DAS

The Records Custodians Dilemma
Public Records vs. Personal Privacy

Public records custodians, both elected and appointed, must be very sensitive to the public's expectation that government will protect their personal data. Conversely, open records are considered a foundational element in government accountability.

Effective government oversight and many businesses (i.e. the land title business; underwriting car insurance; hiring qualified teachers, day care, and healthcare workers) could not function properly without access to public records. Some government offices are attempting to fill the demand for easy access to public records by posting their information on the Internet.

The dilemma for records custodians is balancing the competing interests of individual privacy with the public's need for disclosure. The public's "right to know" wasn't nearly as pressing an issue 10 years ago as it is now. The digital age has changed our relationship with these records.

In the past, public records existed in what has been called "practical obscurity." Even though records were open to the public, you had to physically go to a government building and you had to understand how they were indexed in order to find them.

The internet-based government sites have created "virtual" government offices, designed to facilitate citizens conducting business with government when it is convenient for them. This often requires large databases and record image libraries being posted on the government's web site. These sites are usually available at little to no charge and vast amounts of information, some of it "personally identifiable", are available 24/7 from the comfort of your home. Now increase the complexity of this issue by adding people solely interested in Identity Theft. By combining data from various public sources, a more complete record emerges for someone interested in assembling such information. Simply protecting data in one domain does not protect the overall scope of information relatively easily available. Government must act in concert and in a uniform manner to increase the security of electronically accessible information.

Examples of Public Records Containing Personal Information Available Remotely Via Electronic Access[2]:

- Property Tax Assessor or County Recorder Files. Typical records contain name of owner, description of property, and the assessed value for taxation purposes. Some systems even provide blueprints of the property.
- Motor vehicle records - registration, licensing, and driver history information
- Registered voter files
- Professional and business licenses.
- Court files:
    - Case indexes
    - Tax liens and judgments

- Bankruptcy files
- Criminal arrest and conviction records, and warrants
- Civil court recordings.

These web sites may contain land records, military discharge notices, tax liens, court filings, vital records (i.e. birth, death, and marriage records) and property tax records just to name a few.

But public records also contain a great deal of information about individuals, often very sensitive information. The following examples refer to court proceedings.

- Court records often contain Social Security numbers (SSNs) and financial account numbers. These are commonly available in divorce decrees, child custody cases, and bankruptcy filings. But when account numbers, personal identifiers, and dates of birth are accessible on the Internet, they could be used to commit financial fraud. The crime of identity theft is at epidemic proportions today, fueled in part by easy access to SSNs.

- Family law files typically contain information about children as well as allegations - whether accurate or not -- of wrongdoing and negligence by warring spouses.

- When aggrieved insurance holders sue the insurance company over medical payment claims, the details of their medical conditions are likely to become part of the court record and thereby public. It is a common tactic of companies to threaten to bring highly sensitive medical information, as well as other personal matters, into the case in order to discourage the plaintiff from proceeding.

- For example, in a prominent case of alleged identity theft negligence, the defendant, a credit bureau, obtained the plaintiff's gynecological records in order to attempt to show that she was mentally unbalanced and that her claims had no merit.

- In a dispute with a neighbor, or a business dispute, many allegations can be made that might not be true.

- In employment-related matters such as sexual harassment cases, it is common for the defendant to divulge damaging allegations about the plaintiff, such as lifestyle and sexual history.

- In criminal cases, the statements of victims and witnesses become part of the public file. These often contain highly sensitive personal information. Witnesses' personal safety can be at risk in some cases if their identities are revealed.

It is important to note that in the majority of situations, providing personal information to government agencies and courts is *mandatory*. Individuals have no choice in the matter.

Identity Theft Preventative Measures

Recommendations for Government Records Custodians:

- **Adopt a privacy policy that includes responsible information-handling practices**. The State of Iowa's IOWAccess web portal was one of the first in the nation to have an information privacy policy prominently features on its' web pages. See Appendix A for

the primary state government web site privacy statement. Unfortunately, there is not an ability to force all agencies to abide by such standards

