

# When the Right to Know and the Right to Privacy Collide

The increased ease with which public records and the sensitive information they often contain can be accessed is a concern for many. However, protecting that information through redacting or limiting access causes equal concern for those whose duty or desire for transparency demands these records remain available and unaltered.

**Judy Vasek Sitton, CRM**

In March 2006, Ohio's State Supreme Court handed down an opinion, considered by some a landmark ruling, that Ohio's open records laws trump the Health Insurance Portability and Accountability Act (HIPAA). Texas Attorney General Greg Abbott had reached the same conclusion about Texas laws two years earlier in an extensively researched and detailed 400-page report.

Corporate records managers should not be comforted by believing that only government records officers or those employed in healthcare need to be concerned about open records – that is not the case. These and similar decisions that have been handed down in both large and small U.S. cities have great bearing on the protection of privacy afforded by data-breach laws and good corporate citizenship. They also question the use of technology, challenge the idea of legal domain, and set policy

standards that have an impact on established ways of doing business.

## Heart of the Controversy

Sensitive, confidential information found in court and probate records, deeds, mortgages, death certificates, and other civic records is posted online or can otherwise be easily obtained electronically by anyone who cares to look

for it. The information is available because the records containing it are, by law, public records filed according to provisions of state statutes and maintained at taxpayer expense. In many instances these records contain health information, Social Security and Medicare numbers, birth dates, bank account information, prescription numbers, and information that could be used to steal individuals' identity. For corporations, this could also mean that private information about their employees, customers, officers, operating practices, or perhaps even the corporate entity itself, is freely available.

Although government entities may not have created the documents in question, local government employees are required to make them accessible under open-records, or sunshine, laws. This same information has been historically available, open to all, but it was not as easy to access as it is today. This degree of accessibility has privacy advocates concerned. Data that forms the basis for a

### At the Core

This article

- ▶ Defines the conflict between making records public and protecting the privacy of those whose sensitive information they contain
- ▶ Describes the role of information technology in both exacerbating and abating the controversy
- ▶ Provides possible solutions for serving the public interest and protecting individual privacy

democratic legal system is being mined for purposes not originally intended and in direct opposition to the spirit of laws and regulations, such as HIPAA, the Graham-Leach-Bliley Act, the Fair and Accurate Credit Transactions Act of 2003, and others drafted specifically to protect data distribution and use.

To add one more dimension to this already complex controversy, consider what can happen when these documents, once posted, are available to entities outside the jurisdiction of U.S. laws. Yet to be determined is how much U.S. citizens are willing to limit their rights and freedoms to prevent it.

### Right-to-Know vs. Privacy

On one side of the controversy stand right-to-know advocates. These dedicated individuals, who have history and tradition on their minds and on their side, are undeterred in their efforts to keep records open to the public. Their position is driven by a commitment to keep public business and the judicial process transparent. As Washington State Supreme Court Justice Tom Chambers noted in The Reporters' Committee for Freedom of the Press, "Justice must be conducted openly to foster the public's understanding and trust in our judicial system and to give judges the check of public scrutiny."

On the other side are right-to-privacy proponents, equally dedicated and working tirelessly to protect sensitive information from disclosure. They would rein in unscrupulous data miners and predators who seek information for the purpose of hurting or defrauding others. This group makes its stand based on nothing less than the U.S. Constitution and privacy laws that evolved from it.

By remaining unwavering in their goals and ideals, these groups constitute the concept of checks and balances for which the U.S. democratic system is known. Evolving technology and changing expectations about what is now considered private has set these advocates on a collision course.

This digital double-edged sword may yield awards for innovation while, at the same time, it garners jeers for recklessness – occasionally for the same entity.

Some question whether these changing times require a new look at these issues. "What we are looking at is whether laws and practices that were developed for nineteenth century recordkeeping to protect rights and property interests of citizens are expressions of unchanging values that must be preserved or whether they must change to protect the rights and property interests of twenty-first century citizens confronted with new threats from criminals," said Paul Scott, CRM, CA, records manager for Harris County, Texas. "And, of course, we are facing an evolving standard of personal rights including the right to privacy."

