Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Conflicting Identities: The Digital Government Dilemma

Over the past several years, government organizations have rapidly technologies to improve service delivery to their citizens. However, governments have moved into this new era of "digital government," to balance the complicated issues of privacy, security, and freedom information has become extremely complex. Due to the type of maintained by governments about its citizens, digital government contribute to the growing problem of identity theft. Sensitive information deemed difficult to attain from a government is often...

Copyright SANS Institute
Author Retains Full Rights

AD

Conflicting Identities – The Digital Government Dilemma

Balancing Privacy, Public Records Access & Identity Theft Concerns

Kevin Iwersen
April 26, 2004
GSEC Practical v1.4b, Option 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Kevin Iwersen
April 26, 2004
GSEC Practical v1.4b, Option 1

Conflicting Identities – The Digital Government Dilemma
Balancing Privacy, Public Records Access, & Identity Theft Concerns

Abstract

Over the past several years, government organizations have rapidly adopted new technologies to improve service delivery to their citizens. However, as governments have moved into this new era of "digital government," the struggle to balance the complicated issues of privacy, security, and freedom of information has become extremely complex. Due to the type of information maintained by governments about its citizens, digital government services may contribute to the growing problem of identity theft. Sensitive information once deemed difficult to attain from a government is often now readily available from anywhere in the world, via the use of a simple web browser.

This paper investigates the growing problem of delivering government services via the Internet while also addressing the concerns of identity theft. As citizens continue to demand more simple access to government services, governments must be keenly aware of how they transition their traditional "brick and mortar" services into the digital government age without also endangering the privacy of their constituents. Case examples from various levels of government will demonstrate the ease of access to private information as well as highlight the complexity of this issue. Instances of how local and state governments are attempting to strike a balance on this issue will be provided. The author will conclude this paper by providing a review of federal, state, and local laws that highlight the growing trend of continued legislation to address this perceived problem. Despite the growing debate and increased legislation, the author will conclude by highlighting many digital government services that are yet to be resolved and continue to possibly endanger citizens' privacy.

The Problem

Over the past several years, governments have been rushing to improve service delivery to their citizens by embracing the Internet and on-line web services. Local, state, and federal government agencies have developed extensive web portals to streamline access to government services and information. Government policy makers are often heard echoing a common phrase to their institutions -- "We must get our citizens on-line, not in line." However, due to the nature of government and its open records laws, this continued movement to

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

web-based services has run head on into the complex issue of protecting the privacy of individuals.

Often, information held by governments contains sensitive data that comprise a citizen's identity. Information such as social security numbers, dates of birth, driver's license data, and marriage records are often maintained by various government entities. Other types of personal information held by the government may be found on professional licensing applications, business records, various lien filings, real estate proceedings, and court opinions. Access to such personal identifying information could severely compromise a citizen's identity, if not appropriately protected. With identity theft continually on the rise, and as governments persistently make more information available via the Internet, the concern of contributing to the epidemic problem of identity theft is real.

Identity theft is one of the fastest growing crimes in the nation. In 2003, the Federal Trade Commission received 214,905 identity theft complaints from consumers, up from 86,212 complaints just two years prior in 2001.[1] In other studies by Gartner Research and Harris Interactive, "approximately 7 million people became victims of identity theft in the prior 12 months. That equals 19,178 per day, 799 per hour, 13.3 per minute."[2] According to the U.S. Secret Service, identity theft has directly led to the annual loss of over $745 million to consumers.[3] These continued trends highlight the increasing problem of protecting one's information. In fact, many experts classify identity theft as the fastest growing crime in the nation.

