A Methodology to Assess the Implementation of the Elements of Effective Self-Regulation for Protection of Privacy

Discussion Draft - 6/17/98
Prepared for the National Telecommunications Information Agency
U.S. Department of Commerce

By

Dr. Mary J. Culnan
School of Business
Georgetown University
Washington, D.C. 20057-1008
culnanm@gunet.georgetown.edu
http://www.georgetown.edu/culnan

The author acknowledges the helpful comments of Robert Gellman, Priscilla Regan and Joel Reidenberg on an earlier version of this paper.

A Methodology to Assess the Implementation of the Elements of Effective Self-Regulation for Protection of Privacy

Introduction

On July 1, 1998, The Department of Commerce is scheduled to report to the President on industry efforts to establish self-regulatory regimes to ensure privacy online. Given that much is riding on this assessment, it is important, then, that the conclusions about current practices presented in the Department of Commerce report be viewed as accurate, fairly and objectively determined, and accepted by both the business and public interest communities.

The purpose of this document is to define a methodology to help assess the implementation of self-regulation. Here, self-regulation is defined by the *Elements of Effective Self-Regulation for Protection of Privacy*. This paper translates the principles in the *Elements* paper into a tool that can be used to collect some of the data for the Department of Commerce July 1 report on self-regulation. The methodology can also be used by other organizations to perform their own independent assessments.

It is envisioned that the methodology will be used to assess if a gap exists between "what should be" as defined by the *Elements* paper, and "what is" as represented by the privacy disclosures displayed on web sites. In addition to identifying what constitutes self-regulation (i.e. "what should be"), the steps needed to perform such an assessment include (1) analyzing the content of privacy notices to measure the current state of self-regulation (i.e. "what is"), (2) determining if gaps exists between "what is" and "what should be," and (3) documenting any gaps that are identified. It is critical to note that the methodology is only a tool for gathering data. **The methodology does not define what results would lead the Department of Commerce to conclude that self-regulation is or is not working**. The data resulting from using the methodology, then, can provide one input for the decision processes of the Department of Commerce. It is also important to note that the methodology cannot assess implementation of the *Elements* beyond what organizations disclose in their privacy notices. In other words, the methodology can only assess whether an organization "says what it does," and whether these notices meet certain criteria. It cannot be used to determine if an organization "does what it says."

Here, self-regulation is defined by the *Elements of Effective Self-Regulation for Protection of Privacy* published by NTIA in the *Federal Register* on June 5, 1998. Operational definitions will be developed for each element. An operational definition translates a concept into practice by assigning an unambiguous meaning to the concept so that it can be measured in any concrete situation. Operational definitions will be developed for the prescriptions (e.g. "should do X") in each element of self-regulation. If an element does not contain a prescriptive statement, no operational definition will be developed. Current practices can be measured against these operational definitions.

Operationalizing the *Elements* paper serves two useful purposes for the policy process. First, it makes it possible to move beyond anecdotal evidence and perform an objective assessment based on the *Elements* paper. Second, it provides a way to provide feedback about the elements themselves. The methodology represents an effort to faithfully translate but not add to or to extend the elements as written. Where the methodology is viewed as incomplete or ambiguous, it may suggest a need to revisit the *Elements*. The paper notes any such issues that emerged while developing the methodology.

The remainder of this paper will be organized as follows. First, the methodology will be described including operational definitions for each element of self-regulation. Next, issues related to enforcement will be reviewed. Third, the paper will discuss implementation issues including sampling considerations. The paper will conclude with some general comments about building consumer trust online. A checklist summarizing the methodology is contained in the Appendix.

