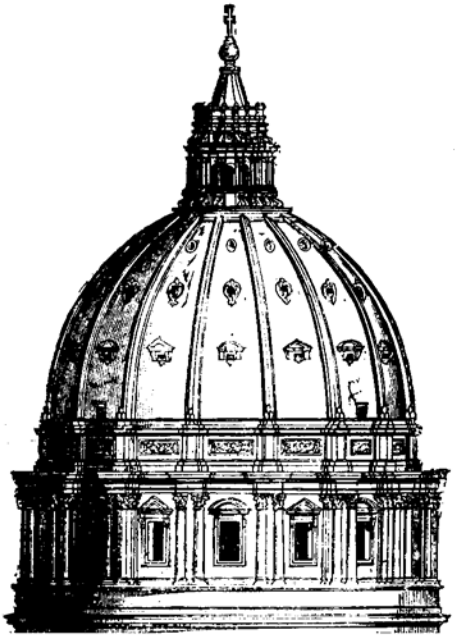
ISSUE BRIEF #02/2009



Privacy Issue Brief

BY DAVID WILLIAMS

CITIZENS AGAINST GOVERNMENT WASTE

1301 Connecticut Avenue, N.W.
Suite 400
Washington, D.C. 20036-1838

1.800.Be.Angry

www.cagw.org

CITIZENS AGAINST GOVERNMENT WASTE

Citizens Against Government Waste (CAGW) is a private, nonprofit, nonpartisan organization dedicated to educating the American public about waste, mismanagement, and inefficiency in the federal government.

CAGW was founded in 1984 by J. Peter Grace and nationally-syndicated columnist Jack Anderson to build support for implementation of the Grace Commission recommendations and other waste-cutting proposals. Since its inception, CAGW has been at the forefront of the fight for efficiency, economy, and accountability in government.

CAGW has more than one million members and supporters nationwide. Since 1986, CAGW and its members have helped save taxpayers more than $1 trillion.

CAGW publishes a newsletter, Government Waste Watch, and produces special reports, and monographs examining government waste and what citizens can do to stop it.

CAGW is classified as a Section 501(c)(3) organization under the Internal Revenue Code of 1954 and is recognized as a publicly-supported organization described in Section 509(a)(1) and 170(b)(A)(vi) of the code. Individuals, corporations, companies, associations, and foundations are eligible to support the work of CAGW through tax-deductible gifts.

1301 Connecticut Avenue, NW
Suite 400
Washington, DC 20036
Phone: (202) 467-5300
Internet Address: www.cagw.org

PRIVACY

The world is in the information age. Electronic communications are helping companies, no matter their size, compete more efficiently and more effectively in global markets. Consumers are using the Internet to purchase goods and services and participate in social networking sites Governments are relying on electronic communications to provide citizens more efficient services. All levels of government are also collecting information and data is being gathered and analyzed at an alarming rate.

In particular, as the Internet and technology become more integrated into everyone's life, the gathering and protection of personal information is critical. The use of search engines and social networking sites has become commonplace. These tools help people connect and explore new concepts in ways that were unimaginable a few years ago. While these new tools may help individuals find a new pair of jeans or stay in touch with their friends, they are testing how people think and feel about sharing so much information about themselves and the boundaries of individual privacy.

Most people do not know when they search for "blue jeans" using their favorite search engine; they are actually sharing a little bit of information about themselves. Some knowingly accept giving up a bit of anonymity for better search results. Others either don't know they are doing so or have to weigh that choice. In some cases, search terms are tracked to better deliver relevant advertising for that individual.

Once that perfect pair of blue jeans is found, the purchase of the product requires sending financial information to the seller. A typical form of payment, credit cards (which contain sensitive information), are increasingly under attack by identity thieves.

Social networking sites also use similar ways to understand user preferences. It is no coincidence that a 42 year-old single male on Facebook receives dating service ads for the 40+ crowd.

The government is also gathering detailed information about people. From tracking regional outbreaks of the influenza virus, to homeland security, governments are relying more and more on databases of information.

There are cases where giving up personal information is voluntary, such as the Clear travel program, administered by the Transportation Security Administration. Clear, according to its website, is "a high-tech card that gives you access to express security lines at airports across the country. Instead of inching along through airport security, you fly through in mere minutes, arriving at your gate stress free."[1] This service costs money and requires relinquishing background information to the private entity that administers the program.