One of the prime reasons identity theft continues to increase so dramatically can be attributed to how easy it is to conduct the crime. Identity theft simply begins by obtaining personal information about a person to be used for malicious or illegal purposes. Identity thieves prey on multiple sources to steal personal identifying information. Some thieves obtain information from bank statements, credit card applications, and other similar documents by physically searching through dumpsters (often referred to as "dumpster diving") or by stealing mail directly from mailboxes. These thieves are consistently looking for any personal information that could assist them in gaining the identity of another person. Medical bills, receipts, real estate proceedings (such as lease or mortgage documents), bank statements, and other similar documents are common sources valued by identity thieves as they physically dig for personal information. However, as with most crimes, if thieves can attain anonymity in some form, they will typically opt to "hide" behind this perceived veil of secrecy instead of physically exposing themselves in the act of the crime. The Internet has provided these thieves with that sense of anonymity. As opposed to digging

[1] Federal Trade Commission. URL: http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf
[2] Identity Theft Resource Center. URL: http://www.idtheftcenter.org/facts.shtml
[3] Cantwell. URL: http://cantwell.senate.gov/ID/statistics.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

through garbage cans or conducting quick "drive-bys" of mailboxes, the thief can now simply sit behind a computer and search the Internet for this same type of information.

With the simple power of a web browser and a search engine, identity thieves are employing new methods to hunt for and steal such information. Reported identity theft cases have revealed thieves searching for data on genealogy web sites[4], phone/address listings, alumni databases, and employment sites. As governments continue to offer searchable databases and on-line documents to their constituents, identity thieves are attempting to leverage these new sources of information for malicious use. Although governments are making their services easier to use with the best of intentions, they are also empowering identity thieves to conduct their crime with greater and greater ease.

Case Examples – Digital Government Services & Identity Theft Concerns

In many cases, local, state, and federal governments understand this complicated issue of improving their services while also trying to protect the privacy of their citizens. However, as they wrestle with the need to find the optimal balance, their laws and rules often tie their hands. As seen in many states, open records laws often contribute to the problem, by encouraging (if not mandating) governments to provide the same level of access to public records on-line as it is provided for in-person requests. The State of Missouri's "Sunshine Law" is a perfect example of legislation that can contribute to agencies placing personal information on the web that may not be best suited for this type of medium. As part of its open records law, the State of Missouri strongly encourages its agencies "to provide access to its public records to members of the public in an electronic format."[5] This push to provide open access to public records via the Internet is designed to streamline government services; however, as demonstrated by the Jackson County government in Missouri, it also causes significant concern on the types of information available on-line. Jackson County recently began offering full on-line services to public documents on its county web site. However, Missouri's local press and the U.S. Postal Inspection Service have raised identity theft concerns with Jackson County's web services.[6] After an exhaustive search of this county's web site, an individual can quickly see the complication of providing government services while limiting the exposure of personal information. Within minutes, anyone on the Internet can quickly access the following information from this county's web site:

- Birth certificates with full name, place of birth, and date of birth;

[4] Fletcher, et al. URL: http://www.personal.psu.edu/users/g/r/grf111/evidence/identitytheft.htm
[5] Missouri Sunshine Law. URL: http://ago.missouri.gov/sunshinelaw/chapter610.htm
[6] Curry. URL: http://www.examiner.net/stories/030604/new_030604024.shtml

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Death certificates with full name, social security numbers, place of birth, date of birth, and last residential address;
- Decrees with full names and social security numbers;
- Discharge of property liens with full names, addresses, and social security numbers;
- Expunged affidavits with full names, addresses, and social security numbers;
- "Intent to home school" applications with full names (student and parents), addresses, and dates of birth;
- Marriage license applications with full names, places of birth, and dates of birth;
- Partial real estate tax liens with full names, addresses, and social security numbers; and,
- Wills with full names, dates of birth, and addresses.

Fort Bend County, Texas, serves as another example of how simple the government has made it for an identity thief to access personal information from public records. Identifying information to include full names, places of birth, dates of birth, social security numbers, and full addresses are readily available through the multiple searches on this county's public web site.[7] Furthermore, Fort Bend County has made a public policy decision to post extensive electronic versions of court documents, fully searchable via the Internet. These documents often include sensitive information such as dates of birth, social security numbers, and photocopies of driver's licenses (including driver's license numbers, current address, and other personal data).