- **Appoint a knowledgeable individual responsible for the privacy policy** -- someone who can be contacted by employees and constituents with questions and concerns. State agencies are already responsible for appointing Agency Records Officer(s) – Iowa Code Section 305.10(b) and Public Records Contact Person(s) - Iowa Code Section 22.1(2).
- **Store sensitive personal data in secure computer systems**. As a best practice, encrypt data and ensure wireless networks are protected with the proper security settings (such as compliance with State of Iowa Enterprise Information Technology Standard S-012-002).
- **Store physical documents in secure spaces such as locked or accessed controlled cabinets.** Data should only be available to qualified persons.
- **Dispose of documents properly**, including shredding paper with a cross-cut shredder and securely deleting electronic files.
- **Build appropriate document destruction capabilities into the office infrastructure**. Place shredders around the office, near printers and fax machines, and near waste baskets. Use cross-cut (confetti) shredders rather than strip-shredders. Make sure dumpsters are locked or are inaccessible to the public.
- **Conduct regular staff training**.
- **Conduct privacy walk-throughs and make spot checks on proper information handling.**
- **Limit data collection to the minimum information needed**. For example, is SSN really required? Is complete date of birth needed, or would year and month be sufficient? All data collected must be appropriately protected. Collecting the minimum necessary data is a good practice and can reduce costs.
- **Limit data displays and disclosure of SSN and other sensitive information**. Do not print full SSNs on paychecks, parking permits, employee badges, time sheets, posted employee rosters, or on constituent reports. Do not print SSNs on mailed documents or require that they be transmitted via the Internet unless allowed by law.
- **Restrict data access to staff with legitimate need to know**. Implement electronic audit trail procedures to monitor who is accessing what. Enforce strict penalties for illegitimate browsing and access.
- **Safeguard mobile devices that contain sensitive personal data**, such as laptops and portable data storage devices (compliance with State of Iowa Enterprise information technology standards S-012-004 and S-012-005.)
- **Notify constituents and/or employees of computer security breaches** involving sensitive personal information in compliance with Iowa Code Chapter 715C.
- **Develop a response plan to be used if sensitive employee or constituent data is lost**, **stolen, or inappropriately acquired electronically**. The plan should include instructions to prevent identity theft if SSNs and/or personally identifiable is obtained illegitimately.

[2]Adapted from Privacy Rights Clearinghouse "*Prevent Identity Theft*

The goal is to strike a balance between keeping SSNs (or other sensitive identifiers that in combination increase risks) out of the hands of identity thieves while giving businesses and government sufficient means to match information to the correct person. Government must eliminate the unnecessary use and disclosure of SSNs as an identifier wherever possible and improve methods of authenticating constituents so, even if the SSN falls into the hands of an identity thief, it is less valuable.

Shifting to new identifiers simply shifts the risk. We need to fundamentally put a citizen in control of their information and how it is to be released. Citizens, except in the case of legitimate public good, should be able to control how information about them is available and used. Thus far, commercial interests have prevailed which in some ways has lead to the dilemna we find ourselves in.

Identity Theft Deterrence

The Federal Trade Commission (FTC) in November 2007 issued a "Red Flags Rule" that requires financial institutions and creditors holding consumer or other "covered accounts" to develop and implement an identity theft prevention program. The compliance date for the "Red Flags Rule" was November 1, 2008. The rule is actually three different but related rules:

1. Debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card.

2. Users of consumer reports must develop reasonable policies and procedures to respond to any notice of an address discrepancy they receive from a consumer reporting agency.

3. Financial institutions and creditors holding consumer or other "covered accounts" must develop and implement a written identity theft prevention program that covers both new and existing accounts. "Creditors" in this instance may include hospitals, utility companies, and other entities with consumer or other "covered accounts".

Additional information is contained in Appendix B.

Submitted by:
John Gillispie
Chief Information Officer
Information Technology Enterprise
Department of Administrative Services
Hoover State Office Building, Level B
Des Moines, IA 50319
John.gillispie@iowa.gov
(515) 281-3462

Appendix A. IOWAccess Disclaimer: Terms, Privacy & Warranty Information

Disclaimer

Terms and Conditions

The State of Iowa and its agencies, officials and employees make no warranty, representation or guaranty as to the content, accuracy, timeliness or completeness of the information provided herein. The State of Iowa, and the Department of Administrative Services, Information Technology Enterprise expressly disclaim any and all liability for any loss or injury caused, in whole or in part, by its actions, omissions, or negligence in procuring, compiling or providing the information contained in this site, including without limitation, liability with respect to any use of this site, or the information contained herein. Reliance on the information contained on this site, is solely at your own risk. The information may change or be altered at any time.

Privacy Statement and Policy

Information Collected By Use of This Site

Personally identifiable information which may be collected by use of this site includes IP numbers, date/time, stamps, methods, path, status code and size of request. The information that is available from governmental web sites is subject to these principles and policies:

Access to personally identifiable information in public records at state and local levels of government in Iowa is controlled primarily by Chapter 22 of the Code of Iowa. Information generally available under Chapter 22 - and not made confidential elsewhere in the Code of Iowa - may be posted for electronic access.

Persons concerned with regard to information about them should contact the custodian of the record, which typically is the state agency or other governmental entity that collects and maintains the information.

The information collected should only be that necessary to provide the information or services sought by a requester, just as a person might provide such information when visiting a governmental office in person.

