

JBW Group, Inc
PO Box 19373
Minneapolis, MN 55419 USA
International Information Security Consulting
1.612.719.2663
www.jbwgroup.com

Position Paper— Endorsing Senate Bill No. 1307- Privacy Notificationⁱ

Privacy, as envisioned by the framers of the United States Constitution does not exist in 21st Century America. In the mid-to-late 1960's, a plan for a central database with information on US citizens was opposed on the grounds that it put too much power of information in the hands of a very few and could easily be subject to abuse. The situation we find ourselves in today is that our personal information is being collected everywhere in our society. Data is gathered in just about every aspect of our daily lives and often little is being done to protect that information.

My local drugstore has a record of my prescriptions and what I'm being treated for, my medical records reside in multiple locations; family physician, specialist clinics, medical plan providers~ etc.

Part or all of my financial history is stored in multiple places; credit bureaus, banks, credit card clearinghouses and my spending habits are monitored on a regular basis. My mailing address and phone number is traded, bought and sold at so rapid a rate as to make it impossible to stop the flood of junk mail and solicitation calls.

The local video store tracks what movies I've rented, the pizza shack has my pizza preferences and delivery history. Northwest Airlines maintains a record of my travel. Political candidates, parties and PACs all have information about my past contributions, and political leanings.

The phone company maintains records of calls on my landline and cell phone and the GPS chip in the phone can be used to track the location of the phone and my travels.

My Internet surfing is monitored by websites in order to develop a profile of my on-line activities in order to more effectively sell me something. ISPs and ASP cache web pages explicitly to provide quicker response to their customers but the implicit benefit is the sale of web traffic analysis, of great value to marketers. My email address is harvested, bought and sold resulting in a mailbox flooded with marketing for recreational Viagra, bootleg software and pornography. Googling can often produce interesting results, revealing information that should be protected but because of a cavalier attitude or ineptitude is not.

As a result of outsourcing offshore, much of our personally identifiable information now is accessed from or resides in countries that have no laws protecting privacy. The business reality is that it is in the best interest of these off-shore businesses to act with the necessary due diligence to protect the information that has been entrusted to them but there is little recourse for the individual if the confidentiality of their personal information is breached.

The horror stories are seemingly endless; Choicepoint had their business process compromised which resulted in the disclosure of personal financial information of 150,000 individuals (probably a lot more)ⁱⁱ. In late February a Bank

of America cyber-security breach compromised 1.2 million federal employee credit card accountsⁱⁱⁱ. In early March a Lexus-Nexus security breach resulted in disclosure of names, addresses, social security numbers, driver's licenses of 32,000 US citizens^{iv}. DSW Shoe Warehouse suffered a breach of security that resulted in the compromise of shopping habits and credit cards numbers of thousands customers of more than 100 stores^v. Until recently it has been common practice for the state Departments of Motor Vehicles to sell driver's license information of its citizens. The Kentucky Health Cabinet recycled computer systems that contained the names and contact information of 10,000 AIDS patients in the state^{vi}. A ring of Eastern European criminals bought and sold valid credit card numbers stolen from e-commerce web sites^{vii}. And loan and credit applications were discovered in bundles of paper at a Wisconsin recycling facility.

I support Senate Bill 1307 as a necessary first step to raise awareness of the erosion of individual privacy and impose responsibility on those collecting data on behalf of those whose data is being collected.

Next steps for ensuring the privacy of the citizens of Minnesota should include;

- Institute a broader definition of what information should be protected (not just name and account information)
- Expand the definition to include information in all forms beyond digital to include paper, digital in transit and at rest, microfiche, video, audio and spoken words.
- Identify the organizations responsible for enforcement and set penalties for violations
- Provide for full and comprehensible explanation of how information will be used at the point it is being gathered (opt-in)
- Require notification to individuals for the purpose of obtaining approval (or not) before personal information is shared (e.g. selling of lists)
- Provide fair compensation for victims of compromised privacy to include recovery of actual losses
- Enact measures to prevent nuisance civil litigation of privacy violations

Respectfully submitted,

John B. Weaver — CISSP, CISA, CISM CPP
President, CEO
JBW Group Inc
International Information Security Consulting

John B. Weaver is British Standards Institute-qualified in BS7799/ISO17799 Information Security Audit and Implementation with over sixteen years experience in Internet and Information Security. He directed Information Security for a global IP network providing security architecture, policy, regulatory compliance, operational processes and security metrics for both public and internal networks. He has provided security consulting to Fortune 1000 and International companies in Energy, Telecommunications, Financial and Healthcare vertical markets. He has trained Law Enforcement on Internet security related to criminal investigations. He is a member of the Federal Bureau of Investigation's Minnesota chapter of InfraGard, serving on the chapter's Executive Board of Directors. He is a sought-after speaker and frequent media resource on issues of Internet and Information Security, Cyberterrorism, regulatory compliance and protection of the National Infrastructure. He has previously spoken before a Minnesota legislative sub-committee on issues of security, privacy and technology.

ⁱ This testimony was presented to the Minnesota Senate Commerce Committee on March 30, 2005. A data breach notification law was passed during the 2005 session of the Minnesota legislature and effective January 1, 2006. See CHAPTER 167-H.F.No. 2121 of Minnesota Law for specific language.

ⁱⁱ The Choicepoint breach was acknowledged in February 2005.

ⁱⁱⁱ The Bank of America breach occurred in February 2005 when the Bank discovered it had lost backup tapes containing the personal and financial information of federal employees and U.S. senators. The tapes were not encrypted.

^{iv} The LexisNexis data breach was acknowledged in March 2005.

^v DSW Shoe Warehouse credit card information breach was acknowledged in April 2005.

^{vi} The Kentucky Health Cabinet incident was made public in February 2003.

^{vii} Selling valid credit card numbers by an Eastern European ring was reported in March 2001.