Amongst state and county governments, the State of Washington is often referred to as the leader in digital government technologies. Washington's county governments are fully embracing this concept of digital services and improving access to constituent information. Snohomish County, located in the northwest section of Washington, has deployed a comprehensive on-line system to access public records. Public records documents such as birth certificates, death certificates, tax liens, marriage applications, releases, name change orders, and numerous other forms are fully available on-line. The "Records/Recorded Documents Search" option at the Snohomish County web site[8] demonstrates how access to government documents unfortunately provides opportunities for possible identity theft.

Within North Carolina, the state's public law (chapter 132) encourages all government entities to provide access to public records at minimal or no cost.[9]

---

[7] Fort Bend County.
URL: http://www.co.fort-bend.tx.us/Admin_of_Justice/County_Clerk/index_info_research.htm
[8] Snohomish County. URL: http://www.co.snohomish.wa.us/auditor/index.asp
[9] North Carolina, Chapter 132.
URL: http://www.ncga.state.nc.us/statutes/generalstatutes/html/bychapter/chapter_132.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

New Hanover County has embraced on-line delivery to achieve this goal. The county has deployed Hart InterCivic's[10] Internet Public Access Module to assist them in making access to public records as accessible and inexpensive as possible. The county predominantly displays its on-line public records search capability[11] via its web portal which provides an extensive search capability for numerous public records that could contain sensitive, personal information. New Hanover County does have a clearly identified privacy policy that obviously permits the disclosure of publicly recorded information; however, this policy does not limit the accessibility to personal information.

Searching for Balance – Policy and Legislation

As demonstrated above, the examples of government on-line systems prove how easy identity theft could occur if governments do not set appropriate policies to protect personal information. Many levels of government are obviously moving forward with deploying robust on-line systems to improve access to public records – often with what appears to be little regard to the complex problem of protecting the identity of individuals. However, there are many county and state governments that are attempting to strike a balance with this complicated issue. Different types of policies and/or legislation have been enacted throughout all levels of government to address this problem.

Mecklenburg County, North Carolina, provides an example of how local governments are improving their information services while attempting to achieve a balance by preventing complete access to identification data via the Internet. For instance, via Mecklenburg County's site[12], individuals can search for birth and death certificate information; however, one cannot view the actual certificate on-line. Access to this specific information still requires a formal request to the recorder's office with appropriate remittance of a document request fee. Although the County restricts direct access to this specific type of information, they do continue to struggle with other forms of public data. For instance, the county still provides complete on-line viewing of bankruptcy filings and tax liens, both of which include full names, social security numbers, addresses, and other personal information.

As other counties throughout the United States have adopted various technologies to ease access to public records, they have also taken steps to limit the scope of access to such data from the Internet. Within the State of Colorado, the Douglas County's web portal provides access to a public records search engine designed to help the county "live up to (its) commitment to provide the

[10] Hart InterCivic. URL: http://www.hartintercivic.com/news/press_releases.asp?id=89
[11] New Hanover County. URL: http://srvrodweb.nhcgov.com/localization/menu.asp
[12] Mecklenburg County.
URL: http://www.co.mecklenburg.nc.us/Departments/Register+of+Deeds/home.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

finest service possible to the public."[13] This search capability provides access to many public records; however, due to a unique approach within Colorado, the access to the majority of identifying information is limited. This is due to the State of Colorado's recognition of the growing problem in providing on-line access to birth, death, and marriage certificates and how these types of services contribute to identity theft. Colorado has taken steps to educate its constituents about this problem on its vital statistics web site.[14] They have provided a general overview of the conflict with identity theft related to the access to vital records, and further provide advice to its citizens on how to protect their identities. More importantly, the State of Colorado has established a statewide policy that all "requests for birth and death records must be accompanied by a photocopy of the requestor's identification (front and back sides) before processing."[15] General detail information for each type of certificate (e.g. birth, death, marriage, divorce, etc) is searchable; however, the specific identifying information is restricted and only available via a formal request at the appropriate county office.