Methodology Overview

The methodology is based on content analysis. Content analysis is a well-established social science research method for studying and analyzing communications in a systematic and objective way. With content analysis, analyzing communication acts as a surrogate for observing behavior directly. Content analysis takes communications such as a published notice or policy that individuals or organizations have produced, and asks questions about them. It is a technique for making inferences by objectively and systematically identifying specific characteristics of communications. Analysis is based on explicit rules that make it possible for different researchers to achieve the same results from analyzing the same communications. Content analysis can be used for many purposes including coding open-ended questions in surveys, identifying cultural patterns or cross-cultural differences in communication or detecting the existence of propaganda. Here, content analysis will be used to audit the content of notices provided on web sites against the requirements contained in the *Elements* paper.

The *Elements* paper identifies two basic elements of a self-regulatory regime: fair information practices and enforcement mechanisms that assure compliance with those practices. The methodology can be used to collect data from notices provided for either or both elements, or for portions of an element: where organizations "say what they do." However, content analysis cannot be used to assess three important aspects of self-regulation. First, it cannot assess compliance: whether an organization's disclosed practices match its actual practices. Second, content analysis cannot assess the effectiveness of various enforcement mechanisms. Third, the methodology cannot assess the effectiveness of a particular notice: whether consumers understand the policy that has been disclosed, or the impact of notice on overall public awareness. Additional research will be needed to assess all three of these issues.

Because the Department of Commerce assessment is focusing on the Internet, the methodology is designed primarily for analyzing the written disclosures such as notices

or policies that organizations have posted on their web sites[1]. The methodology can be applied to online services that are accessed directly without using the Internet. It may also be used to analyze the content of other written documents including privacy policies and notices developed by individual organizations, and industry codes of conduct or other self-regulatory programs designed for a wider audience. The methodology is intended to be unobtrusive and easily replicated by anyone wishing to assess the state of self-regulation based on the notices organizations provide. It can also be used over time to assess trends.

Research on privacy has found that while fair information practices are important and make people more comfortable about disclosing personal information, people's privacy preferences vary. Therefore, the methodology measures whether or not a particular notice is present, but does not address the effectiveness or the format of these notices. Disclosing that an organization observes fair information practices helps build the trust that is central to acquiring and retaining customers[2]. Therefore, where privacy practices exceed minimum standards, these practices can provide a source of differentiation for organizations, providing that an organization's practices are consistent with its disclosed policies. Under self-regulation, an organization should be free to develop notices that have the look and feel of its other marketing communications, and that it believes are appropriate and effective for the target audience[3].

Throughout this paper, the term "consumers" is used to refer to any individual who accesses an Internet web site or an online service. The term "identifiable personal information" is used to refer to any data element that can be used to identify or to link back to an identifiable person. For each element, the text from the *Elements* paper is shown in italics, followed by the criteria for assessing its implementation.

The Methodology

I. Fair Information Practices

A. Awareness. *At a minimum, consumers need to know the identity of the collector of their personal information, the intended uses of the information, and the means by which they may limit its disclosure. Companies collecting and using data are responsible for raising consumer and awareness and can do so through the following avenues:*

(1) Privacy policies. Privacy policies articulate the manner in which a company collects, uses, and protects data, and the choices they offer consumers to exercise

[1] The term "disclosure" can be used to mean notice in the sense that an organization discloses its policies and practices. It can also be used to mean the disclosure of the content of a record as in providing consumers access to their records. To avoid ambiguity, here "notice" is used to refer to all types of written disclosures organizations make about their policies and practices. Thanks to Bob Gellman for this distinction.

[2] See for example Culnan and Armstrong, "Information Privacy Concerns, Procedural Fairness and Impersonal Trust."

[3] Thanks to David Johnson for making the argument that "a thousand flowers" should be allowed to bloom.

rights in their personal information. On the basis of this policy, consumers can determine whether and to what extent they wish to make information available to companies.

(2) Notification: A company's privacy policy should be made known to consumers. Notification should be written in language that is clear and easily understood, should be displayed prominently, and should be made available before consumers are asked to provide personal information to the company.

