Final Report

of the

Federal Trade Commission

Advisory Committee

on

Online Access and Security

15 May 2000

1 INTRODUCTION

The purpose of the Advisory Committee on Online Access and Security ("ACOAS", the Advisory Committee, or Committee) is to give advice and recommendations to the Federal Trade Commission ("FTC") concerning providing online consumers reasonable access to personal information collected from and about them by domestic commercial Web sites, and maintaining adequate security for that information.

In particular, the Charter of ACOAS directs that the Advisory Committee "Will consider the parameters of reasonable access to personal information and adequate security and will present options for implementation of these information practices in a report to the Commission." (Charter of the Federal Trade Commission Advisory Committee on Online Access and Security "Charter)[1]."

The Committee was comprised of 40 members who met four times in public meetings at the FTC in Washington, DC. Smaller working groups were formed to conduct work of the Committee between the meetings. The Committee received 39 public letters of comments and heard public testimony at each of its meetings.

This is the final report of the Committee. The Committee considered access and security as it relates to online information. The context of this Committee's consideration was not to provide consensus definitions or options for legislation, mandatory regulation or self-regulation; nor is the report intended to replace more detailed and industry-specific initiatives in fields regulated by law, such as health care and financial services. Rather, the Advisory Committee here presents a range of definitions or options that have been identified as ways to implement the Fair Information Practice principles of access and security. Except for security, a clear recommendation was agreed to by all members of the Committee, no one definition or option represents a consensus of the members of the Advisory Committee.

[1] See Appendix A

2 ONLINE ACCESS

This section considers "the parameters of reasonable access", which the Committee refers to as "Access".. As the Committee's deliberations revealed, this principle of the FTC's Fair Information Practices (which include notice, choice, access, and security) can be complicated – and controversial. This Section seeks to unpack the concept of access in a way that helps Web sites and policymakers understand the difficult questions that must be answered in fashioning an access policy.

We first identify the questions that must be answered in defining access – does it mean the ability to review the data or does it include authority to challenge, modify, disable use, or delete information?

We then ask "Access to what?" What is personal information for purposes of the access principle? Businesses gather a wide variety of data from many sources. Information is sometimes provided by the individual consumer and sometimes by a third party. At times it is inferred or derived by the business itself, using its own judgment or processes. And sometimes the data is imperfectly personalized – it relates to a computer that may or may not be used only by one person. Given the breadth of data classification involved, how much of the data that businesses possess about consumers is covered by the access principle?

Our next overarching question is "Who provides access?" Is it just the entity that gathered the data? Does it include its corporate affiliates and agents? Or every company to which the data may have been passed?

The last of our ground clearing questions is "How easy should access be?" Should Web sites charge a fee to cover some or all of the cost of providing access? Is it fair to impose limits on multiple or duplicative access requests? How much effort should be required, from the consumer or the business to meet the access requirement?

Having explored these four foundation questions, the Committee next lays out four illustrative options that show the many different ways in which the access principle could be implemented. The broadest option, Option 1, would give consumers "total access" - access to any information a commercial Web site may have about them. Under Option 2, consumer access becomes a default rule; personal information would be made accessible to consumers if the information were retrievable in the ordinary course of business. Option 3 takes the access decision case-by-case; and would not create a presumption for or against access but would take into account a variety of factors, including industry sector, the content, the data holder, the source, and the likely use of the information. The narrowest option, Option 4, entitled "access for correction," would provide access only to information that is used by the commercial Web site to grant or deny a significant benefit to the consumer, and then only if access is likely to produce an improvement in the accuracy of the information that justifies the costs.

Finally, this section turns to an issue that links access and security – authentication. How does a Web site know it is providing access to the right person? Giving access to the wrong person could turn a privacy policy into an anti-privacy policy. The final section of this report examines the difficulties and possible solutions inherent in trying to authenticate requests for access to personal data.