California has taken similar actions to prevent identity theft associated with access to vital records. Sonoma County's web site states that "in an attempt to stop the illegal use of vital records, and as part of statewide efforts to reduce identity theft, a new law (effective July 1, 2003) changed the way certified copies of birth and death certificates are issued. Certified copies to establish the identity of a registrant can be issued only to authorized individuals."[16] This new law changed the method that Sonoma County provides access to such certificates via the Internet, and even changed how they issue documents via their traditional request processes. For instance, if you are not an authorized individual, the county will now only issue "Certified Informational Copies" with the following phrase imprinted across the document -- "Informational, Not a Valid Document to Establish Identity."

As demonstrated by Colorado and California, public policy and law are starting to recognize the identity theft concerns, at least within the realm of public vital statistics data. This type of information – birth, death, and marriage certificates – are obvious sources of personal data. However, there are many more data sources that contain detailed, personal identifying information. It is within these other forms of data that the public policy debate continues. One of the heavily debated aspects of these additional types of data revolves around the access to various court documents. As reported in a Wired article in 2001, "because court documents contain social security numbers, bank account records or excruciatingly embarrassing details about one's personal life, privacy advocates

---

[13] Douglas County Clerk & Recorder.
URL: https://secure.douglas.co.us/NASApp/pubdocaccess/simpleSearch.jsp

[14] Colorado Department of Public Health and Environment.
URL: http://www.cdphe.state.co.us/hs/certs.asp

[15] ---. URL: http://www.cdphe.state.co.us/hs/birth.html#documentation

[16] Sonoma County Clerk. URL:
http://www.sonoma-county.org/Clerk/HTML_Documents/BDMCerts/Frameset_BDMCerts.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

see online access to legal records as a worrisome proposition."[17] Since that article, multiple court access systems have popped up across the Internet, providing extremely simple access to court documents that contain personal information. This type of information, if not appropriately controlled, could potentially be used to conduct identity theft. For instance, within Kootneai County, Idaho, the district court provides an on-line capability to view the court's opinions. While this capability provides a tremendous service to the legal and public community, it also contributes to identity theft concerns. For instance, within various court opinion documents viewable on its web site[18], one can quickly find highly specific identifying information (such as within child custody proceedings). The Seventh District Court of Appeals within the State of Ohio provides a very similar functionality with a feature-rich search engine for all of its court opinions since 1999.[19] This functionality enables a malicious person to quickly search through court documents for personal identifying information.

Due to these concerns of privacy and on-line access to court documents, the Florida Supreme Court issued an administrative order[20] on November 25, 2003, restricting the extent to which court records can be published on the Internet. This court order was the direct result of a study conducted by Florida's Judicial Management Council to review the impacts of providing court information via the Internet. The Council "concluded that current regulation of access to court information is minimal, and may be inadequate in some instances to protect the privacy interests of the public and those directly or indirectly involved in court proceedings, while assuring public records."[21] In the interim, the Council recommended an immediate suspension of on-line court systems until a more complete review, with detailed recommendations, could be made. Based in large part to the Council's report, Florida Chief Justice Harry Lee Anstead issued the temporary court order that essentially stopped any further "bulk electronic distribution"[22] of court records on Florida government web sites until the issue can be more fully addressed by the Florida Supreme Court's Committee on Privacy and Court Records. The order does permit certain types of information to be distributed via the web; however, the overwhelming majority of Florida court documents cannot currently be accessed on-line. Users who attempt to access information that was previously accessible through the Internet are now greeted with messages such as this one: "Documents previously available on this page have been removed pursuant to Administrative Order AOSC03-49 (Nov. 25,

---

[17] Glasner, Joanna. URL: http://www.wired.com/news/politics/0,1283,41967,00.html
[18] Kootenai County District Court. URL: http://www.co.kootenai.id.us/departments/districtcourt/
[19] Supreme Court of Ohio. URL: http://www.sconet.state.oh.us/rod/documents/?source=7
[20] Supreme Court of Florida No. AOSC04-4. p1.
URL: http://www.flcourts.org/sct/clerk/adminorders/2004/sc04-04.pdf
[21] --- p2. URL: http://www.flcourts.org/sct/clerk/adminorders/2004/sc04-04.pdf
[22] Supreme Court of Florida, Press Release. URL:
http://www.flcourts.org/pubinfo/documents/pressreleases/11-25-2003_PressReleasePrivacyCourtRecords.pdf#xml=http://www.flcourts.org/cgi-bin/texis.exe/webinator/newsearch/xml.txt?query=committee+on+privacy&db=db&id=4088ceff0

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

2003)."[23] Recommendations to the Florida Supreme Court on how to achieve a more optimal balance between privacy and public records are due sometime in the summer of 2004.

