Privacy Rights Clearinghouse
3100 – 5th Ave., Suite B
San Diego, CA 92103
Voice: (619) 298-3396
Fax: (619) 298-5681
Web: www.privacyrights.org

Comments Submitted to the Federal Trade Commission
for Consideration in the Third Privacy Roundtable (March 17, 2010)

by the Privacy Rights Clearinghouse
Beth Givens, Director
March 5, 2010

Privacy Roundtables
Comment, Project No. P095416

Scope

The Privacy Rights Clearinghouse (PRC) respectfully submits the following comments to the Federal Trade Commission for its consideration in the third Privacy Roundtable, to be held March 17, 2010.

Our comments are most relevant to the third question, as posted on the FTC's Privacy Roundtable web page, http://www.ftc.gov/bcp/workshops/privacyroundtables/#comment .

3. How do we determine what information is sensitive?
   What standards should apply to the collection and uses of such information?

Background

The Privacy Rights Clearinghouse is a nonprofit consumer organization, established in 1992 and located in San Diego, California. It has a two-part mission: consumer education and consumer advocacy. The PRC has published more than 50 guides, called "Fact Sheets." These provide a wealth of practical information on strategies that consumers can employ to safeguard their personal information. http://www.privacyrights.org/Privacy-Rights-Fact-Sheets

Topics include: identity theft, credit reporting, employment background checks, online privacy and safety, telemarketing, direct marketing, financial privacy, children's safety and privacy on the Internet, wireless communications, and more.

The PRC invites individuals to contact the organization with their questions and complaints. Over the course of our 18-year history, PRC staff members have communicated with tens of thousands of consumers who have contacted us by phone, e-mail, and our website's inquiry form. The comments in this document about sensitive information reflect, in large part, our observations gathered from direct contact with individuals over the years.

Consumers' Perception of "Sensitive" Personal Information

In addressing the FTC's question regarding what information is considered sensitive, we draw primarily from the PRC's records of consumer complaints. Two general observations are:

- The type of information consumers consider to be sensitive varies widely.
- Even directory information – names, addresses, and phone numbers – is considered to be extremely sensitive to a significant number of individuals.

We present the following "cases" from our own files and from news stories to illustrate our observation that, depending on the individual's situation, any personal information could be considered sensitive.

1. Several years ago, a cable television company in a large metropolitan area that offered phone service in addition to television service erroneously exposed the names and addresses of its unpublished customers. The cable company provided a database of its customers to the local phone company so that a merged phone directory could be printed. But the cable company failed to delete the records for those customers who had chosen to be unpublished, thus exposing their names, addresses and phone numbers.

   Many of those customers had opted for unpublished listings because of personal safety issues. They included police officers, judges, court employees, parole officers, probation officers, school teachers, and mental health workers – individuals who, for a variety of reasons, did not want their addresses and phone numbers available to those who might try to harm them and their families. The company contacted the Privacy Rights Clearinghouse which assisted in crafting a mitigation strategy for the affected individuals.

   The cable company provided financial assistance to many individuals and families affected by the database error – by installing security systems in some homes, by moving others to new apartment units, and by helping others find and purchase new homes. It was an expensive endeavor, not to mention a public relations disaster for the cable company.

   What this situation revealed was the sensitivity of directory information – simply names, addresses, and phone numbers -- to a significant number of individuals.

2. The PRC was contacted by an environmental activist who lived in a large metropolitan area. He was concerned that his address could be obtained from county property tax records that the county had recently posted on its website. His activism was controversial and he had personal safety concerns for himself and his family.

3. We have learned that for victims of domestic violence and stalking, all personal information is sensitive. If a victim's personal information is compromised, such as address and phone number, the result could be significant personal harm to the victim and the family. Such individuals go to great lengths to keep their personally identifiable

information (PII) confidential. At least 31 states offer address confidentiality services such as California's Safe at Home, administered by the Secretary of State. http://www.ncvc.org/src/main.aspx?dbID=DB_AddressConfidentialityPrograms160 .

4. As personal information becomes increasingly available via the Internet, more people are viewing any info about them as sensitive because it can be linked so easily with data from many sources. When such personal information is combined, the profile could well be sensitive, even though the individual data elements are not sensitive.

   This is particularly apparent with the growth of the online information broker industry. The PRC receives complaints and questions from individuals about online information brokers on a daily basis. These companies create and sell profiles of individuals based on information found in public records, semi-public records and online searches. Information for purchase on a consumer can include a wide range of data elements such as name, address(es), social media profiles, "social net handle" (user name), telephone number, age, known relatives, average income, a map to one's house and often much more.

   Consumers who do not want their information listed rely on companies to voluntarily adopt a method of opting-out, since no laws exist that would mandate the right to opt-out. While some companies provide an opt-out option for individuals, many do not. We re aware of two companies that charge a fee for individuals to opt-out: USSearch and Zabasearch.

