

DATA SHARING AND PRIVACY
PANEL DISCUSSION
HOW TO SURVIVE AND STRIVE WITH TECHNOLOGY
Roselyn Marcus, Lead Attorney
Washington State Department of Information Services

1. Introduction

Privacy not a new issue. It takes different forms with each technology advancement. Privacy concerns started with door to door salesman, seen by many as an intrusion on home privacy. This led to no trespassing laws and no salesman allowed signs in many home communities.

As the mail system became more popular so began the selling of addresses. This led to junk mail, catalogues, etc. which in turn led to legislation on opting out of address selling, consent to sell address, request to be taken off lists.

By then, the dream of universal telephone service had pretty much become a reality. So began the selling of home telephone numbers, which led to unwanted telemarketers. We began seeing legislation restricting telemarketers, allowing people to have their telephone numbers taken off the list, etc.

Now you have computer systems, databases and web sites. This leads to the collection and sharing of information. Some people think it has gotten out of hand, so you begin seeing legislation to restrict these activities. Where it will end up, no one is quite sure.

First, I will spend a little time telling you what is going on in the legal arena, state, federal and courts. I will then talk about having an agency privacy policy and what should be addressed in it. If you have a web site, I recommend a privacy notice and will discuss what should be addressed in that notice. Last, if you are going to share data, I will talk about a data sharing agreement and what should be addressed in such an agreement.

2. What is happening in the legal arena.

This issue is problematic because of the delicate balance between privacy and openness. If you listen to privacy groups, the sky is falling and there is no privacy left. They advocate the need for strict regulation and government enforcement. If you listen to commercial groups, there is no problem, sharing information is proper and beneficial and any government restrictions or regulation will inhibit free enterprise and hurt consumers. Where is the truth ? Probably someplace in between.

Currently there is both state and federal laws in this arena. There are state consumer protection laws, laws protecting financial and medical information, etc. You need to know the law in your particular area. There are also federal laws in this area. The Graham-Leach-Bliley Act deals with protecting financial information. The Health Insurance Portability and Accountability Act (HIPPA) protects medical information. Recently the Department of Health and Human Services implemented HIPPA regulations promulgated by the Clinton Administration.

On the horizon, many bills were proposed this past session in the state legislature; everything from prohibiting the use of cookies on the government websites, to creating the office of privacy protection in the Attorney General's Office. None of these bills appear to have made it through the process. However, a bill that exempts from public disclosure the release of volunteer's home addresses and telephone numbers was signed into law.

On the federal level, the Congressional Privacy Caucus, a bipartisan committee, is looking into privacy issues. This Caucus is co-chaired by Republican Richard Shelby (Ala) and Democrat Christopher Dodd (Conn). In addition, there are about 30 bills pending in the federal legislature that deal with privacy issues; from protecting Social Security numbers, creating the Commission for the Comprehensive Study of Privacy Protection, consumer protection bills that deal with the ability to either opt-in or opt-out to the collection of information on the web and the distribution or sale of this information.. Although there has been some discussion as to not continue on the path of piecemeal legislation, and trying to slow down the process, that causes several problems. In particular, various industry group do not want to the states to legislate in this area first.

The courts are beginning to weigh in and it looks like privacy is winning. US Court of Appeals in DC ruled that Trans Union Corporation, a credit information company, does not have the right to sell credit information without the consumers consent. This was a big blow and may be just the beginning. More and more, both courts and legislation are moving in the direction of notice and consent. This means that people should be given notice as to what info is collected and what it is being used for, and get consent before it can be shared.

3. Agency Privacy Policy

If you collect personal information, whether you do so on paper or the net, keep the information in file cabinets or databases, you should have a privacy policy. This policy serves as the framework for the collection, use, storage and sharing of data within an entity.

Canada recently enacted new privacy laws. The laws were taken from a Model Code for the Protection of Personal Information (handout). The Code covers

areas that should be thought through in any organization that deals with personal information and are areas that should be included in an agency privacy policy.