In the 2003 legislative assembly within the Virginia Commonwealth, the issue of balancing privacy with on-line public access of court information was a much-debated issue. House Bill 2426, "Posting Certain Information on the Internet; Prohibitions," sought to restrict specific identifying information from being posted onto county web sites. As part of this legislation, "no court clerk shall post on a court-controlled website any document that contains the following information: (i) an actual signature; (ii) a social security number; (iii) a date of birth identified with a particular person; (iv) the maiden name of a person's parent so as to be identified with a particular person; (v) any financial account number or numbers; or (vi) the name and age of any minor child."[24] After much debate regarding the language within this bill, both the House and Senate approved the bill. The bill became law on April 3, 2003, when the Governor concurred with this action. However, the new law does provide an "escape clause" in which subscription-based services do not have to comply so long as the on-line service has been approved by Virginia's Department of Technology Planning. Because of this clause, many entities are still concerned that Virginia's legislation permits too much access to personal data and does not truly achieve the appropriate balance.[25] However, others believe that the new law is too restrictive and violates the principles of open government. For instance, in King George's County, a private company is attempting to gain access to the county's court documents (via a Freedom of Information request) and place them on-line.[26] Although Virginia leads many other states with this new law, it is evident that the debate rages on.

As opposed to legislation, Wisconsin's courts have attempted to strike a balance with this precarious issue by developing a "Policy on Disclosure of Public Information Over the Internet."[27] The policy was put in place to address growing privacy and identity thefts concerns with the popular Wisconsin Consolidated Court Automation Program (CCAP).[28] Per Wisconsin Court System's Chief Information Officer, Jean Bousquet, the Wisconsin Circuit Court Access site has

---

[23] Supreme Court of Florida, Briefs and Other Documents.
URL: http://www.flcourts.org/pubinfo/summaries/briefs/01/01-2351/
[24] Nixon. URL: http://leg1.state.va.us/cgi-bin/legp504.exe?ses=031&typ=bil&val=hb2426
[25] Stollenwerk. URL: http://www.fauquiernews.com/012202issue.htm
[26] Davis. URL: http://www.opengovva.org/courts/publicdatabase.html
[27] Wisconsin Court System – Director of State Courts. URL: http://wcca.wicourts.gov/AB0304.xsl;jsessionid=AADC313A862D534E6601B587FD92BA7D.render4
[28] Wisconsin Court System – Circuit Court Access. URL: http://wcca.wicourts.gov/index.xsl;jsessionid=AADC313A862D534E6601B587FD92BA7D.render4

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

over 925,000 searches on a daily basis.[29] This system has proven to be extremely valuable to the courts, lawyers, and individuals. However, because of the sensitive nature of the information contained within the system, Wisconsin developed this specific privacy policy. Upon examination, the policy does not necessarily add any new protections for private information; however, it does provide a construct to educate the public on how the system is designed to comply with existing public records laws.

In addition to court records, private identifying data can easily be attained from motor vehicle records if not protected appropriately. Many states have taken actions to address this concern. As a case in point, the State of Iowa attempted to resolve this access problem by enacting a new section of state code – 321.11.[30] This law allows individuals to protect their personal information contained within motor vehicle records from public disclosure by requiring that only certain authorized officials (such as law enforcement personnel) can request driver information when requested by plate number. In addition to protecting motor vehicle information, Iowa also passed a law that helps protect identifying information on voter registration records. Iowa Code section 48A.11 was modified to allow citizens to remove their Social Security number, middle name, and telephone number from these records. On the new Iowa voter registration cards (as evidenced on Polk County's web site)[31], the privacy notice now states that the request for the social security number is voluntary and not required, thus providing the citizen an opportunity to limit the amount of identifying information maintained by the county and state government.