2.1 WHAT IS ACCESS?

Commercial Web sites and their customers often have a common interest in making sure that customers are aware of the information that the Web site has collected about the consumer. To take one example, think of a Web site that receives an order from a new customer and within 24 hours is ready to ship. It is only prudent for the Web site to give the customer access to the shipping information, perhaps sending an email to say, "This is what we think you ordered and this is where we think you want it shipped." Both consumer and Web site have an interest in the accuracy of information, and sharing it with the consumer is a useful safeguard against errors or fraud in the order process. The same interest in preventing errors may lead commercial Web sites to provide their customers with access to other personal information that the Web site has maintained about the customer. Similarly, banks and

consumers both benefit from the transmission of detailed credit card statements each month. Among other things, providing an opportunity to review each transaction protects both parties against fraud.

While there is broad agreement on this point, the issue of consumer access to personal information does not lend itself to consensus. For some, exceptions from the principle of access should be rare and narrow. They view access as a broad principle to ensure accountability and build trust. For others, it is the access principle itself that should be interpreted narrowly. They contend that the costs of access – in money, convenience, and privacy risks – are often too high, for businesses and consumers alike.

This report cannot bridge the range of strong and honest opinions across the Committee regarding how and when Web sites should provide access to personal information. What it can do, and what we hope it does do, is illuminate ways of thinking about and talking about access so that even those who disagree profoundly can communicate in a common tongue. With that in mind, the Committee first turns to the question of defining access. What do we mean when we say that a consumer will have "access" to personal information in the hands of a commercial Web site? This question leads in turn to several different questions about how access may be defined.

Type of Access. The first way of measuring access is to focus on the type of consumer access, which can be quite varied. The terms used by the Committee to convey the type of access included "view," and "edit access. If "view" access were provided, consumers would be able to view or obtain a copy of the information. "Edit" access, in contrast, would allow consumers to correct, amend, challenge, or dispute information or, further, to have the information be made unavailable for use by the Web site in its ordinary course of business or to have particular information removed from their file. (There are, of course, significant practical differences for both consumers and Web sites between allowing correction of data and allowing challenges to the data.).

The Committee did not agree on a single appropriate type of access for every situation. Instead, the type of access may vary among the access options put forth in following sections. The type of access may vary in light of other considerations such as whether the Web site in question is the original source of the data and what form of authentication the consumer utilizes in order to obtain access.

Means of Access. Access can also be provided through a variety of means. For example, information can be provided online, over the telephone, through the mail, or in person. In addition, information can be provided in real time, at the consumer's request, at regular intervals, in response to a specific event, or on some other schedule. Determining the most appropriate means of providing access is best done with due consideration to the usability for consumers, the authentication necessary to limit unauthorized access, the cost to businesses and consumers, and the security requirements surrounding the data.

Ease of access. Likewise, ease of access will vary depending on the circumstances. It will be influenced by how "usable" the access system may be for those without technical training, the form in which the information is presented, the availability of the access system, and the notice by which consumers are made aware of what information is available and how to access and correct this information. Easy to use access will be more meaningful to consumers. The cost of providing easy to use access systems is likewise a consideration. These costs may include the cost of creating and maintaining new or special capabilities to provide access, adding customer service staff to handle customer requests, additional security systems, and other costs.

2.2 WHAT IS PERSONAL INFORMATION?

Defining the term personal information is central to the task of considering various options for providing access. Over the course of its meetings and deliberations, the Committee discussed various approaches to defining the information that is made available for individuals to access. The discussion below examines several factors to be considered in defining the information available for access. Defining personal information is one factor in determining what data will be accessible to individuals. The scope of access will be further influenced by the access option chosen (section 2.5) and decisions about the appropriate points and means of access discussed below.

"Fit"-- perfectly v. imperfectly personal data. Information is linked to individuals in various ways. Data can be tightly tied to a specific individual's name, address, and birth date. Data can be tied to a device such as the individual's telephone, Internet browser, or computer in which case it may reflect the individual's activities as well as the activities of others who use the device. In such instances, we are left with data that is often personal to an individual but perhaps not unique to the individual. The data collected in both cases may be used for nearly identical purposes, despite differences in its specificity. For example, information about an individual's use of a credit card may be used to determine the advertising inserts placed in their monthly billing statement, just as information about the actions of a computer browser may be used to determine the advertising placed on the next page the browser visits. Committee members expressed different opinions as to whether the definition of personal information should include imperfectly personal data in addition to perfectly personal data.