However, most federal government data collection is not voluntary and does not provide anyone with an "opt out" option. New security measures at the border are testing the boundaries of privacy. For example, the federal government has authorized itself to detain and search suspicious laptops.

The government's role and responsibility in protecting one's privacy is becoming more important as the governments at all levels collect and retain information on many aspects of Americans' lives. Everyone has a Social Security number and everyone who has income fills out a tax return. Such information has to be protected. Just one example of the vulnerability of individual privacy is an incident in May 2006 at the Department of Veterans Affairs. According to CNN, a "laptop was stolen… from the home of a Veterans Affairs employee who, in violation of agency regulations, took it to a private residence. It contained Social Security numbers, names and addresses for more than 26 million veterans as well as possibly millions of current service members and reservists."[2]

[1] Available at http://www.flyclear.com/what/index.html, accessed December 1, 2008.

[2] Available at http://www.cnn.com/2008/US/03/25/stolen.laptop/index.html, accessed November 17, 2008.

Online privacy has morphed into a global issue of our times. Undergirding the matter are a collection of local, national and international laws – each putting their personal fingerprint on the topic. The European Union, for example, describes an individual's entitlement to privacy as a "fundamental" right. In the Asia-Pacific region, there is a concerted effort for laws and regulations to strike a balance between online privacy protections and economic and trade objectives.

In the U.S., there is much more of a patchwork system. Some states have already enacted their own privacy laws, many of which focus on specific industries, issues or practices. Data breach notification laws are increasing in number faster than other types of privacy laws. For its part, the U.S. federal government has passed privacy laws that impose rules for telecommunications carriers, cable companies, healthcare providers and financial firms. These are complemented by still more laws targeting children's online safety, spam, phishing and mass marketing.

Businesses, anxious to comply with the privacy rules and laws that apply to them, need clear guidelines. Forward-looking, cohesive, and comprehensive yet flexible national laws are needed to stay ahead of online privacy pirates.

This Issue Brief is the first in a series to explore the privacy challenges and the role of government in data governance.

THE PRIVATE SECTOR VS. THE GOVERNMENT

There is a profound difference as to how the private sector reacts to new privacy challenges contrasted to the government's reaction. If history is any guide, government solutions tend to be slow, inadequate and expensive while the private sector tends to react to market demands.

The private sector has not been without its missteps. High profile cases such as Federal Trade Commission v. Petco Animal Suppliers (November 2004) in which Petco failed to protect consumer information from hackers show that not even the private sector is immune to problems.

The fundamental difference is the incentive to change. The private sector has to be more vigilant because failing to do so would mean a potential competitive disadvantage to not changing. There is only one federal government and people do not have the luxury of shopping around for another government.

Understanding the need for increased privacy and what it means to their bottom line, more and more commercial websites are including privacy policies on their homepage.

Another important step forward in protecting privacy is the Global Network Initiative, formed by the three biggest players in the Internet search engine market, Google, Microsoft, and Yahoo!.

According to Forbes.com, the initiative "is based on principles that the companies have spent 18 months hashing out with representatives from the human rights community, academics and ethical investment groups. Among those endorsing the new program Tuesday were Human Rights Watch, the Committee to Protect Journalists, the Center for Democracy and Technology, Harvard University's Berkman Center for Internet and Society and the Calvert Group, a socially responsible money manager. The initiative aims to protect free speech and user privacy, say company representatives. It also aims to deflect efforts by either the private sector or the U.S. Congress to impose their own standards on companies."[3]

[3] Elizabeth Corcoran and Andy Greenberg, "Google, Yahoo!, Microsoft's Privacy Plan," Forbes.com, October 28, 2008.

Not only are there ad hoc private sector groups such as the Global Network Initiative being formed to address these issues, the private sector is starting to offer products and services directly to consumers to protect themselves. For example, Lifelock charges a monthly fee to guard against identity theft. The company is so confident in its ability to protect one's identity that their advertisements feature the chief executive officer driving around New York City boldly displaying his Social Security number.

The establishment of the Global Network Initiative and private sector companies reacting to the challenges facing Americans are two reasons why the government should stay away from regulating privacy. Another reason is the government's track record on this issue.