In the Wisconsin legislature, significant actions to more fully restrict on-line disclosure of private information have been pursued. The Associated Press reported on an initiative headed by Representative Marlin Schneider to prevent agencies from publishing various types of personal data on Internet-accessible web sites.[32] Assembly Bill 541 would have prevented agencies from publishing "a) the individual's birthdate; b) the number of a driver's license issued to the individual by the Department of Transportation; c) the social security number of the individual; d) the telephone number at the individual's place of employment; and e) the unpublished home telephone number of the individual."[33] The bill died within Wisconsin's Government Operations and Spending Limitations Committee; however, the intensity of the debate on this issue has not subsided.

Obviously, the entire subject of privacy, identity theft, and public access to government records is not limited solely to local and state governments. The

---

[29] Bousquet. URL: http://www.courtaccess.org/states/wi/documents/wi-article-bousquet-policyonaccess.doc
[30] Iowa Code 321-11. URL: http://www.legis.state.ia.us/IACODE/1999/321/11.html
[31] Polk County. URL: http://www.co.polk.ia.us:8080/downloads/elect/VoterRegistration.pdf
[32] Richmond. URL: http://www.courtaccess.org/states/wi/documents/wi-article,richmond-lawmakerstargetidtheft03.pdf
[33] Schneider. URL: http://www.legis.state.wi.us/2003/data/AB-541.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Federal government has taken various actions to protect individual's privacy rights, particularly as it relates to identity theft. In 1998, Congress approved the Identity Theft and Assumption Deterrence Act. This Act makes it a federal crime when anyone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[34] Whereas this law does not necessarily address the public policy issues of restricting access to personal information maintained by governments, it does provide an enormous tool in ensuring that those who do take advantage of on-line government services can be prosecuted accordingly.

In addition, the Federal government has taken specific actions that do assist local governments with the public policy debate of how to protect certain types of citizen data. As an example, the Driver's Privacy Protection Act of 1994 puts restrictions on the disclosure of personal information within motor vehicle records.[35] Likewise, the Family Educational Rights and Privacy Act of 1974 also stipulates limitations on access to educational records. Agencies that maintain educational records must ensure the privacy of certain types of information; otherwise, they will no longer receive federal funding.[36] These examples do not necessarily address the entirety of the issue for local governments; however, they do illustrate the trend by the Federal government to continue to enact legislation for specific types of information that must be protected.

Conclusion

The quandary with this entire issue of balancing privacy and identity theft concerns with access to public records is the scope of the problem. All levels of government contain specific information about its citizens, and many of these government echelons have made public policy decisions (to some extent). The Federal government has attempted to resolve the privacy issue with motor vehicles data; several States have specifically addressed access issues with vital health records (such as birth and death certificates); and many local county governments have decided not to post divorce documents. However, the number of different types of information can be overwhelming if governments continue to try to address each specific dataset within its own specific echelon of government. Property tax assessor files, voter registration files, professional licenses, business licenses, court files, case indexes, tax liens, judgments, bankruptcy files, criminal arrest records, warrants, and civil court proceedings are all examples of the plethora of government information that possibly contains

---

[34] U.S. Code Title 18, Part 1, Chapter 47, Sec 1028.
URL: http://www4.law.cornell.edu/uscode/18/1028.html

[35] U.S. Code Title 18, Part 1, Chapter 123, Sec 2721.
URL: http://www4.law.cornell.edu/uscode/18/2721.html

[36] U.S. Code Title 20, Chapter 31, Sec 1232g.
URL: http://www4.law.cornell.edu/uscode/20/1232g.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

personal and identifying information. Each of these areas, and many others, need to be addressed with an intentional public policy decision.