### Conflict in the News

This controversy has received a lot of media attention. People accustomed to performing jobs in anonymity in basements and back rooms are suddenly finding themselves in the spotlight and on the news for doing what they have done without fanfare or controversy for many years – except now they are doing it electronically. As reported by one newspaper editor following the controversy in her particular geographic region, "The Internet has changed the face of public information – and quite often personal information – making it all accessible to anyone with a computer worldwide."

This digital double-edged sword may yield awards for innovation while, at the same time, it garners jeers for recklessness – occasionally for the same entity.

Dianne Wilson, county clerk in Fort Bend County, Texas, found herself exactly in this situation. According to a host of articles in local newspapers and on the Internet, Wilson and her office have been in the heat of a HIPAA audit and surrounded by controversy for what she released electronically or posted on the county website. She has had to justify the sale of millions of historical county records to a data broker to save county staffing and operating costs. At the same time, she has had to explain how she unwittingly made available personal information, not only of former House Majority Leader Tom Delay and other Fort Bend County residents, but also about herself and her own family. An April 17, 2006, *Computerworld* article speculated that she is not alone. Recordkeeping officials in Broward County, Florida, Maricopa County, Arizona, and probably a great number of the 3,600 county governments around the country post sensitive data on the web.

Ironically, Wilson also has received accolades for the very actions that are now drawing fire. She was honored as Public Elected Official of the Year in March 2006 and has received awards for innovation in community service, innovation in information technology, and improvement and enhancements in delivery of governmental services.

News stories dealing with this controversy have brought to light abuses – and opportunities for abuse – that can occur

The process of redacting the information from records published on the Internet has been slower than expected due to software limitations and the volume of documents.

when information derived from public records is used for stalking or for other criminal intent. The stories report banks using information to deny home loans to minorities, share horrors of a widow trying to protect intimate details surrounding the tragic death of her celebrity spouse, and warn of the physical danger associated with disclosing where someone lives.

On the other hand, the articles also question the validity of claims that posting personal information poses great risks to privacy and security. In the same *Computerworld* article cited above, Darity Wesley, chief executive officer of Privacy Solutions Inc., said, "There is also little evidence to show that the public availability of personal information on government sites has contributed to an increase in identity theft. For most identity thieves, the chore of sifting through millions of public records for useful data simply isn't worth the effort."

The reports collectively frame the questions: Who is responsible for securing personal data collected unnecessarily? Who should pay to protect people or entities from illegal or improper use of data that should never have been made available?

### Technology's Role in the Conflict

In this controversy, records managers will find that there are multiple technology-related issues at play. Both the corporate and government sectors rely heavily on technology to accomplish daily tasks, save time and money, and protect sensitive

information. As in the corporate world, nearly all government documents or records are created electronically. In addition, many of the records produced in the pre-computer age have now been scanned.

Although the controversy is not entirely related to the use of IT, Internet postings are crucial to the increased availability of the data involved. A *South Florida Sun-Sentinel* article pointed out the significant change from the way transactions have been handled historically.

"Previously, records were somewhat protected by the concept of 'practical obscurity,'" said Sharon Bock, Palm Beach (Florida) county clerk and comptroller. That is, people could trek to the bowels of a county courthouse to dig out files, but very few bothered to do so. "Now it's all available to be perused 24/7, and you can be in Slovenia to do it," she said in the *South Florida Sun-Sentinel* article.

The online storage of large volumes of records and the ease with which they can be searched are also significant. In the Fort Bend County, Texas, controversy, a December 2005 local newspaper story estimated that Wilson posted 15 to 20 million records. Her decision to post them was justified, she said, because they are "public records, and the public has the right to access those records [according to] state statute." The article continued, "Wilson said 'it made sense' to make the public records available on the Internet because 200 to 300 people a day visited her office in search of such documents."

### Possible Solutions – Limited Access, Redacting

Some privacy advocates suggest setting a limit on Internet use, either by changing the way the information can be searched or by eliminating access completely. *Wired News* discussed a Minnesota committee recommendation that would not allow web searches of court records by defendants' names and a Florida special commission that wished to limit Internet access. The essence of the controversy was summed up by South Dakota attorney Sue Larson, who hosts a website called "Public Access to Court Records." "Saying certain public records should remain public – but not made widely available – goes against the fundamental principles of open records laws," Larson said.

