

## **Individual Privacy: How Laws Impact Researchers, Whether the Laws Apply Or Not** **Howard Fienberg**

Director of Government Affairs, CMOR: Promoting and Advocating Survey Research

[hfienberg@cmor.org](mailto:hfienberg@cmor.org)

1111 16<sup>th</sup> St. NW, Suite 120

Washington, DC 20036

### **Introduction**

The research profession must take privacy more seriously than most any other, because if researchers do not maintain the privacy of respondents and participants' personally identifiable information, else they will forfeit the opportunity to collect it. It has unfortunately become routine for participants to receive notification from companies, institutions, and government agencies, letting them know that their personal data may have been compromised. A top priority for the research profession must be ensuring that such notices never have to be sent by a research organization.

Unfortunately, Americans are learning not to trust anyone with their personally identifiable information (PII). They are more aware about identity theft, and the prevalence of attempted identity theft, then ever before. Respondent paranoia is an important element of the privacy atmosphere -- and makes the job of an opinion researcher even harder.

According to the CMOR 2006 Research Profession Image Study, 8 in 10 respondents are concerned about their privacy. Even more worrisome, since 2001, only between 25 and 30% of respondents have felt that survey organizations can be trusted to protect their 'rights to privacy.' Finally, around one-quarter of respondents feel that survey and opinion research constitutes an invasion of privacy – concerns that have remained stable since 1990.

This paper will provide an overview of privacy issues for the survey and opinion research profession, and explain how privacy laws – even laws that do not apply to researchers – impact research work.

### **Telephone Privacy: TCPA**

The 1991 Telephone Consumer Protection Act (TCPA) (47 U.S.C. 227) directed the Federal Communications Commission to balance the fair practices of telemarketers with consumer privacy concerns. Some TCPA provisions apply only to commercial and sales-related communications, such as the fax, call abandonment and time of day restrictions, but still impact researchers. However, some of the TCPA restrictions on artificial or prerecorded messages, and the restrictions on calling cell phones, apply to all callers, including researchers.

### **Faxes**

The TCPA aimed to reduce the amount of unsolicited facsimile advertisements sent to businesses and residences. The TCPA requires that any telephone facsimile (fax) machine "clearly marks, in a margin at the top or bottom of each transmitted page or on the first page of each transmission, the date and time sent, an identification of the business, other entity, or individual sending the message, and the telephone number of the sending machine or of such business, other entity, or individual." The TCPA also prohibits any person from sending an "unsolicited advertisement to a telephone facsimile machine."

A later amendment of the law, the Junk Fax Prevention Act (JFPA), requires senders of permissible fax advertisements (those sent under an established business relationship or with the recipient's prior express permission) to provide specified notice and contact information on the fax that allow recipients to "opt-out" of future faxes from the sender. Junk fax senders that receive a request not to send further faxes must honor that request within the shortest reasonable time from the date of such request, not to exceed 30 days. They are also prohibited from sending future fax advertisements to the consumer unless the consumer subsequently provides prior express permission to the sender.

While legitimate survey research is outside the scope of these restrictions, CMOR recommends that all researchers adopt fax policies addressing respondent opt-out requests in order to promote respondent cooperation.

### **Call Abandonment**

The TCPA also prohibits telemarketers from abandoning more than three percent of all telemarketing calls that are answered live by a person. A call is considered abandoned if it is not connected to a live sales representative within two seconds of the called person's completed greeting. While these restrictions apply only to telemarketing calls, professional associations like CMOR recommend that researchers strictly limit their call abandonment rates.

### **Time of Day**

The TCPA restricts the time of day for sales and fund-raising calls to between 8am and 9pm (local time for the called consumer). While researchers are exempt from such restrictions, professional associations generally recommend abiding by these restrictions as a best practice.

### **Artificial or Prerecorded Messages**

The TCPA prohibits telemarketing calls to any residential phone using an "artificial or prerecorded voice to deliver a message without the prior express consent of the called party."

While that does not apply to survey researchers, the TCPA requires all artificial or prerecorded messages to disclose (at the beginning of the call) the identity of the business, individual, or other entity initiating the call, and if a business is responsible for initiating the call, the name under which the entity is registered to conduct business with the State Corporation Commission (or comparable regulatory authority) must be stated.

During or after the message, messages must also state clearly the telephone number (other than that of the autodialer or prerecorded message player which placed the call) or address of such business, other entity, or individual. Furthermore, the telephone number provided during the disclosure may not be a 900 number or any other number for which charges exceed local or long distance transmission charges.