As demonstrated throughout this document, the continued concern of protecting citizen's privacy (specifically as it relates to the opportunity for identity theft) and the desire to simplify access to government services and information continues to be debated at all levels. Many county and state governments are embracing this issue head-on and are attempting to address it through either policy or legislation. In some circumstances, as demonstrated by the Florida Supreme Court, governments have placed self-imposed moratoriums on publishing personal data on-line until they can come to a consensus on how to address this growing problem. However, as also demonstrated, many levels of government are simply transitioning their existing public record processes into robust, feature-rich web portals -- all in the name of improving government access. For many of those government entities that are moving forward with digital government initiatives, they have simply adopted a public policy position that mirrors their existing open records laws – stating that the information is open to the public and should therefore be accessible via the Internet. This debate will continue to be held in multiple forums – from the local county commissioner meeting rooms to the halls of Congress. Until these public policy debates address this issue, the risk will be evident – personal, identifying information will be accessible via the Internet and may contribute to the danger of identity theft.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

Bousquet, Jean. "Policy on Access to Court Records." URL: http://www.courtaccess.org/states/wi/documents/wi-article-bousquet-policyonaccess.doc (24 Apr 2004).

Cantwell, Senator Maria. "Fighting Identity Theft." URL: http://cantwell.senate.gov/ID/statistics.html (20 Mar 2004).

Colorado Department of Public Health and Environment. "Birth and Death Certificates." URL: http://www.cdphe.state.co.us/hs/birth.html#documentation (26 Apr 2004).

Colorado Department of Public Health and Environment. "Identity Theft and Vital Records." URL: http://www.cdphe.state.co.us/hs/certs.asp (26 Apr 2004).

Curry, Dan. "On line records may tell more than you'd like." The Examiner. 6 Mar 2004. URL: http://www.examiner.net/stories/030604/new_030604024.shtml (24 Apr 2004).

Davis, Chelyen. "Records Access on Trial." The Free Lance-Star. 28 Dec 2003. URL: http://www.opengovva.org/courts/publicdatabase.html (25 Apr 2004).

Douglas County Clerk & Recorder. "Douglas County Public Document Access." URL: https://secure.douglas.co.us/NASApp/pubdocaccess/simpleSearch.jsp (24 Apr 2004).

Federal Trade Commission. *National and State Trends in Fraud and Identity Theft, January-December 2003.* 22 Jan 2004. URL: http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf (15 Feb 2004).

Fletcher, Gregory, et al. "Identity Theft – A Case of Stolen Identity." URL: http://www.personal.psu.edu/users/g/r/grf111/evidence/identitytheft.htm (20 Mar 2004).

Fort Bend County. "County Clerk -- Index Information Research." URL: http://www.co.fort-bend.tx.us/Admin_of_Justice/County_Clerk/index_info_research.htm (20 Mar 2004).

Glasner, Joanna. "Courts Face Privacy Conundrum." Wired News. 26 Feb 2001. URL: http://www.wired.com/news/politics/0,1283,41967,00.html (26 Apr 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Hart InterCivic. "Press Release: New Hanover County Will be First in North Carolina With Hart InterCivic's Advanced Indexing System for Public Records." 2 Apr 2003. URL: http://www.hartintercivic.com/news/press_releases.asp?id=89 (26 Apr 2004).

Identity Theft Resource Center. "Facts and Statistics." 15 Feb 2004. URL: http://www.idtheftcenter.org/facts.shtml (20 Mar 2004).

Iowa Code 321-11. "Records of Department." 18 Mar 2004. URL: http://www.legis.state.ia.us/IACODE/1999/321/11.html (24 Apr 2004).

Kootenai County District Court. "District Court Home – Opinions." URL: http://www.co.kootenai.id.us/departments/districtcourt/ (20 Mar 2004).

Mecklenburg County. "Register of Deeds" URL: http://www.co.mecklenburg.nc.us/Departments/Register+of+Deeds/home.htm (25 Apr 2004).

Missouri Sunshine Law. "Chapter 610, Governmental Bodies and Records." 8 Jan 2004. URL: http://ago.missouri.gov/sunshinelaw/chapter610.htm (15 Feb 2004).

New Hanover County. "Register of Deeds." URL: http://srvrodweb.nhcgov.com/localization/menu.asp (26 Apr 2004).