The medium of collection: online v. offline. Information is collected from individuals through a variety of mediums. In both the "brick and mortar" and "click and mortar" worlds data is gathered from individuals through a variety of means. Members of the Committee expressed different opinions as to whether the scope of access should be limited to data collected online or should include all data regardless of what collection medium was used.

The source of collection: individual v. third parties. Information about an individual can be collected directly from the individual or from third parties. A business may purchase information about its existing customers from another business or it can purchase a list containing information about individuals it would like to attract as customers, such as a mailing list. Similarly, a business may purchase data that is used to enhance the information that it has collected about its own customers. Committee members expressed different opinions as to whether the scope of access should include all data regardless of its source or should be limited to data collected directly from the individual.

The method of collection: passive v. active. Information is collected from individuals actively and passively. Information is actively solicited from the individual through the use of surveys, registration forms, and other solicitations. At other times data is gathered without the individual's explicit cooperation as in the collection of clickstream data. This is commonly referred to as passive data collection because the individual is not actively providing information. Passive collection is akin to observation or monitoring. Members of the Committee expressed different opinions as to whether the scope of access should include all data collected or be limited to actively collected data.

The type of data: factual v. inferred and derived data. Inferred or derived data is information that the business has not "collected" either passively or actively about the individual, but rather has inferred from other data. It includes the assumptions or conclusions that a business makes about an individual, not the factual record of the individual's action or behavior. In this discussion, we have drawn a distinction between inferred data, which is based on information about a sample population, and derived data, which is based on information gathered from or about the individual consumer.

Committee members expressed different opinions as to whether the scope of access should include inferred and derived data or be limited to factual data. Advocates of providing access to inferred and derived data argue that it is used to make decisions about consumers and should therefore be available to them. Critics of providing access to such data make three arguments: that disclosing the data will invite competitors to discover proprietary information, that it will chill communications, such as candid opinions expressed about consumers by third parties or employees, and that providing access to the underlying facts is sufficient to allow consumers to know whether inferences about them are accurate.

2.3 WHO PROVIDES ACCESS? THE THIRD-PARTY ISSUE

Even after access has been defined, questions remain. In particular, who is to provide access to personal information?

Information is mobile, especially on the Web. This is true for personal information as well. Take our order-fulfilling Web site example from the last section. There may have been a time when businesses all had their own shipping departments, perhaps even their own delivery vans. But increasingly today; the shipping information supplied by our Web site may have come from and gone to several third parties – such as credit card processors, fulfillment houses, and overnight delivery firms.

How should the access principle take account of the movement of information from and to third parties? We identified three areas of particular salience. First, we dealt with the question of whether and how third parties should provide access. Second, we examined the centralization risk associated with expanding the access obligation to corporate affiliates. And third, we dealt with the question of providing "edit" access to information supplied by third parties.

Upstream and Downstream Parties. If a Web site says that it provides access to personal information, the Web site itself is plainly covered by that promise. But should the assurance also bind third parties?

There are at least two kinds of third parties involved in the access equation. These may be characterized as "upstream" third parties and "downstream" third parties. Upstream third parties are suppliers of information used by the Web site. Downstream third parties receive information from the Web site. (We will consider a third category later).Upstream information is often purchased. A business may purchase information about its existing customers (a credit report, for example) or it may purchase information about individuals it would like to attract as customers (a mailing list, for example). Similarly, a business may purchase data that provides demographic details to enhance the information that it has collected about its own customers. As discussed above, Committee members expressed different opinions about whether and how to provide access to such upstream information.

Even if consumers receive access only to information gathered by the Web site, there remains the question of what to do about downstream third parties. Again, Committee members expressed different opinions about the extent to which those third parties should be expected to provide access.

The Committee generally agreed that companies that provide access to information should also provide access to the data held by their agents,, such as the fulfillment house in our Web site example. However, beyond that point, opinion divided. Some members of the Committee thought that providing access to information in the hands of downstream third parties was unworkable and should not be attempted. Some argued that consumers could be protected using notice instead of access, if such notice thoroughly described the transfer of information to third parties. Others held that it will be impossible to adequately provide effective notice and consumers will not be aware of the existence of third parties, let alone how to contact them and gain access to their information. Still other members of the Committee believed that downstream parties should provide full access, although the type of access may vary in particular circumstances.