### **Calling Cell Phones**

Automatic telephone dialing systems, according to the TCPA, cannot be used to contact a cell phone without the user's "prior express consent" -- a content-neutral requirement that applies to all calls, including survey and opinion research calls. The TCPA defines "automatic telephone dialing system" as equipment that has the capacity to store or produce telephone numbers to be called using a random or sequential number generator, in conjunction with dialing such numbers. As clarified by the FCC's 2003 Report, this includes all forms of auto-dialers and predictive dialers, and applies to intra-state calls, interstate calls and calls from outside the United States. Furthermore, the TCPA definition of "call" includes text messages sent to cell phones. There is also no good faith exception for inadvertent or accidental calls to cell phones.

While telephone sample providers have been made aware of this law, and NeuStar provides a useful service for recognizing wireless numbers that have been "ported" from residential lines, their methods may not be a perfect solution to the problem. CMOR is working in Washington, DC to amend the TCPA to exempt research calls. In the meantime, to ensure full compliance with this federal law, in the absence of express prior consent, CMOR recommends that researchers manually dial cell phone numbers (where a human being physically touches the buttons on the phone to dial the number).

### **The Telemarketing Sales Rule (TSR)**

The 1994 Telemarketing Sales Rule (TSR) (16 C.F.R. 310) prohibits certain deceptive telemarketing activities, and regulates sales and fund-raising calls to consumers, as well as consumer calls in response to solicitation by mail.

The TSR also prohibits deceptive activities commonly known as *sugging* and *frugging*. *Sugging* is the practice of selling under the guise of research and *frugging* is fund-raising under the guise of research. Selling, in any form, is differentiated from regular consumer contact, like survey research. Occasionally,

survey research companies will offer an incentive/gift to the respondent in appreciation of his or her cooperation. Such an incentive/gift could be a cash donation to a charity, a product sample, or a nominal monetary award. But, sales or solicitation is not acceptable or permitted in legitimate and professionally-conducted survey and opinion research and potentially violates federal law.

To enforce the law, the TSR allows consumers to bring private civil lawsuits in federal district courts.

#### **The Do Not Call registry (DNC)**

While the TCPA first required that companies maintain their own internal do not call registries, starting in 2005, Congress amended the TCPA and the TSR to create a federal DNC registry operated by the Federal Trade Commission (FTC) in conjunction with the FCC. Telemarketers and sellers are required to search the registry at least once every 31 days and drop from their call lists the phone numbers of consumers who have registered.

Calls placed to registered lines are allowed with prior written consent, or under similar established business relationship rules as the in the TCPA's fax restrictions.

The DNC Registry does not apply to survey research calls, but, a researcher that accesses the DNC Registry, for whatever reason, becomes legally bound by it – i.e. responsible for scrubbing their calling lists for registrants, just like a telemarketer.

#### **Children's Online Privacy Protection Act (COPPA)**

The federal COPPA, signed into law in 2000 (16 CFR Part 312), applies to the online collection of personal information from children under the age of 13. The primary goal is to place parents in control over what information is collected from their children online. The rules spell out what a web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children's privacy and safety online. The rules cannot be sidestepped by simply including a disclaimer, making the collection of PII optional, or surreptitiously inviting children to falsify their age.

COPPA applies to operators of commercial websites or online services directed to children under 13 that collect PII from children, operators of general audience sites that knowingly collect personal information from children under 13, and operators of general audience sites that have a separate children's area and that collect personal information from children under 13.

The FTC applies a sliding scale approach to the practice of collecting PII from children. It balances the level of information sought from a child and the level of information needed from the child's parent to verify parental consent. Information that the website operator will keep for internal purposes requires simpler consent methods than information that might be externally shared with the public or a third party.

Although COPPA applies only to children under 13, CMOR recommends researchers seek parental consent for contact with any respondents under the age of 18.

#### **Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)**

The federal CAN-SPAM Act, signed into law in 2003 (16 CFR Part 316), established commercial e-mail distribution requirements, penalties for violation of the law, and consumers' rights to opt out of future e-mailings.

The law bans false or misleading header information, meaning that e-mails must contain accurate "From" and "To" fields and routing information including the originating domain name and email address. It also prohibits deceptive subject lines. Commercial email must be identified as an advertisement or solicitation and include the sender's valid physical postal address, as well as explicitly state that the recipient can opt-out of future emails.

The law not only requires that e-mails include a method for recipients to opt out, but that senders strictly honor such requests within ten days, and for at least 30 days after sending the commercial email. In addition, CAN-SPAM prohibits the sale or transfer of the opt-ed out email address.