(3) Consumer education: Companies should teach consumers to ask for relevant knowledge about why information is being collected, what the information will be used for, how it will be protected, the consequences of providing or withholding information, and any recourse they may have. Consumer education enables consumers to make informed decisions about how they allow their personal data to be used as they participate in the information economy. Consumer education may be carried out by individual companies, trade associations, or industry public service campaigns.

- 1. The identity of the organization that is collecting personal information shall be clearly identified. This is particularly important for web sites where the URL or the name of the site is not the same as the name of an organization. For example, the computers.com web site is run by CNet; CNet is clearly identified on the home page of the computers.com web site.

- 2. The organization's privacy notice shall be accessible from the home page of the web site through a direct link.[4] A home page is defined as the URL that corresponds to the DNS address for a web site.

- 3. At a minimum, the notice shall disclose (1) the intended uses of identifiable personal information and (2) the means by which the consumer may limit its disclosure. The notice should be made available before consumers are asked to relinquish information to the company. For example, because consumers do not always enter a web site at the home page, there should also be a link to the notice on all web pages where consumers provide personal information. Notice shall apply to a) email addresses, b) personal information provided through site registration, c) transaction information and d) cookies or other technological means of collecting personal information.

- 4. Organizations should engage in consumer education. Consumer education may take a variety of forms on the web including: a) an email address and a toll-free number combined with an invitation to ask questions, b) Frequently Asked Questions (FAQ's), c) explanations that expand on part of the site's privacy policy or notice such as explanations about the functioning of secure transactions or cookies, d) links to additional material, or e) links to other sites that provide

[4] Obviously, an organization could choose to display its privacy notice on the home page instead of providing a link.

educational material including trade associations or seal programs to which the organization belongs.

Comment:

A major shortcoming of the *Elements* is that only collectors of personally identifiable information are explicitly required to provide notice. Transparency or notice is the most basic principle of fair information practices. Absent notice, there is no basis to know whether or not the organization collects identifiable personal information. The *Awareness Element* should be modified to state that all organizations, including those that do not collect identifiable personal information, should provide notice describing their policies.

The *Awareness Element* does not require that an organization provide notice about the types of identifiable personal information that the web site collects. Since personal information can be gathered unobtrusively, e.g. by tracking how an individual moves through the web site, this is an important omission. The *Awareness Element* needs to be modified to also require notice about what identifiable personal information is collected.

B. Choice. *Consumers should be given the opportunity to exercise choice with respect to whether and how their personal information is used, either by businesses with whom they have direct contact or by third parties. Consumers should be provided with simple, readily visible, available and affordable mechanisms -- whether through technological means or otherwise -- to exercise this option. For certain kinds of information, e.g. medical information or information related to children, affirmative choice by consumers may be appropriate. In these cases, companies should not use personal information unless its use is explicitly consented to by the individual or, in the case of children, his or her parent or guardian.*

- 1. The web site should describe the method by which the consumer may specify a) whether their personal information may be used by this organization, b) how their information may be subsequently used by this organization including whether or not they wish to be contacted, and/or c) whether personal information may be shared with third parties. The mechanism must be simple, available and affordable meaning individuals should be able to register their objection online (1) via the web site by checking a box or filling in a form, (2) by email, or (3) by technological means such as P3P. In addition, organizations may also choose to allow individuals to register their objections by (1) calling a toll-free number that is displayed on the web site and/or by (2) faxing or mailing a letter to a number/ address that is displayed on the web site.

- 2. For web sites that use information from children aged 12 and below, the web site shall obtain the affirmative consent of the child's parent or guardian prior to using any identifiable personal information about that child.

- 3. For medical information, the organization should gain the affirmative consent of the consumer before the information is used. Medical information includes information about a person's health, or information that can be used to infer that the consumer may suffer from a particular medical condition and includes 1) drugs and medical devices and 2) conducting searches for information about diseases or other medical conditions.