Harris County's Scott adds, "We traditionally build courthouses with entrances on all four sides so that citizens may approach justice (and the records that protect their rights) from any direction. But this has changed in the last two decades to restrict access through a single entry point so that visitors must be scrutinized. Frankly, I question the wisdom of giving up our liberties in the name of security."

Redaction software, which can be used to mask or remove sensitive data – or as right-to-know advocates may perceive it, to alter or censor records – may provide another solution and figures significantly in pending legislation. Some hope that software will retroactively redact items that have already been posted. As yet, no software has been proven to be completely effective.

According to an article by David Bloys in *News for County Officials* newsletter, his organization was "unable to identify any company offering software that claims 100 percent accuracy or any ability to automatically redact handwritten numbers. Many, if not most, Social Security numbers appear in the online records in handwritten form." The article goes on to say that "when Gov. Jeb Bush was notified that his hand-written Social Security number appeared on the Dade County website, he signed a law allowing Florida residents to

---

request that their numbers be redacted from official sites.” Though Bush’s own Social Security number was removed very quickly, copies of the non-redacted documents released prior to Bush’s action can still be found posted on other sites on the Internet.

The process of redacting the information from records published on the Internet has been slower than expected due to software limitations and the volume of documents. Fred Baggett, general counsel for the [Florida] state clerk’s association, estimates seven billion official records and 10 billion court records are kept statewide.

Is removing those numbers, whether by redaction software or other means, tampering with government documents? It may be. According to *Computerworld*, even in Florida, “for now, recorders have ‘no statutory authority to automatically’ remove such information from documents.” In Fort Bend County, Texas, Wilson has requested a ruling from the attorney general about what is permissible. She discussed her dilemma in a 2005 *Herald Coaster* article saying that in accordance with a law that went into effect September 1, 2005, she can remove Social Security numbers from public records for living persons, but she did not yet know if she could remove them for those deceased. Wilson was also unsure if the ruling applies to property and court records. She also says that a September 1, 2003, law gives the public the right to take out Social Security numbers and driver’s license numbers before a document is recorded, but the legislature has said that once it is recorded, all information remains on the document.

Harris County’s Scott suggested that, “Redacting public records is a relatively recent practice – in Texas dating only back to the 1980s. Indeed, for hundreds of years those concerned with record-keeping labored to create laws and practices to prevent people from altering records and to detect if something was removed.

“Intricate patterns common on the

edges of public records books were not merely decorative – it was done so that removal of even a single page, similar to a color-coded file being out of order, would be noticeable,” Scott said. “Skeptics may well question the practical value of redacting documents filed decades ago, especially when even more current and sensitive information may

be found on the Internet or in corporate or government laptops that go missing with depressing regularity.”

New legislation alone is not likely to solve this controversy. In fact, according to Charles Bacarisse, district clerk of Harris County, Texas, district clerks are hoping for direction from the courts rather than from the legislature because

the courts' rulemaking process is more straightforward. The decisions mentioned above, however, show that the legal domain for this issue is not simple. If public records contain information expressly protected under a federal law, can that mean that they are not truly public records? Making records available contrary to privacy laws could subject recordkeepers to severe fines and penalties, but not making the records available is considered a breach of duty. Yet, to be frozen without action while the debate rages is simply not an option.

### Impact on Corporate Entities

Corporate records managers are also affected by this situation. The same technology, with its assets, liabilities, and limitations, is available in the corporate arena. Responsible decisions must be made regarding its use in that environment. Information once posted on the Internet or otherwise accessible electronically, can not easily be retracted, revised, removed, or recalled, and there is little or no control over who has access to it. Increasingly, diligence must be taken before release to ensure accuracy and protect rights. Protected information, if disclosed, can cause real, irreversible harm and its release can garner severe penalties.