The CAN-SPAM Act applies to those that distribute commercial e-mail messages. However, survey research emails **may** be covered under the false or materially misleading header provision – usually a non-issue, given the typically ethical nature of research contacts. Of course, researchers using email to **solicit** business or **sell** goods or services are bound by the law. Survey researchers that are recruiting or inviting respondents to participate in a survey are not legally required to abide by the opt out provisions or email identification provisions of the Act because recruiting and taking surveys is not a commercial or sales-related activity.

However, as a best practice, researchers are encouraged by CMOR and other professional associations to include opt out notices in all email distributions, regardless of whether the message is commercial or non-commercial in nature. This becomes especially important in certain states, since several state spam laws regulate bulk emails, regardless of content.

### **The Gramm-Leach-Bliley Act (GLB)**

The GLB, signed into law in 1999 (15 U.S.C. § 6801-6809), includes provisions regulating the privacy and security of consumer financial information, which are overseen by the FTC and a variety of financial regulatory agencies.

The law restricts the disclosure of consumers’ “nonpublic personal information” by “financial institutions,” and requires explicit notices to customers about information-collection and sharing practices. The GLB Act allows for consumers to opt out of having their information shared with third parties, and all financial institutions are required to provide notice and opt out opportunity before they may disclose information to non-affiliated third parties (with certain caveats).

The FTC defines the term “financial institution” as any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution. An institution must be “significantly engaged” in financial activities to be considered a “financial institution.”

So, in order for researchers to acquire customers’ PII from financial institutions under the GLB’s “Privacy Rule”, the institutions must either: (1) provide customers notice of such disclosure and their ability to opt out of it; or (2) utilize an exception in the law. Under this exception, the financial institution is still required to provide notice to its customers about its information sharing practices, but PII can be disseminated without the opt out provision to third parties who provide services for the financial institution – like survey researchers conducting research for the financial institution. To take advantage of this exception, survey researchers would have to enter into a contractual agreement with the financial institution to keep the PII confidential.

Additionally, though the onus is generally on the financial institution itself and not the contracted or third party researcher, the GLB’s “Safeguards Rule”, which requires significant controls on how a company or organization handles and protects PII in the physical and virtual worlds.

### **Protected health information**

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (42 USC § 201 et seq.) was enacted by Congress to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage and to simplify the administration of health insurance. The important aspect of the law for survey and opinion researchers is the HIPAA Privacy Rule, which requires health care providers to limit disclosure of individually identifiable health information (also known as protected health information, or PHI) without the patient’s authorization. The Privacy Rule also protects PHI when it is used, created or maintained for a

provider by a “business associate.” Business associates perform functions or services for the covered entity that involve the use of protected health information. They may include survey and opinion researchers.

Survey researchers receiving PHI from healthcare providers or collecting, using or maintaining PHI on behalf of providers are required to comply with the HIPAA Privacy Rule. Failure to comply may result in civil and criminal penalties.

While the HIPAA Privacy Rule only applies in these kinds of circumstances to survey and opinion researchers, researchers should be aware of the law because legislators and others are considering extending the HIPAA requirements to all entities that collect and handle PHI.

#### **FTC restrictions on deceptive practices**

The FTC regulates survey and opinion researchers in another very broad way -- breaking your promises can mean breaking the law. Violating your stated privacy policy can be actionable under Section 5 of the FTC Act as an unfair or deceptive trade practice, as well as under similar laws at the state level.

#### **The bad actors make all the actors look bad**

Privacy is the cornerstone of the survey and opinion research profession. While respondents will always have to buy goods or services in some fashion, few respondents recognize any inherent need to respond to surveys (or value in responding to them) – not even the decennial Census. If the profession violates respondent privacy, or is perceived to have done so, respondents will stop cooperating with research efforts.

Moreover, every new data security breach makes respondents more wary of research participation – even though research firms and organizations are not the culprits. The Privacy Rights Clearinghouse has calculated that more than 154 million private data records have been breached since 2005. Research respondents are aware of these breaches and, as demonstrated earlier in this paper by the results from the CMOR 2006 Research Profession Image Study, take them very seriously.

Therefore, every contact with respondents becomes a vital opportunity to reinforce the confidential nature of the research process. Also, because of the detrimental impact of bad actors, the strict enforcement of professional codes and standards (like those of the American Association of Public Opinion Researchers or the Marketing Research Association) and the full involvement of the survey and opinion research profession in shaming and prosecuting unethical and illegal practices within the profession and beyond, are key components of continued respondent cooperation. Researchers also must do their part by maintaining and following a privacy policy and always treating respondents and their information with care and respect.

#### **About the author**

Howard Fienberg is Director of Government Affairs for CMOR. CMOR is a non-profit organization which works on behalf of the survey and opinion research profession to improve respondent cooperation and to promote positive legislation and prevent restrictive legislation which could impact the research profession.