Comment:

As written, this *Element* could be interpreted as allowing a consumer to object to personal information they provided for a disclosed purpose being used for that purpose. The *Choice Element* needs to be modified to specify that the individual may object to use for purposes that are not compatible with the stated purpose(s) for collecting the identifiable personal information provided under *Awareness* unless such uses are required by law.

For medical information and for information gathered from children, the *Element* states that consent is required before the information is used. The *Choice Element* should be modified to state that consent is required before the information is collected.

C. Data Security. *Companies creating, maintaining, using or disseminating records of identifiable personal information should take reasonable measures to assure its reliability for its intended use and should take reasonable precautions to protect it from loss, misuse, alteration or destruction. Companies should also strive to assure that the level of protection extended by third parties to whom they transfer personal information is at a level comparable to its own.*

- 1. The web site should include a description of the precautions the organization has established to protect and to assure the reliability of identifiable personal information and to protect the information from loss, misuse, alteration or destruction 1) during transmission, 2) while stored by the organization and 3) when transferred to third parties.

Comment:

The notice should be at a level of detail that is adequate to create consumer confidence but not so detailed as to create an exposure for the firm. See for example: http://www.landsend.com.[5]

[5] Lands End stated that the number of questions concerning credit card security declined after they explained security and privacy issues "up front" on their web site. See: Sharon Machlis, "More Put Credit Cards Online: Comfort Zone for Web Buying Expands," *Computerworld*, March 16, 1998, p. 6.

D. Data Integrity. *Companies should keep only personal data relevant for the purposes for which it has been gathered, consistent with the principles of awareness and choice. To the extent necessary for those purposes, the data should be accurate, complete and current.*

- 1. Organizations should provide notice about the procedures they employ to ensure that data are relevant, accurate, complete and current.

Comment:

As reflected by this *Element*, the disclosures for awareness and choice should encompass some aspects of data integrity. Some aspects of data integrity also appear to be implied by data security as defined above. Further, consumers also play a role in insuring accuracy through an organization's access procedures.

E. Consumer Access. *Consumers should have the opportunity for reasonable, appropriate access to information about them that a company holds, and be able to correct or amend that information when necessary. The extent of access may vary from industry to industry. Providing access to consumer information can be costly to companies, and thus decisions about the level of appropriate access should take into account the nature of the information collected, the number of locations in which it is stored, the nature of the enterprise, and the ways in which the information is to be used.*

- 1. The web site should describe in its notice how consumers may access the personal information that an organization may hold about them

- 2. The web site should describe the procedures for correcting or amending that information as appropriate.

Comment:

At a minimum, consumers should have the right to see and to correct or amend the information they provided (e.g. name and address) or that is related to the maintenance of their account (e.g. billing records). Where it is not feasible to provide access to all the stored information that is associated with an individual, particularly information acquired from third parties, the consumer should at a minimum be able to learn the kinds of information that are contained in their records. Providing notice to this effect should enhance both transparency and consumer trust. One approach to developing such a notice would be to adopt a format similar to the one used for the data cards provided by list brokers or in mailing list catalogs[6]. These listings identify the fields that may be used to select the records to be included in a mailing list.

[6] See for example the Standard Rate and Data Services (SRDS), *Direct Marketing List Source*, a catalog of mailing lists issued six times per year. See www.srds.com.

In some instances, there will be legitimate exceptions to access, amendment and correction. This needs to be stated in the *Access Element*.

Finally, this *Element* needs to be modified to state that organizations should be responsible for authenticating the identity of any consumer making an access request and ensuring that records are not disclosed to unauthorized individuals[7].

F. Accountability. *Companies should be held accountable for complying with their privacy policies.*

- 1. Organizations should provide notice about the procedures they have implemented to insure their information practices have been implemented as represented: 1) information practices are subject to self-assessment, 2) information practices are subject to an external audit, 3) information practices are subject to an internal audit, 4) membership in a trade association that makes adherence to privacy policies a condition of membership, or 5) participation in a program that independently audits the organization's privacy practices. Organizations that adopt methods (4) or (5) above should provide a link to a description of the policies to which they are subject.