Nixon, Samuel A. Commonwealth of Virginia. "HB 2426 Posting certain information on the Internet; prohibitions." URL: http://leg1.state.va.us/cgi-bin/legp504.exe?ses=031&typ=bil&val=hb2426+ (24 Apr 2004).

North Carolina, Chapter 132. "Public Records." URL: http://www.ncga.state.nc.us/statutes/generalstatutes/html/bychapter/chapter_132.html (26 Apr 2004).

Polk County. "Iowa Voter Registration Information." URL: http://www.co.polk.ia.us:8080/downloads/elect/VoterRegistration.pdf (26 Apr 2004)

Richmond, Todd. "Wisconsin Legislature: Lawmaker targets identity theft." Twincities.com. 5 Sep 2003. URL: http://www.courtaccess.org/states/wi/documents/wi-article,richmond-lawmakerstargetidtheft03.pdf (24 Apr 2004).

Schneider, Marlin D Representative. "2003 Assembly Bill 541." 29 Sep 2003. URL: http://www.legis.state.wi.us/2003/data/AB-541.pdf (25 Apr 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Sonoma County Clerk. "Birth, Death, & Marriage Certificates." 4 Feb 2004. URL: http://www.sonoma-county.org/Clerk/HTML_Documents/BDMCerts/Frameset_BDMCerts.htm (26 Apr 2004).

Snohomish County. On-line Government Information & Services. "Auditor's Home Page." URL: http://www.co.snohomish.wa.us/auditor/index.asp (20 Mar 2004).

Stollenwerk, Mike. "Fairfax Citizen Urges Strengthening and Passing HB 2426 Amending the Data Collection and Dissemination Practices Act." Fauquiernews.com. 22 Jan 2003.
URL: http://www.fauquiernews.com/012202issue.htm (25 Apr 2004).

Supreme Court of Ohio. "Reporter of Decisions – Opinions & Announcements." 1 Dec 2003. URL: http://www.sconet.state.oh.us/rod/documents/?source=7 (20 Mar 2004).

Supreme Court of Florida, Briefs and Other Documents. "Case No. 01-2351" 25 Nov 2003. URL: http://www.flcourts.org/pubinfo/summaries/briefs/01/01-2351/ (24 Apr 2004).

Supreme Court of Florida No. AOSC04-4. "In Re: Committee on Privacy and Court Records." 25 Nov 2003.
URL: http://www.flcourts.org/sct/clerk/adminorders/2004/sc04-04.pdf (24 Apr 2004).

Supreme Court of Florida, Press Release. "Supreme Court Adopts Policy to Protect Privacy in Court Records." 25 Nov 2003. URL: http://www.flcourts.org/pubinfo/documents/pressreleases/11-25-2003_PressReleasePrivacyCourtRecords.pdf#xml=http://www.flcourts.org/cgi-bin/texis.exe/webinator/newsearch/xml.txt?query=committee+on+privacy&db=db&id=4088ceff0 (24 Apr 2004).

U.S. Code Title 18, Part 1, Chapter 47, Sec 1028. "Fraud and related activity in connection with identification documents and information."
URL: http://www4.law.cornell.edu/uscode/18/1028.html (10 Apr 2004).

U.S. Code Title 18, Part 1, Chapter 123, Sec 2721. "Prohibition on release and use of certain personal information from State motor vehicle records."
URL: http://www4.law.cornell.edu/uscode/18/2721.html (10 Apr 2004).

U.S. Code Title 20, Chapter 31, Sec 1232g. "Family educational and privacy rights." URL: http://www4.law.cornell.edu/uscode/20/1232g.html (22 Apr 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Wisconsin Court System – Circuit Court Access. "Access to the Public Records of the Consolidated Court Automation Programs (CCAP)." URL: http://wcca.wicourts.gov/index.xsl;jsessionid=AADC313A862D534E6601B587FD92BA7D.render4 (25 Apr 2004).

Wisconsin Court System – Director of State Courts. "Policy on Disclosure of Public Information Over the Internet." URL: http://wcca.wicourts.gov/AB0304.xsl;jsessionid=AADC313A862D534E6601B587FD92BA7D.render4 (25 Apr 2004).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**