Records managers can play an important role in keeping information private from its creation through final disposition. To minimize risks for internal staff members, collect their personal information only when warranted. For example, consider whether including Social Security numbers on time sheets, expense reports, or other company documents is absolutely necessary. If so, track those records through their processing to identify potential security gaps.

Even though legislation, legal opinions, and legal jurisdictions often produce conflicting opinions and applications, the responsibility to comply is not diminished. The Sarbanes-Oxley Act has increasingly become a *de facto* standard for publicly held businesses of all

sizes. Privacy and access legislation to regulate corporate entities will, in many instances, be emulated in government agencies as well. Being aware of the

issues and involving yourself and others in monitoring current and pending legislation is imperative to ensuring compliance. ■

**Judy Vasek Sitton, CRM**, is a senior staff consultant for PacoTech, Inc., an information management consulting firm based in Houston, Texas. She has more than 25 years of experience and involvement in records management. She may be contacted at judysitton@pacotech.com.

### References

- Abbott, Greg. "Preemption Analysis of Texas Laws Relating to the Privacy of Health Information & the Health Insurance Portability & Accountability Act & Privacy Rules (HIPAA)." *Report of the Office of the Attorney General of Texas*, 1 November 2004. [www.oag.state.tx.us/notice/hipaa.pdf](http://www.oag.state.tx.us/notice/hipaa.pdf) (accessed 3 August 2006).
- Bacarisse, Charles. Interview by author, Houston, Texas, 6 June 2006.
- Bloys, David. "The Truth About Redaction Software." *News for County Officials*, 25 February 2006. [www.davickservices.com/REDACTION.htm](http://www.davickservices.com/REDACTION.htm) (accessed 3 August 2006).
- Buck, Amanda. "New Rule to Make Sealing Court Cases More Difficult." *The Reporters Committee for Freedom of the Press*, 16 March 2006. <http://rcfp.org/news/2006/0315-sct-newrul.html> (accessed 3 August 2006).
- "City Citations for Lead Paint Violations Must Be Disclosed Under Ohio Public Records Law." Select Opinion Summaries of the Supreme Court of Ohio, 17 March 2006. [www.sconet.state.oh.us/Communications\\_Office/summaries/2006/0317/050068.asp](http://www.sconet.state.oh.us/Communications_Office/summaries/2006/0317/050068.asp).
- Ferris, Nancy. "HIPAA Doesn't Protect All Health Information, Ohio Court Rules." *Government Health IT*, 28 March 2006. [www.govhealthit.com/article92752-03-28-06-Web](http://www.govhealthit.com/article92752-03-28-06-Web) (accessed 3 August 2006).
- Katz, Ian. "Cities, Counties Walk a Fine Line to Keep Public Records Open and Personal Information Secret." *South Florida Sun Sentinel on TMCnet*, 30 April 2006. [www.tmcnet.com/usubmit/2006/04/30/1625164.htm](http://www.tmcnet.com/usubmit/2006/04/30/1625164.htm) (accessed 3 August 2006).
- Ogles, Jacob. "Court Documents Not Fit for Web?" *Wired News*, 23 November 2004. [www.wired.com/news/politics/privacy/0,65703-0.html](http://www.wired.com/news/politics/privacy/0,65703-0.html) (accessed 3 August 2006).
- Pollock, B. J. "County Clerk Dianne Wilson Sold Millions of Fort Bend's Records." *Herald Coaster*, 12 December 2005. [www.herald-coaster.com/articles/2005/12/12/news/top\\_story/topstory.txt](http://www.herald-coaster.com/articles/2005/12/12/news/top_story/topstory.txt) (accessed 3 August 2006).
- "Re-elect Dianne Wilson" campaign website. [www.diannewilsoncountyclerk.com](http://www.diannewilsoncountyclerk.com) (accessed 3 August 2006).
- Riddick, Rebecca. "Court Clerks Culling Personal Information Closer to Immunity." *Daily Business Review* 13 April 2006.
- Scott, Paul. Interviews by author, Houston, Texas, April – June 2006.
- Vijayan, Jaikumar. "Counties Post Personal Data in Documents." *Computerworld*, 17 April 2006. [www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110585&pageNumber=1](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110585&pageNumber=1) (accessed 3 August 2006).