

Privacy and the research industry in the US

The rising concern over unsolicited telephone calls, the acquisition, use and dissemination of personal data, Internet privacy and numerous other privacy issues have created tremendous friction between the researcher's need for information and the privacy concerns of respondents. In the US privacy is now front-page news and is a major focus of legislative activity at the state and federal level. The following is a brief look at these issues and of the current privacy atmosphere surrounding research.

Telephone privacy

Since 1999 there has been a record number of bills aimed at regulating the use of the telephone and the collection and use of personal information. For the most part, these measures concern the activities of telemarketers and distinguish sales-related calls from calls for research purposes. However, other issues such as monitoring telephone calls go beyond the telemarketing industry and impact all uses of the telephone, including research.

Do-not-call legislation

Unwanted telephone calls are among the paramount privacy concerns of the public. In reaction to these concerns, a category of legislation was developed referred to as “do-not-call” bills. Designed to allow individuals to request that they not receive certain sales calls, these laws require telemarketers to comply with the do-not-call requests and abide by any state-compiled do-not-call registries.

This issue of unwanted telephone calls became so widespread that in 1991 Congress passed the Telephone Consumer Protection Act (47 U.S.C. 227), which requires telemarketers to comply with individuals’ do-not-call requests. In addition, it requires such requests to be honored for 10 years from the time the request is made. Many states have similarly legislated the telemarketing industry, imposing compliance with do-not-call requests and, in some cases, establishing statewide databases of individuals who do not wish to be called. When legislators attempt to impose this requirement on telemarketers, the language used sometimes implicates research. Examples include legislation introduced in some states that would require compliance with do-not-call requests for calls that “seek marketing information for any purpose.” Although not the intent, the effect of legislation such as this is to regulate the research industry. With the increase in the number of do-not-call bills being introduced across the country, the number of bills such as these that pose a threat to the research industry has and will continue to increase.



Diane Bowers,
Executive Director, Council of American Survey Research Organizations; President, Council for Marketing and Opinion Research

Electronic monitoring

Legislative activity surrounding the issue of electronic monitoring has alternated the years between a frenzy of bills and dormancy. For example, although a federal two-party consent bill had been introduced in 1998, it was successfully amended and was never enacted into law. However, beginning in 1999, the atmosphere changed. Due in part to the presidential scandal and its inclusion of secretly taped telephone conversations, electronic monitoring was pushed to the forefront of legislative activity. Constituents and in turn lawmakers became concerned about the secret monitoring of telephone calls and more than four dozen bills were introduced nationwide in 1999 and 2000 on this subject. Moreover, state and federal legislation addressing employer monitoring of employees also intensified. While no legislation restricting research activities was passed into law, clearly the privacy concerns of the public are being amplified in the legislative arena.

Data privacy

The EU Directive on Data Privacy has had a significant impact on the US. Most importantly for the US, the Directive states that EU countries may not transfer personal data to countries that do not have ‘adequate’ privacy protection.

Since the US does not have strict data privacy laws addressing all of the enumerated principles in the EU Directive, but instead relies primarily on self-regulation, the US is deemed to be a country without “adequate privacy protection.” In addition to ongoing privacy hearings and workshops by various government agencies, the US Department of Commerce started working with the EU to develop ‘safe harbors’. The ‘safe harbors’ are a set of common principles to provide the specified standard of “adequate privacy protection” for the transfer of information from participating countries to the United States. On July 27, 2000, the European Commission ruled that the Safe Harbor Privacy Principles submitted by the US provided adequate protection.

According to the Department of Commerce, “the safe harbor eliminates the need for prior approval to begin data transfers.” Organizations that decide to participate in the Safe Harbor Program, which is entirely voluntary, must comply with the Safe Harbor requirements and must publicly declare their adherence. To do so, an organization self-certifies annually to the Department of Commerce in writing that it agrees to adhere to the Safe Harbor Program’s requirements. The organization must also state in its published privacy policy statement that it adheres to the Safe Harbor Program. The Department of Commerce, in turn, maintains a list of

all organizations that file self-certification letters and makes both the list and self-certification letters publicly available.

To qualify for the Safe Harbor Program, an organization can:

1. join a self-regulatory program that adheres to the Safe Harbor's requirements and certify to the Department of commerce;
2. develop its own self-regulatory privacy policy that conforms to the Safe Harbor and certify to the Department of Commerce; OR
3. be subject to the statutory, regulatory, administrative or other body or law that effectively protects personal privacy.

The Safe Harbor Program consists of seven principles:

1. **Notice** – about what is collected, how it is collected, its purpose and disclosure to third parties as well as choices and means the organization offers for limiting its use and disclosure
2. **Choice** – (opt-out) allows individuals to choose not to have their information used or disclosed to a third party or to be used for a purpose incompatible with the purpose for which it was originally collected
3. **Onward Transfer** – transfer only to third parties who also comply with the Safe Harbor principles.
4. **Access** – provide individuals with access to their personal information and allow them to correct, amend, or delete that information where it is inaccurate (except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual would be violated).
5. **Security** – reasonable precautions must be taken to protect information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
6. **Data Integrity** – use data consistent with the purpose disclosed to the individual.
7. **Enforcement** – must have mechanisms for assuring compliance. Specifically, there must be:
 - a) readily available and affordable independent mechanisms for the hearing of complaints by individuals and awarding of damages where law or private sector initiatives provide them
 - b) procedures for verifying that the commitments companies make to adhere to the Safe Harbor Principles have been implemented and
 - c) obligations to remedy problems arising out of a failure to comply with the principles.

In addition, sanctions must be sufficiently vigorous to ensure compliance.



Internet privacy

Another highly publicized aspect of data privacy is the collection and use of personal information over the Internet. Recent media attention has focused the nation and its lawmakers attention on internet privacy issues.

As a result, in 1999 and 2000 there has been a growing amount of legislative activity surrounding this issue. While some states have introduced legislation to create special task forces to further investigate the various privacy issues and concerns surrounding the Internet, other lawmakers have acted more directly on the issue by, for example, introducing legislation to prohibit email or Internet service providers from disclosing the personally-identifiable information of their subscribers (including email addresses) without notice and consent.

After ESOMAR's first guideline on Internet Research in 1998, CASRO has now passed Internet standards, and we hope to harmonise requirements in the future. CASRO's standards require research companies to verify that individuals contacted for research by email have a reasonable expectation that they will receive email contact for research. Such agreement can be assumed when ALL of the following conditions exist:

- A substantive pre-existing relationship exists between the individuals contacted and the research organization, the client or the list owners contracting the research (the latter being so identified);
- Individuals have a reasonable expectation, based on the pre-existing relationship, that they may be contacted for research;
- Individuals are offered the choice to be removed from future email contact in each invitation; and,
- The invitation list excludes all individuals who have previously taken the appropriate and timely steps to request the list owner to remove them.

The ESOMAR Professional Standards, of which I am a member, will discuss how we can move to harmonise our guidelines further. Both the federal government and state lawmakers are reacting to the intense media attention and public outcry regarding online privacy issues. The result is the introduction, and in some cases, the enactment of all-encompassing online privacy measures that will implicate the research industry.

The privacy concerns of respondents in turn become the privacy concerns of lawmakers. To continue its vitality, the research industry must stay receptive to the privacy concerns of our respondents and be aware of the resulting state and federal legislative activities. ■