II. Enforcement.

A. Consumer Recourse. *Companies that collect and use personally identifiable information should offer consumer mechanisms by which their complaints can be resolved. Such mechanisms should be readily available and affordable.*

- 1. Organizations should provide mechanisms for consumers to submit complaints and to have their complaints resolved. "Readily available" means the web site should describe the procedures the consumer should follow, and the notice should be easy to locate. "Affordable" means the consumer should not incur significant costs to submit a complaint. For example, consumers should be able to choose from a range of methods such as submitting a complaint electronically, by calling a toll-free number, by fax, or by regular mail.

Comment:

The *Elements* paper implies that consumer complaints can be satisfactorily addressed by the company, but this is not always the case. The *Elements* should be modified to indicate that rights of appeal and additional dispute resolution mechanisms need to be provided in the event that the company is unable to satisfactorily resolve the consumer's complaint.

[7] See for example Robert O'Harrow, "For Sale on the Web: Your Financial Secrets," *The Washington Post, June 11, 1998, p. A1.*

B. Verification. *Verification provides attestation that the assertions businesses make about their privacy practices are true and that privacy practices have been implemented as represented. The nature and extent of verification depends upon the kind of information with which a company deals -- companies using highly sensitive information may be held to a higher standard of verification. Because verification may be costly for business, work needs to be done to arrive at appropriate, cost-effective ways to provide companies with the means to provide verification.*

Comment:

This element does not contain any prescriptive statements (i.e. "should do X"), therefore, no operational definition was developed.

C. Consequences. *For self-regulation to be effective, failure to comply with fair information practices should have consequences. Among these may be cancellation of the right to use a certifying seal or logo, posting the name of the non-complier on a publicly available "bad-actor" list, or disqualification from membership in an industry trade association. Non-compliers could be required to pay the costs of determining their non-compliance. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may be liable for fraud and subject to action by the Federal Trade Commission.*

- 1. Organizations that make compliance with fair information practices a condition of 1) employment, 2) membership or 3) the right to use a "trustmark" or other seal or logo should develop sanctions as part of their compliance procedures. Sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion.

- 2. Organizations that make compliance with fair information practices a condition of 1) employment, 2) membership or 3) the right to use a "trustmark" or other seal or logo should disclose how they assure compliance. For example, trade associations or seal organizations could issue regular reports summarizing for the reporting period, the types of complaints received and how they were resolved. Depending on how frequently such reports are issued, they may help address the requirement in the *Element* for swiftness.

- 3. As part of their compliance procedures, trade associations and other organizations that certify privacy practices through membership or a "trustmark", seal or logo should provide a readily available and affordable method for consumers to report non-compliance such as an ability to send email from the certifying organization's web site.

Concluding Comments on the *Elements* Paper and the Methodology

The *Elements* paper and the methodology do not address the issue of verification satisfactorily, and this is a weakness of both. Colin Bennett identifies three elements that are necessary for implementation of the Canadian Standards Association (CSA) Model Code: "Say what you do, do what you say, and be verified by an independent agency." The "catch 22" of the Department of Commerce *Elements* is that in assessing a current purely self-regulatory regime, there is no place to require third party verification unless the private sector voluntarily steps up to the plate. Absent such independent verification, there is no way to state unequivocally that organizations' practices are consistent with what they disclose. Verification is also critical to bridging the emerging "trust gap" in cyberspace and creating a level of consumer comfort necessary to realize the potential of the Internet for conducting electronic commerce. Clearly this is one area where additional efforts will be required.