Corporate Affiliates and the Risks of Centralization. The Committee recognizes that many companies that hold personal information are made up of a 'family' of businesses, each with a business (and therefore a data-driven) relationship with customers. Some Committee members believe that access should be granted across the corporate lines of affiliated companies, even if the information has not been directly traded from one entity to the other. This might be called the problem of "side-stream" third parties. In this context, concerns were raised that an obligation to provide consumer access across corporate lines might compel companies to create databases that gather all information into large central structures. Paradoxically, combining and centralizing previously separated databases in order to enhance access might pose an increased threat to personal privacy.

The Committee members agreed that centralizing and linking personal information is not the purpose of the access principle. Access should not be interpreted to encourage the creation of a new file or record on an individual. In response, it was noted that companies could provide central points to serve consumers access requests without actually centralizing the maintenance or storage of data.

For example, parent companies could create a single point of access for consumer access requests, which would either transmit the requests to affiliates or provide information that would allow consumers to identify and make requests directly to the affiliates. Some questioned the workability of even this approach - whether companies could easily " match up" consumers that they might know under different names or authorities (does a joint bank account held by "Mr. and Mrs. Smith" get matched with a brokerage account held by John Smith?) without creating a central database. They also argued that such a central point might be difficult to manage for companies that regularly acquire and divest subsidiaries.

The Committee recognizes a second concern about providing a single point of access to all affiliates' information. It may increase the vulnerability of an individual's information to compromise – e.g.,

if bad actors can determine the password, they can get access to private information from one convenient location. Such a decision therefore must be accompanied by a risk assessment and installation of appropriate authentication and security.

Third Parties and "Edit" Access. "Edit" access poses special problems in the context of third parties. Suppose that a Web site obtains information about a consumer from a third party, adds it to its files, and shares the information with a downstream advertiser as well. Then suppose that the customer wishes to challenge or modify the data. Should the Web site simply make a note in its files or should it do something about the upstream and downstream third parties? There are many issues in this scenario, and we reached no conclusions. The Committee recognized the desirability of correcting errors up and down the data stream. It also recognized that no company could know for sure where the data may have gone once it left the company's control. Some Committee members took the view that requests for "edit" access should always be directed to the authoritative source of the information in order to assure the integrity of the information. Other Committee members felt a general principle requiring consumers to return to the original source as overly burdensome, especially in instances of public records where they might not realize that such a source of personal information exists. For example, if the information is from a public source, a fair credit reporting agency, or other entity that is identified as the authoritative source of the data, then any efforts to challenge or correct the information should be directed to that source and not to downstream recipients of the data.

2.4 COST OF ACCESS

We discussed whether businesses should charge consumers for access. The possibilities discussed ranged from never charging a fee to always charging a fee. Businesses might charge a nominal fee commensurate with the type of data being accessed, the use of data being accessed, or the amount of data being accessed. The fee might also be based on the frequency of a user's access requests or the nature of the access requests. For example, a request for real time access might incur a larger fee where a request for delayed access might be less costly. Alternatively, the service provider could be free to charge any reasonable fee within specified limits.

Charging a fee would allow businesses to recover at least some of the cost of providing access and would provide a means to shift the cost of providing access to those consumers who use access rather than passing it on to all consumers indirectly through higher prices. Experience suggests that many if not most consumers never seek access to their personal data. Fees might also provide a deterrent to frequent, nuisance or harassing access requests.

Fees may limit the ability of consumers to access their information or lessen the attractiveness of accessing personal information. There was a wide range of opinion about when, if ever, an access fee should be charged. Some members of the Committee have argued there should never be a charge for reasonable access. Others thought any fee would be inappropriate where an adverse decision was based upon the information being accessed, but supported nominal fees, not greater than cost, in other cases. Still others contended that it was necessary to charge some fee to reflect what could be substantial access costs and to discourage frivolous (or even fraudulent) requests.

2.5 ACCESS OPTIONS

There are many possible answers to the questions set forth above. The answers determine how a Web site would implement the access principle. In this section, we provide a range of possible options for providing access to personal information. The broadest option, Option 1, would give consumers "total access" - access to any information a commercial Web site may have about them. Under Option 2, consumer access becomes a default rule; personal information would be made accessible to consumers if the information were retrievable in the ordinary course of business. Option 3 examines the access decision case-by-case; and would not create a presumption for or against access but would take into account a variety of factors, including industry sector, the content, the data holder, the source, and the likely use of the information. The narrowest option, Option 4, entitled "access for correction," would provide access only to information that is used by the commercial Web site to grant or deny a significant benefit to the consumer, and then only if access is likely to produce an improvement in the accuracy of the information that justifies the costs.

