller

cc: Hon. Michael Miller
William J. Risner, Esq./Kenneth K. Graham, Esq. – Risner & Graham
County Attorney – Civil Division – Christopher Straub, Esq./Thomas A. Denker, Esq.

Lynne Booth
Judicial Administrative Assistant