In September 1997, the American Institute of Certified Public Accountants (AICPA) announced its CPA WebTrust whereby organizations can be audited to assure that web sites meet certain minimum standards of disclosure, and more important, that their practices meet standards of "transaction integrity and sound business practices." While a number of the elements of fair information practices (e.g. disclosure of collection of identifiable personal information) that are covered under seal programs for privacy are not explicitly addressed by WebTrust, the *WebTrust Principles and Criteria* may represent one approach to operationalizing verification as a component of self-regulation. See http://www.aicpa.org/webtrust/index.htm for additional information about WebTrust.

While not a substitute for systematic independent audits, field research could also be conducted to assess in a limited way if some of an organizations' disclosures match their practices, that is do they "do what they say." For example, it is a simple matter to determine if a firm discloses it does not use cookies when in fact it does, or if a consumer asks not to receive email from the firm and subsequently does. Complaint and redress procedures can be tested by email, telephone or postal mail to see if organizations are responsive. An organization's information access practices can be tested in the same way. However, it is difficult to conduct such research in a way that will create public confidence that self-regulation is working on a widespread basis. Further, in cyberspace it is difficult to determine whether an organization shares personal information with third parties. In the offline world, consumers can attempt to track third-party disclosures of their name and address by supplying a unique spelling of their name and tracking the mail received. This method is not practical for email addresses.

Implementation Issues

Since web sites are a primary means of communication between consumers and firms, data will be collected primarily by analyzing the content of web sites. Personal web sites created by an individual or a family for non-commercial purposes will be excluded from the analysis. All other organizations doing business in the United States

are expected to self-regulate including non-profit organizations, educational institutions, commercial organizations engaged in business-to-business or consumer marketing, and government organizations. Data will be collected on the notices provided for both elements of self-regulation: fair information practices and enforcement mechanisms.

Two methodological considerations, reliability and validity, are critical. Reliability refers to the extent to which observations are consistent and stable. In content analysis, the data are based on the judgments humans make about written communications. Therefore, two types of reliability assessments are necessary. The first type of reliability is stability or intracoder reliability: the extent to which the same results are achieved when the same content is coded more than once by the same coder. The second type of reliability is intercoder reliability: the extent to which content classification produces the same results when the same text is coded by more than one coder. Both types of reliability are measured as the percent of agreement.

Validity refers to the extent to which the population in question is adequately sampled, and the representativeness of the sample to the population at large. Sampling is key to being able to draw conclusions about the effectiveness of self-regulation. A random sample, where any member of the population has an equally likely chance to be selected is the most effective way to perform a study with strong external validity. Because it is impossible to draw a true random sample of the web, this study should be conducted using stratified random sampling.

Stratified random sampling involves dividing the population, here the World Wide Web, into strata or sectors, and drawing random samples from each sector. In some cases, it may be possible to evaluate an entire sector. Sectors could include members of a trade association, companies within an industry, the Top 100 web sites, colleges and universities, organizations that market to children, etc[8]. Stratified random sampling is appropriate for two reasons. First, as stated above, it is not possible to sample the WWW as a single population. Second, there is a tradition in the United States to address privacy issues on a sectoral rather than an omnibus basis. It is important to note, however, that with stratified random sampling, a conclusion that self-regulation is or is not working for a particular sector cannot be generalized beyond that sector.

The following steps will be needed to implement the methodology:

1. Develop a coding form to be used to analyze the content.

2. Select and train the individuals who will analyze the content.

3. Define the samples to be used in the study.

4. Create hardcopy of the content to be analyzed. To enhance public confidence in the results of the study, copies of the data should be made available so

[8] See for example the FTC's June 1998 report to Congress available at www.ftc.gov. The FTC sampled web sites from 6 sectors.

interested parties can perform their own independent analyses using the same methodology and the same data.