REAL ID – Poster Child for Privacy

The Real ID Act of 2005 has become the poster child for the federal government's naiveté related to privacy concerns.

Sneaking through the legislative process without any congressional hearings or deliberation, the Real ID Act became law before most members of Congress had a chance to review it. Latching onto the lapels of the May 2005 emergency spending bill, the Act exploited the fears many Americans still have after September 11. Touted as an anti-terrorist and immigration reform bill, the Real ID Act has far greater ramifications. In addition, the multi-billion dollar unfunded mandate to states, Real ID was also a giant step backwards for privacy concerns.

In short, the legislation requires, for the first time, a set of federal minimum standards for authenticating and securing driver's licenses. States will now have to verify birth certificates, federal immigration documents, and Social Security numbers with the appropriate federal departments, build a database to store and secure individuals' identification documents, and train personnel to use the new system. Even though taxpayers and privacy groups scored a small victory when the Department of Homeland Security (DHS) decided that radio frequency identification chips will not be used, there are still some very serious privacy concerns.

Implementing REAL ID will require states to build a new system to verify, track, and store driver information, costing a total of $23 billion.[4] With governments' long history of technological ineptitude, the task is daunting. Furthermore, any storage device concerns privacy groups from both sides of the political aisle. The federal government may not limit the information to only storing a driver's information, but could eventually add a wealth of other data, such as health records (for instance, how many visits to and from hospitals or mental facilities), banking and credit card reports, family history, and a multitude of other personal material.

Security experts question whether the federal government will be able to protect the new "national ID system"[5] against ID thieves. They point out that there are ways to secure the information from thieves (such as building multiple firewalls), but trusting the government, especially DHS which has received four consecutive F grades on the Federal Information Security Management Act scale, is not the best solution.

States are also struggling with privacy issues. In particular, a Pennsylvania grand jury is investigating whether or not a taxpayer funded database was used for political purposes. According to the Philadelphia Inquirer, "The database, developed by GCR & Associates under a contract signed in 2002 by then-Majority Leader John M. Perzel (R., Phila.), is built on a technique called data mining to create detailed profiles of

[4] United States Department of Homeland Security, 6 CFR, Part 37, Docket NO. DHS-2006-0030, p.106.

[5] Lisa Vaas, "Analysts: 'Real ID' Act Could Help ID Thieves," *eWeek*, May 6, 2005, (viewed on October 6, 2005), <http://www.eweek.com/print_article2/0,1217,a=151449,00.asp>.

individuals, which helps lawmakers better tailor messages to constituents. The state Attorney General's Office is scrutinizing use of the GCR database as part of its expanding Bonusgate probe, which is now focusing on whether lawmakers from both parties misused taxpayer-funded technology. While lawmakers for years have used state discretionary accounts to improve technology in their legislative caucuses, it is illegal to use public money or resources for campaigns. Walter Cohen, a Harrisburg lawyer who represents Perzel, said Friday that state investigators were questioning the GCR work as part of a broader review of technology contracts of both parties in the House and Senate."[6]

2008 AND BEYOND

With the election of a new President and a new Congress, the question is how politicians and bureaucrats will use technology and gather information.

Whether it's President Obama's BlackBerry or his more advanced and secure PDA, electronic communications are at the heart of how our new chief executive conducts daily business. His work habits placed electronic privacy in a new light and opened a debate. Should the leader of the free world run the risk of electronic communiqués on his PDA being pirated? Or, more to the point, why shouldn't the U.S. president use the technology to which he is accustomed, the technology that makes him most effective, to do his job? Is it not incumbent on the government and industry to devise the electronic information controls that enable the new U.S. commander-in-chief to communicate as he prefers?

One positive sign is a statement on then Sen. Obama's website, "the open information platforms of the 21st century can also tempt institutions to violate the privacy of citizens. As president, Barack Obama will strengthen privacy protections for the digital age and will harness the power of technology to hold government and business accountable for violations of personal privacy." Let's hope his follow through is as strong as his words.

United States Congress

When the 111th Congress considers privacy issues, members will have the choice to legislate in a rigid or flexible manner, or not to legislate at all.

Rigid legislation would consist of creating a concrete definition of privacy and how it can be violated. This would be more detrimental to protecting privacy because it would tie the hands of authorities in trying to prosecute criminals. All the criminals would have to do is exploit a loophole in any newly created definition of privacy.