2.5.1 ACCESS OPTION 1: TOTAL ACCESS APPROACH

Commercial Web sites should provide access to all personal information regardless of medium, method, or source of collection, or the type of data in question.

The "total access" option works from the presumption that consumers would benefit from having access to all their information in the possession of commercial Web sites. Under this option, no personal information would remain off-limits or confidential. This option allows consumers to verify the accuracy of that data, and places them in the position of knowing how their personal information is collected and used. In keeping with the purpose of providing consumers as much access as possible, businesses would provide initial access for free, while charging for repetitive access requests or terminating access upon unduly repetitive access requests. This option would also allow consumers to exercise all types of access.

The "total access" option would only apply to existing records. For example, information possessed by a data collector but not yet linked or joined with online information would not be subject to access. In addition, more comprehensive records of individuals should not be created under the guise of establishing "total access". Such action could centralize even more personal information andthat could pose a threat to personal privacy.

Proponents of this approach would argue:

1. By providing greater access rights, businesses could increase the reliability and accuracy of data, build consumer confidence and trust, experience a public relations benefit, make better decisions based on better data, expand markets by giving consumers greater confidence in online privacy, and experience greater efficiencies if they limit information collection to only what is necessary.
2. Consumers might experience an enriched understanding of data collection practices, increased confidence in the online environment, more control over the accuracy of personal information, the ability to identify inaccurate data before it harms them, the ability to make better privacy decisions in the marketplace (including decisions to protect anonymity), and the ability to better police businesses for compliance with any stated policies.
3. This option presents uniformity and predictability for both businesses and consumers. Businesses would know what scope of access to provide from the outset of their operations. By creating a clear standard for access, this option may allow companies to minimize what could be a costly implementation. Moreover, that clear standard could also provide consumers with an easy-to-understand expectation of access.

Opponents of this approach would argue:

1. For businesses, this approach would lead to a substantial increase in costs, including, among others, any required modifications or new design requirements placed on existing systems, new storage costs, new personnel costs, new legal costs and losses due to the disclosure of internal practices and proprietary information and affect the confidentiality of procedures companies use to make decisions and assumptions about user data.
2. The costs of implementing this option could provide a significant business incentive to find offsets, likely through new uses for the information that could be accessed based on software and other systemic design changes. This might well have an accompanying affect on consumer privacy.
3. Consumers would also experience additional costs, such as: pass through costs for system upgrades, new personnel and potential opportunity costs of businesses not investing in developing new products. These costs could unfairly fall on those consumers who do not use the access system.
4. Both businesses and consumers could be harmed by unauthorized access to a greater amount of information. Businesses may face a higher liability in this case and consumers may be risking more of their privacy.

2.5.2 ACCESS OPTION 2: DEFAULT TO CONSUMER ACCESS

Commercial Web sites should provide access to personal information that is retrievable in the ordinary course of business.

The "default to consumer access" approach works from the presumption that consumers should have access to their personal information. This approach recognizes that consumer access to personal information serves multiple purposes, including but not limited to ensuring accuracy. This approach seeks to promote openness and consumer awareness in the belief that they aid oversight and compliance and promote greater trust between businesses and their customers. Openness and awareness may increase consumer demand for limited data collection and encourage privacy-sensitive business practices.

Under this option, information is not accessible to a consumer unless it can be retrieved by taking steps that are taken in the regular course of business with respect to that information, or steps that the organization is capable of taking with the procedures it uses on a regular basis. This limitation on access is designed to ensure that businesses need not create new and more elaborate databases -- the creation of which in and of itself poses a substantial threat to personal privacy --solely to meet the access requirement. However, limiting access in this fashion means that some personal information may be out of reach under this option. Personal information is not retrievable in the ordinary course of business if retrieval would impose an "unreasonable burden" on the business. The "unreasonable burden" concept is not a stand-alone exemption; its sole purpose is to help define what is and what is not retrievable in the "ordinary course of business." It allows for a purpose or cost-benefit analysis in those situations where the ability to retrieve the information would be very costly or disruptive to the business. It is here that the sensitivity of data, the uses of data, the purpose of the request, etc. could be considered. If an organization uses this exception to limit access, it should refer the individual to the provisions in its privacy notice that discuss its data collection use, and consent/choice policies, or provide the individual with information equivalent to the privacy notice.