5. Test code a sample of text

6. Assess the intracoder and intercoder reliabilities of the coders.

7. Revise the coding rules as appropriate. Repeat steps 4-6 as necessary.

8. Code all the text collected for the study

9. Tabulate results by sector and assess the intercoder reliability.

Conclusion: Building Consumer Trust Online

Consumer transactions are traditionally conceptualized in terms of a single utilitarian exchange where goods or services are given in return for money. This is the "first exchange." A variety of labeling requirements apply to this first exchange. For example, the majority of products we buy at the grocery store carry nutritional labels. Clothing labels describe fabric content and provide instructions for care. These labels help promote consumer confidence in the products they buy, and promote consumer education and choice. Firms also develop marketing campaigns to communicate the benefits of their products and services to consumers.

However, consumer transactions also include a "second exchange" consisting of the personal information generated as a by-product of the transaction. Here the consumer makes a non-monetary exchange for intangible benefits such as higher quality service and personalized offers by disclosing personal information to the organization. It is this "second exchange" that provides the ongoing flow of customer information needed to support a customer relationship and to enable decision-making by the organization about its products and services.

The second exchange is not new. In earlier times, data gathered from the second exchange were maintained in ledgers or in the proprietor's head. Technology, however, has transformed the second exchange into a competitive asset by connecting the point-of-sale with one or more databases. The richness of the data yielded by the second exchange varies with the characteristics of the point-of-sale transaction, ranging from a face-to-face cash transaction using cash registers without scanning capability where essentially no customer data are recorded to an Internet transaction where all of the customer's "electronic footprints" are recorded, even if the individuals browses without making a purchase. The ability to record browsing behavior online makes it possible for the second exchange to occur without the first exchange. This is one factor that distinguishes the cyberspace from the offline world where browsing occurs anonymously.

The notices defined in this paper are based on fair information practices and serve as labeling requirements for the second exchange. As is the case with the first exchange,

providing these notices builds consumer trust, increases the willingness of consumers to disclose personal information, and promotes consumer education and choice. Because recent privacy surveys suggest that an emerging trust gap is threatening consumers' willingness to disclose personal information online, building consumer trust is critical if the potential of electronic commerce is to be realized. For example, a 1998 *Business Week* survey found that privacy concerns were the most cited reason for not going online.

Prior research on privacy found that individuals are willing to disclose their personal information in exchange for some economic or social benefit if they trust the organization that is collecting the information. Trust includes a belief that their personal information will subsequently be used fairly and the individual will not suffer negative consequences in the future as a result of disclosing the information.

How does "labeling" the second exchange build consumer trust? By disclosing that a firm observes fair information practices, the firm signals to the consumer that it can be trusted with the information disclosed through the second exchange, provided that the firm's practices are consistent with its disclosed policies. This signaling function is particularly important for the Internet where consumers are less likely to deal with a human being or a familiar brand, and must depend on strangers to act in their best interests. Because fair information practices reflect a set of norms that the majority of consumers find acceptable, disclosing that the firm observes fair information practices provides an assurance to the consumer that the organization through its employees will not behave opportunistically. Therefore, observing fair information practices is in the interest of business as it promotes customer acquisition and retention by building consumer trust.

Appendix: Self-Regulation Checklist

I. Fair Information Practices

A. Awareness

- ❑ Organization's identity clearly identified
- ❑ Privacy notice accessible from home page by direct link
- ❑ Notice includes:
  - ❑ How information is used
  - ❑ Means by which consumer can limit disclosure
- ❑ Direct link to notice on pages where consumer is asked to provide information
- ❑ Notice applies to:
  - ❑ Email addresses
  - ❑ Site registration
  - ❑ Transaction information
  - ❑ Cookies and other technological methods of gathering personal information
- ❑ The web site provides for consumer education including:
  - ❑ email address or toll-free number and invitation to ask questions
  - ❑ frequently asked questions (FAQ)
  - ❑ additional explanations
  - ❑ links to additional educational materials
  - ❑ links to sites that provide educational materials