   To view the PRC's list of online information brokers, visit: http://www.privacyrights.org/ar/infobrokers.htm

5. Even information that has supposedly been anonymized can be considered to be sensitive.

   5a. In 2006 America Online (AOL) posted 20 million search queries of 658,000 of its subscribers to a website. Before releasing the data, AOL had tried to anonymize it by removing PII. However, in order to maintain the usefulness of the data to researchers, it provided unique identification numbers which allowed correlation of searches to individual users. Despite removing identifiable information from the data, researchers were able to identify specific individuals' searches. http://technology.findlaw.com/articles/00006/010208.html

   5b. In the same year, Netflix publicly released 100 million records revealing how nearly 500,000 of its users had rated movies. Each record disclosed the movie, the numerical rating, and the date. Netflix anonymized the records, removing PII and assigning a unique identifier to preserve continuity. By combining movie recommendations found on the Internet Movie Database with the Netflix data, researchers found that individuals could be reidentified from the Netflix data. The Netflix case illustrates the principle that while data itself may seem anonymous, it can be when paired with other existing data to create opportunities for

reidentification. In *Doe v. Netflix*, a lesbian mother filed a lawsuit against Netflix alleging that the information they released was insufficiently anonymized and therefore "outed" her. http://www.wired.com/threatlevel/2009/12/netflix-privacy-lawsuit/

5c. The Massachusetts Group Insurance Commission (GIC) purchased health insurance for state employees. In the mid-1990s, it released "anonymized" data showing the hospital visits of state employees to researchers requesting the information. By removing PII, GIC assumed that it had preserved patient privacy. Dr. Latanya Sweeney, a professor of computer science at Carnegie Mellon University and director of its Laboratory for International Data Privacy, requested a copy of the data. Using available information, Dr. Sweeney was able to identify and obtain the personal medical records of then-Massachusetts Governor Weld, among others. In 2000, Dr. Sweeney showed that 87% of Americans could be uniquely identified by knowing just three data elements: ZIP code, date of birth, and sex. http://portal.acm.org/citation.cfm?id=1179615

6. In today's environment of massive data collection and increasingly targeted marketing, databases abound which aggregate information about consumers – from political affiliations to medical diagnoses to shopping habits. Some of the most serious privacy violations occur when these databases are combined. In such instances, each piece of otherwise inconsequential data adds another layer to a detailed portrait of an individual consumer. This provides an exceptional opportunity for market researchers and other users to delve into the personal habits and demographics of consumers. It also results in a significant level of privacy invasion.

   Much public attention has already been drawn to the privacy concerns of combining different databases. Facebook's Beacon program combined social networking profiles with online purchases at seemingly unaffiliated websites. Google Buzz culled data from personal email communications to create public user profiles on a new social network. In each of these instances, consumers had initially exercised choice: they willingly provided their personal information to these companies. The privacy violations occurred when the companies used the data in a way the consumer did not expect, namely by combining it with other sets of data.

   The public outcry over these incidents points to a larger issue in protecting privacy. Consumer data must be safeguarded from uses not specifically explained when the data is originally collected. Even non-sensitive data becomes personal, sensitive and frequently identifiable when combined with other sets of data not considered sensitive. In the final section of this document, we discuss how the Principles of Fair Information Practices can be used to develop a more level playing field for individuals.

Concluding Thoughts about Sensitive Personal Information

We close this section by providing the following quote, which succinctly describes many of the points we have raised in our comments:

> *The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.*

The reader might think this statement is relatively contemporary, given that it so aptly describes behavioral advertisers culling information from unknowing consumers, online information brokers combining and selling records on individuals, and data aggregators compiling data from a variety of sources for targeted direct marketing. But this quote was published more than 30 years ago, as part of a wide-ranging report by the Privacy Protection Study Commission, *Personal Privacy in an Information Society* (p. 533, 1977).
http://epic.org/privacy/ppsc1977report/

Principles of Fair Information Practices

The final question that we address is: What standards should apply to the collection and uses of such information?

The PRC is a strong proponent of the Principles of Fair Information Practices (FIPs). These provide a framework to protect PII, not just sensitive information, but all information that can be associated with individuals.

Several versions of the Fair Information Principles exist. At the level of least protection are the principles of Notice and Choice. In today's complex digital environment, these are not even minimally effective in giving individuals the tools to control what is done with their personal information.

In recent years, the Federal Trade Commission has promoted a five-part set of Fair Information Principles to guide the use of personal information. These are: Notice, Choice, Access, Security, and Enforcement. A description of these principles is provided on the FTC website:
http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Unfortunately, these FIPs do not include principles that prevent the collection of more information than is necessary for the task at hand, and, further, that limit the uses of such information.

We believe that the eight principles developed in 1980 by the Paris-based international body, the Organization for Economic Cooperation and Development (OECD), provide a significantly stronger framework for privacy protection. These principles are:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness

- Individual participation
- Accountability

To read the full text of these principles, visit:
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[From "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Organisation for Economic Cooperation and Development, 1980.]

The Canadian federal government has gone further than the OECD's guidelines by implementing a 10-point set of Fair Information Practices in its national privacy law, the Personal Information Protection and Electronic Documents Act. PIPEDA came into effect in 2001, with health provisions implemented in 2002, and commercial activities covered as of January 2004. For more information, visit the website of the Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/legislation/02_06_01_e.cfm .]

The 10 principles that form the framework for PIPEDA are:

- Accountability
- Identifying purpose
- Consent
- Limiting collection
- Limiting use, disclosure, and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance

For an overview of FIPs, read our analysis, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." http://www.privacyrights.org/ar/fairinfo.htm

In summary, we believe that a robust set of Fair Information Principles, such as the OECD Guidelines and the principles that form the basis of the Canadian law PIPEDA, will provide a strong framework for standards that should apply to the collection and uses of, not only sensitive personal information, but all personally identifiable information.

Thank you for the opportunity to submit these comments for the Federal Trade Commission's third privacy roundtable.