In certain circumstances where information is retrievable in the ordinary course of business other compelling public policy considerations may limit access. For example, while the Privacy Act provides individuals with access to records the government maintains about them it requires the government to redact information about others contained in an individual's files in order to preserve the other individual's privacy. This approach is consistent with U.S. Federal statutes that provide access and correction, but may limit them due to other compelling public policy considerations.

Proponents of this approach would argue:

1. This approach provides broad access rights and reasonably matches consumer expectations that they can access personal information collected about them.
2. This approach places the burden of establishing reasons for not providing access on the data holder, making it more likely that access will be provided when it is not overly burdensome to do so. While other compelling public interests can limit access, such considerations occur within a framework that favors access ensuring that they will not be misused or expanded.
3. This rule is straight forward and clear yet sufficiently flexible to adapt to evolving technology. By avoiding possibly complex balancing decisions in routine requests, the default rule may be easier to administer for most e-commerce companies, and it is similarly likely to be easier to administer by third party enforcement programs, whether governmental or self-regulatory.
4. This approach avoids subjective or intrusive probing as to the requester's intent in asking for access or his/her need for access, because it requires such considerations only if the data holder can show that providing access is very burdensome.
5. The approach does not unduly force businesses to provide access to aggregations of data that it does not already possess and retrieve itself - the consumer is given access to information about them that is commensurate with the view what the business itself possesses and uses.

Opponents of this approach would argue:

1. 1. The 'unreasonable burden' standard provided in this approach is too high for businesses to justify limits on access where the consumer's need for access is unclear or not compelling. Lots of data collected by Web sites cannot be corrected, because it is observational in nature (such as clickstream data) or inferred or derived (assumptions and conclusions) that are not capable of correction per se. The presumption of access, limited only by the high threshold of 'unreasonable burden', places a heavy burden on businesses in cases where the consumer interest in access may be weak.
2. This option is too vague for Web sites to understand and apply. The claimed exception for 'compelling public policy' provides no reliable protection either for the Web site business' proprietary data or for confidential information supplied by third parties. And when read carefully, the purported exception for 'ordinary business practices' disappears, turning into a question of whether providing access would be 'very costly or disruptive.
3. This option would require Web sites to provide access that is costly and disruptive, as long as it is not 'very' costly and disruptive. The cost of this option will fall on the many consumers who never use this excessively elaborate access system.
4. This approach is overly restrictive. Because businesses would not be required to provide access unless personal information is "retrievable in the ordinary course of business," access rights could vary quite a bit from business to business, or across different types of businesses. Businesses may try to use nuances in the interpretation of "retrievable in the ordinary course of business" to avoid providing access. Potentially, a business could even set up its data structures so that the data could be used to make decisions about consumers without being retrievable as a separate bit of information. Similarly, the proprietary exception may inappropriately limit access. Consumers may have a significant interest in viewing derived or inferred data that is used to make decisions about them.
5. This approach is overly restrictive because the exceptions give businesses the ability to unilaterally deny consumers access and will lead to confusing and unpredictable results. Vesting businesses with the ability to deny access due to costs is inappropriate. Such determinations should be narrow and made through fair, open, and accountable processes. Although the rule may be very straightforward for the majority of situations, difficulties in determining whether or not a particular business falls within the exceptions would require businesses to become experts in this area. In this regard, the rule may make access unduly complex for businesses.

2.5.3 ACCESS OPTION 3: CASE-BY-CASE APPROACH INCLUDING SECTORAL CONSIDERATIONS

Commercial Web sites should provide access depending on a variety of considerations and the level of access may differ for different types of information or in different sectors.

A third approach would be to treat different information differently depending on a calculation that takes into consideration, among other things, the content of the information, the holder of the information, the source of the information, and the likely use of the information. This approach is necessarily more complex, recognizing that whether access is appropriate depends on a variety of factors. Different sectors, record-keeping systems, and types of data raise different issues. The challenge, therefore, would be to develop a set of rules that is easy to administer.