B. Choice

- ❑ Description of methods by which consumers may specify:
  - ❑ Whether their personal information may be used by this organizationl
  - ❑ How their personal information may subsequently be used by this organization:
    - ❑ Future contact by organization
    - ❑ Shared with third parties
- ❑ Mechanism must be:
  - ❑ Simple
  - ❑ Available
  - ❑ Affordable
- ❑ Objections may be registered online:
  - ❑ Web site
  - ❑ Email
  - ❑ Technological means
- ❑ Additional means to register objections:
  - ❑ Toll-free number (number displayed on web site)
  - ❑ Faxing or mailing a letter (number/address displayed on web site)
- ❑ Parental consent if using personal information related to children
- ❑ Affirmative consent for medical information

C. Data Security

- Describes protections for and means to ensure the reliability of personal information and to protect it from loss, misuse, alteration or destruction:
  - During transmission
  - In storage
  - When transferred to third parties

D. Data Integrity

- Notice of procedures to insure data are:
  - Relevant
  - Accurate
  - Complete
  - Current

E. Consumer Access

- Describes methods for:
  - Access
  - Correcting errors
  - Amending personal information

F. Accountability

- Notice on web site that:
  - Practices subject to self-assessment
  - Practices subject to external audits
  - Practices subject to internal audits.
  - Trade association membership with mandatory compliance (with link to description of trade association policy)
  - Participation in program with independent audits (with link to description of program)

II. Enforcement

A. Consumer Recourse

- Mechanism for submitting complaints is:
  - Easy-to-locate description on web site
  - Affordable
    - Electronic submission
    - Toll-free number
    - Fax
    - Regular mail

B. Verification

- No additional notice required

C. Consequences

- Description of procedures to assure compliance where compliance is a condition of:
  - Employment
  - Membership
  - The right to display a seal
- Procedures are:
  - Stiff
  - Swift
- Certifying organizations provide a means for consumers to submit complaints

Bibliography

Bennett, Colin J. 1997. The Canadian Standards Association *Model Code for the Protection of Personal Information:* Reaching Consensus on Principle and Developing Enforcement Mechanisms. In. *Privacy and Self-Regulation in the Information Age.* Washington: U.S. Department of Commerce. Pp. 157-165.

Bennett, Colin J. 1995. *PLUS 8830: Implementing Privacy Codes of Practice.* Ontario (Canada): Canadian Standards Association.

Culnan, Mary J. and Pamela K. Armstrong. 1998. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science,* forthcoming.

Culnan, Mary J. and Sandra J. Milberg. 1998. Consumer Privacy. In. Culnan, Mary J., Robert J. Bies and Michael B. Levy, eds. *Information Privacy: Looking Forward, Looking Back.* Washington: Georgetown University Press (forthcoming).

Culnan, Mary J. and Sandra J. Milberg. 1998. Managing the Second Exchange in Customer Relationships: Information Privacy as a Strategic Opportunity. Unpublished manuscript, School of Business, Georgetown University.

Holsti, Ole R. 1968 Content Analysis. In. G. Lindzey and E. Aronson, Eds. *The Handbook of Social Psychology,* 2nd ed. Reading: Addison-Wesley. Vol. 2, pp. 596-692.

Kerlinger, Fred N. 1973. *Foundations of Behavioral Research,* 2nd ed. New York: Holt, Rinehart and Winston, Inc.

Krippendorff, Klaus. 1980. *Content Analysis: An Introduction to its Methodology.* Newbury Park: Sage Publications.

Nachmias, David and Chava Nachmias. 1976. *Research Methods in the Social Sciences.* New York: St. Martin's Press.

Rosenthal, Robert and Ralph L. Rosnow. 1984. *Essentials of Behavioral Research: Methods and Data Analysis.* New York: McGraw-Hill Book Company.

U.S. Federal Trade Commission. 1998. *Privacy Online: A Report to Congress.* Washington: Federal Trade Commission. Available at www.ftc.gov.

Weber, Robert Philip. 1990. *Basic Content Analysis,* 2nd ed. Newbury Park: Sage Publications.