- **Accountability** – Every agency is responsible for the information it collects. The agency should designate an individual or individuals who are accountable for compliance. The agency should let these individuals know they are accountable.
- **Identify Purpose** – When you collect information, you should know why you are collecting it, what is the purpose. The agency should ideally identify this purpose before collecting the information, but at least identify the purpose at the time the information is collected.
- **Consent** – When a person is asked to provide information, the person should know what information is collected, how it will be used and when and to whom it will be disclosed or shared. Also, the person providing the information should consent to this.
- **Limiting Collection** – An agency should limit the information collected to that which is needed to fulfill the purpose for which it is collected. Agencies should respect individuals' rights to their information and not ask more than is needed. The agency should collect the information in fair and lawful ways.
- **Limit Use, Disclosure and Retention** – In the same way you limit collection, you should limit disclosure or sharing of information to those who have a need for the information, unless consent or required by law. In addition, the agency should only keep the information for as long as needed.
- **Accuracy** – If you maintain personal information, and especially if you share it, ensure it is accurate, complete and up-to-date.
- **Safeguards** – The agency needs to determine the sensitivity of the information and then ensure that the proper safeguards and security measures are in place to protect the information. This is going to differ with the type of information collected. Safeguards includes decisions on where you store it, who you give access to, and how access is protected.
- **Openness** – You should allow individuals to know of your practices and procedures regarding the collection, use, storage, protection, and sharing of their data.
- **Individual Access** – If an individual asked, you should let them know what information you have about them, what you use it for, who you disclose it to. The agency should allow individuals access to their information and provide the ability to review information. The agency should allow feedback on the accuracy or completeness of the information. The agency can close the loop

by correcting incorrect information and letting the person know its been corrected.

- **Challenging Compliance** – If the agency is not following its policy, there should be an avenue through which someone can register a complaint. There should also be a process for the complaint to be investigated and practices corrected.

4. **Web site Privacy Notice**

One of the biggest privacy concerns is tracking web usage and information collected at web sites, either knowingly or unknowingly, and what the entity does with this information. Although there is disagreement as to these practices, it seems to be universally recommended and generally acceptance that a web site contain a privacy notice that at least lets people know of their practices. If not voluntarily done, you may see legislation in this area, both at the state and federal level.

The Federal Trade Commission has issued a report on web site Privacy Notices and recommended that all web sites have a notice and that the notice cover four areas: Notice, Choice, Access and Security.

Notice – Includes what information is collected, how that information will be used, and whether the information will be shared with third parties.

Choice – Lets visitor know whether they have a choice as to whether the information is collected, the consequences for not providing the information or not allowing the information to be shared.

Access – Should have a system in place where a person can access the information collected, be able to review and correct the information and delete it if desired. How to do that should be included in the notice.

Security – Should let visitors know generally about the security of the site and the information collected.

Governor Locke issued an Executive Order (EO 00-03) on 2000 dealing with privacy and included a requirement that all state agencies have a privacy notice, prominently linked from the agency's home page and every other page where personal information is collected. The notice is to include those four areas outlined above and some additional areas as well. DIS prepared a Model Privacy Notice that agencies need to use in drafting their own. Included as handout.

5. **Data sharing Agreement**

You should have a data sharing agreement with whomever you are going to share the data with. This allows you to set forth the responsibilities and liabilities for each entity. The data sharing agreement should, at a minimum, address the following areas:

- What data you will share;
- Who you will share the data with;
- Who needs to sign a separate agreement – entity or employees;
- What can be done with the data shared;
- Instructions on how the data should be maintained;
- Liability for violating agreement terms.

6. Conclusion

It appears that the trend is towards protecting privacy. Notice and consent may rule the day. To get ahead of the curve, it would be good practice to incorporate notice and consent in your procedures.