Unlike the 'default to consumer access' option that is premised on a presumption of access, under this approach there is no presumption for or against access. Rather, the access inquiry requires an analysis of the relevant factors, including an explicit weighing of costs versus benefits. This determination will depend both upon the nature of the data in question (e.g., information regarding children or medical information) and the record-keeping system in question. On the other hand, it is clear that under this third approach, there would be categories of data to which access is more limited than in the other approaches. For example, inferred data, "non-factual data" or internal identifiers might be less accessible under this approach than under the previously detailed approaches.

This option supports access for a variety of purposes, including but not limited to promoting consumer awareness. Access itself may not only enhance "consumer privacy" per se, but also ensure the accuracy of data and protect against adverse decisions based upon incorrect data.

Applying this approach, in some instances access may be limited for purposes of correction of erroneous data. This approach also may allow a more precise weighing, in light of the nature of the data and the sector involved, the consumer's reasonable expectations about the data, and the costs of providing access, of whether access to the particular type of data is warranted. As with all options, the cost of providing access is a consideration that must be factored into the analysis. As the purpose for the data use becomes more significant, however, cost may become less of a factor.

U.S. privacy laws have developed as the result of a sector-by-sector approach similar to this option. This approach could also result in classes or categories of data receiving similar treatment across various sectors. This approach considers data privacy in the context of specific types of information or sectors and whether it is likely to be used in a way that could adversely affect the data subject. For example, access as the ability to view and correct is the norm with regard to financial information used to make credit granting and employment decisions under the Fair Credit Reporting Act. Several laws provide for access and correction. These include the Family Education Rights and Privacy Act (20 USC 1232) that allow students the ability to view, dispute, and delete parts of student records. The Cable Communications Policy Act (47 USC 551) interprets access as the ability to view and correct.

The U.S. Privacy Protection Study Commission also addressed access issues in the mid-1970s. The Commission recommended access and correction as a component of fair information practices as essential to fairness in many areas. They recognized that decisions about when and how to provide access to information might be unique to the particular information systems or sectors.

This approach would provide different access possibilities to different sectors or types of data. Depending on the number of factors in the calculation, the permutations could be extensive. This approach could afford access to all sensitive data such as financial information, health information, or information relating to children, and other data in sectors of the economy that may affect individuals in a materially adverse way if it is inaccurate. In these instances, it would yield the same result as the Default Rule and Total Access approaches. Conversely, substantially less access could be made available to data that is inherently less sensitive or from sectors of the economy that can have less of a material affect upon a consumer.

Proponents of this approach would argue:

1. The approach affords greater flexibility than the other options while maintaining the principle of access where it is warranted.
2. By considering each type of data and industry sector on its merits, the approach may more accurately balance factors bearing on whether to provide access.
3. This approach may more realistically address the expectations of both consumers and businesses. Consumers tend to be interested in obtaining access to information that makes a material difference in their lives. Where the information does not make a difference, consumers appear to be less interested in obtaining access.
4. In circumstances in which consumer access fees do not fully cover the costs of providing access, this approach would reduce costs to consumers, and more fairly apportion costs of access. Specifically, it would avoid the problem under a broad-based approach encouraging access to most data of forcing consumers uninterested in obtaining access to bear the costs of creating the access infrastructure.

Opponents of this approach would argue:

1. This approach departs from the principle of access. It replaces the presumption of access found in privacy laws and policies, and substitutes a subjective process of reasoning that lacks meaningful standards. This approach could result in decisions to deny or grant access that vary business by business, data element by data element, or, in the extreme, individual by individual.

2. The approach may involve far too many factors to allow a comprehensible set of rules to emerge. Moreover, many of the factors, e.g., sensitivity, are difficult to assess objectively.
3. The complexity of this approach may yield inconsistent results if different decision makers are assessing issues such as sensitivity. This inconsistency may lead to consumer confusion.
4. Consumers may not agree that any information maintained about them does not warrant access on the basis of someone else's perception of the sensitivity of the data.