The information collected is subject to the same controls and uses as that collected by governmental offices visited in person, again subject to the access and confidentiality provisions of Chapter 22, or to other applicable sections of the Code of Iowa. You do not have to provide personal information to visit the web sites or download information. The IP (Internet Protocol) numbers of computers used to visit these sites are noted as part of our statistical analysis on use of our web sites and how to better design services and facilitate access to them. No marketing databases are created nor are any commercial uses made of any such data. Government agencies may request personally identifiable information from you in order to provide requested services, but such information is handled as it would be on an in-person visit to a government office.

Various other web sites may be linked through this site. Private sector sites are not subject to Chapter 22. Visitors to those sites may wish to check their privacy statements and be cautious

about providing personally identifiable information.

Links to Other Sites

This site has links to other web sites as a convenience to our customers. These links may be operated by other government agencies, nonprofit organizations, and private businesses. When you use one of these links you are no longer on this site and this Privacy Statement and Policy will not apply. When you link to another web site, you are subject to the privacy policy of the new site.

When you follow a link to one of these sites neither the State of Iowa, nor any agency, officer, or employee of the State warrants the accuracy, reliability, or timeliness of any information published by the external sites, nor endorses any content, viewpoints, products, or services linked from these systems, and cannot be held liable for any losses caused by use of or reliance on the accuracy, reliability or timeliness of the information. Any person or entity that relies on any information obtained from these systems does so at his or her own risk.

Warranties

The information contained on this web site is provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. The State of Iowa assumes no responsibility for errors or omissions in this publication or other documents which are referenced by or linked to this publication. References to corporations, their services and products, are provided "as is" without warranty of any kind, either expressed or implied. In no event shall the State of Iowa be liable for any special, incidental, indirect or consequential damages of any kind, or any damages whatsoever, including, without limitation, those resulting from loss of use, data or profits, whether or not advised of the possibility of damage, and on any theory of liability, arising out of or in connection with the use or performance of this information. This publication could include technical or other inaccuracies or typographical errors. Changes are periodically added to the information herein; these changes will be incorporated in new editions of this publication.the State of Iowa may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

Appendix B. Appendix B. Federal Trade Commission (FTC) 'Red Flag' Requirements for Financial Institutions and Creditors[3] (November 1, 2008 Implementation Date)

New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft

Identity thieves use people's personally identifying information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. Financial institutions and creditors soon will be required to implement a program to detect, prevent, and mitigate instances of identity theft.

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must be in place by November 1, 2008, and must provide for the identification, detection, and response to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

Who must comply with the Red Flags Rules?

The Red Flags Rules apply to "financial institutions" and "creditors" with "covered accounts." Under the Rules, a financial institution is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, *or any other entity that holds a "transaction account" belonging to a consumer.* Most of these institutions are regulated by the Federal bank regulatory agencies and the NCUA. Financial institutions under the FTC's jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts.

A transaction account is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

A creditor is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors. Most creditors, except for those regulated by the Federal bank regulatory agencies and the NCUA, come under the jurisdiction of the FTC.

A covered account is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.

Complying with the Red Flags Rules

Under the Red Flags Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs – or "red flags" – of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

How flexible are the Red Flags Rules?

The Red Flags Rules provide all financial institutions and creditors the opportunity to design and implement a program that is appropriate to their size and complexity, as well as the nature of their operations. Guidelines issued by the FTC, the federal banking agencies, and the NCUA (ftc.gov/opa/2007/10/redflag.shtm) should be helpful in assisting covered entities in designing their programs. A supplement to the Guidelines identifies 26 possible red flags. These red flags are not a checklist, but rather, are examples that financial institutions and creditors may want to use as a starting point.

They fall into five categories:

- alerts, notifications, or warnings from a consumer reporting agency;
- suspicious documents;
- suspicious personally identifying information, such as a suspicious address;
- unusual use of – or suspicious activity relating to – a covered account; and notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts. More detailed compliance guidance on the Red Flags Rules will be forthcoming. For questions about compliance with the Rules, you may contact RedFlags@ftc.gov.

References

[1]Privacy Rights Clearinghouse. 2006. *Public Records on the Internet: The Privacy Dilemma.* Retrieved on November 21, 2008 from http://www.privacyrights.org/ar/onlinepubrecs.htm

[2]Privacy Rights Clearinghouse. 2006. *Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace.* Retrieved on November 21, 2008 from http://www.privacyrights.org/ar/PreventITWorkplace.htm

[3]Federal Trade Commission. 2008. *Federal Trade Commission (FTC) Business Alert.* Retrieved on November 24, 2008 from http://www.twua.org/Federal%20Trade%20Commission(2).pdf.