To legislate in a flexible manner would be to increase enforcement of violators. This allows for an ever-changing landscape that would be able to adapt as criminals create new schemes.

Anti-spam legislation is a perfect example of what to do and what not to do. In 2003, Citizens Against Government Waste applauded the announcement of industry recommendations aimed at reducing junk emails by the Anti-Spam Technical Alliance (ASTA). ASTA members include America Online Inc., EarthLink, Microsoft Corp. and Yahoo!. The group worked for more than a year to develop industry

[6] Mario Cattabiana and Angela Couloumbis, "Pa. Now Probes GOP Database," *Philadelphia Inquirer,* November 15, 2008, (viewed on November 17, 2008), <http://www.philly.com/philly/hp/news_update/20081115_Pa_now_probes_GOP_database.html?adstring=ph.news/news_update;!category=news_update;&randomOrd=111508095435>.

recommendations that if implemented will go a long way toward reducing unwanted, intrusive spam. The suggestions focus on eliminating email forgery and preventing internet service providers' customers from being the source of spam.

CAGW noted that "as technology advances, spammers will always find new ways to infiltrate email accounts. The private sector can better adapt to these changes, while still allowing legitimate mass emailers to function. Government intervention would hinder such productivity."[7]

Congress should conduct oversight to ensure that federal agencies are mindful of privacy concerns when creating databases. Congress should also ensure that enforcement agencies have the appropriate resources to deal with violators.

Executive Branch

The new President and individual agencies will have a critical role to play in privacy policy. When creating new software programs or safeguarding personal information through stricter security regarding who can access sensitive information, agencies will be at the forefront of privacy protection.

For example, in March 2008, MSNBC reported that State Department officials snooped illegally into the passport information of three of the presidential candidates, Sens. Hillary Clinton (D-N.Y.), John McCain (R-Ariz.), and Barack Obama (D-Ill.). According to MSNBC, "The incidents raise questions as to whether the information was accessed for political purposes and why two contractors involved in the Obama search were dismissed before investigators had a chance to interview them. It recalled an incident in 1992, when a Republican political appointee at the State Department was demoted over a search of presidential candidate Bill Clinton's passport records. At the time, Clinton was challenging President George H.W. Bush."[8]

The loss of sensitive information by the Veterans Administration also shows that each agency has an important role in protecting privacy.

CONCLUSION

With data collection comes responsibility. And, as technological advances continue at breakneck speed, governments at all levels need to protect our tax dollars and privacy. Outdated thinking and failure to react to a changing technological landscape could put tax dollars and privacy at risk.

The President of the United States, the Congress, companies and the American people will be faced with many questions about data governance and privacy. In many cases privacy will be balanced with the need for better homeland protection. The government's seemingly benign collection of data will also be under intense scrutiny. Just as the private sector is learning that there is a difficult balancing act between enhanced customer service through data mining and preference tracking, so will the government.

While there is no single solution to the problems, it is clear that the government and the private sector can learn from each other as they both wade through this new unfamiliar waters.

A positive step in the direction of more cooperation between the private and public sector is the Consumer Privacy Legislation (CPL) Forum. The CPL Forum was created by Microsoft, eBay, Hewlett-Packard, the

[7] Available at: http://www.cagw.org/site/PageServer?pagename=news_NewsRelease_06232004, (viewed on November 17, 2008).

[8] Available at: http://www.msnbc.msn.com/id/23736254/, (viewed on November 17, 2008).

Center for Democracy and Technology, and Professor Peter Swire of Ohio State University to come up with a framework to analyze and consider consumer privacy legislation.

Although there is no playbook for how to best protect online privacy, a few common sense ideas are as follows:

- Respect that private data has a life span. Its retention and storage should not be infinite. Policies should be established that control and curtail the life span of private data.

- The technology already exists to protect against unauthorized access and misuse of private data. These systems should be liberally employed.

- Take steps to prevent the loss of private data. Whether it be through encryption or technology that prevents access to sensitive data when it is outside an organization's direct control, loss prevention is key.

- Use "smart" data controls. These are controls that can find problems and resolve the difficulties.

It is a brave new (technological) world out there for consumers and the government and privacy will be a key issue for all.