2.5.4 ACCESS OPTION 4: ACCESS FOR CORRECTION

Commercial Web sites should provide a consumer with access to personal information if (1) the information is used to grant or deny the consumer a significant benefit and (2) providing access will improve the accuracy of the data in a way that justifies the cost.

This option begins by asking why access to personal data is important to consumers. One reason for allowing access – correcting errors – is of interest to both the individual and to the Web site. If the Web site uses personal data to grant or deny some significant benefit to consumers, then errors in the Web site's files could cause real harm to the consumer. Giving the consumer access to the data allows the consumer to challenge or correct errors. Both the consumer and the Web site have an interest in the accuracy of such data, so allowing access and correction helps both parties. Thus, even if allowing access increases the Web site's costs, as it often will, and even if the costs cannot be passed on to consumers, the Web site itself will get some benefit from access designed to improve the accuracy of important data.

This option treats error-correction as the principal reason for incurring the costs of providing access. It gives little weight to other justifications that have been advanced for access, such as the view that giving consumers access to the files maintained about them will discourage Web sites from gathering sensitive or unnecessary information.

Maintaining an access system imposes costs on Web sites and their customers – not just in money but also in convenience and even risks to privacy.

The "access for correction" option seeks to minimize those costs while preserving the error-correction rationale that it treats as the touchstone for defining reasonable access.

Under this option, a Web site would grant access to personal data in its files only after answering two questions in the affirmative: (1) Does the Web site use personal data to grant or deny significant benefits to an individual? (2) Will granting access improve the accuracy of the data in a way that justifies the costs?

The first question resolves many of the issues that are more difficult to resolve under the other options presented here. Examples of information that is used to grant or deny significant benefits include credit reports, financial qualifications, and medical records. In contrast, information used for marketing purposes, such as targeted ads or direct mail, would not be treated as conferring or denying a significant benefit to a consumer. The approach calls for access only to information that is collected and retrieved in the ordinary course of business. With some qualifications set out below, however, the approach would allow access to information that has been provided by a third party, as long as the information is used to grant or deny significant benefits.

The second question – whether allowing access to correct errors justifies the cost – raises a variety of possible exceptions to access. Inferred data, such as judgments made about the consumer by third parties or Web site employees or even expert information systems, are not usually susceptible to direct correction, although obviously the underlying data used to generate the inference can be corrected. Additionally, this option takes account of costs that are not simply financial. Thus, access is not ordinarily justified if it would reveal trade secrets. Nor is it justified if it would compromise expectations of confidentiality on the part of third parties or Web site employees (e.g., comments by the Web site's "help desk" employees on the civility of particular customers). Under this option, as the likelihood of improving the accuracy of personal data declines and the cost of providing secure access increases, the cost-effectiveness of access also declines and the public-policy justification for access grows weaker.

Proponents of this approach would argue:

1. The most obvious goal served by allowing access to personal data is correction of erroneous data that may be used to make important decisions about an individual. The access principle has often been implemented in contexts where correction of data is essential – such as credit reports and other instances where errors have a direct impact on the individual and where those errors can be reduced by allowing access.
2. The other goals advanced for access -- education, accountability, consciousness-raising -- are better served by consumer notice instead of an expensive and little-used access system. These reasons for access do not justify the costs of providing access, which include not just time and expense but in some circumstances a very real risk to privacy if access itself results in the compromise of personal data. Rather than pay those costs and take those risks for a large body of mostly insignificant data, we should concentrate on providing access to data that is important and whose correction can make a difference in the lives of consumers.
3. There is no compelling reason to provide access to uncorrectable data, unless the real goal is to raise the cost of maintaining personal data so high that Web sites just give up and stop gathering the information. Those who want to restrict information gathering should argue for that goal explicitly and not try to achieve the goal indirectly through unnecessarily broadening the access principle.

Opponents of this approach would argue:

1. Access serves broader purposes of openness, accountability, and fairness. This option reduces the principle of access to a single purpose – correction of errors. Sometimes data may not be correctable but may be used in inappropriate or unfair ways with significant impact on the individual.
2. Access is necessary for informed consumer choice. Only broad access will create the kind of accountability that is required among Web sites. Once consumers truly know what Web sites are collecting about them, they will force those sites to adopt responsible data collection policies.
3. Industry should bear the costs of handling data responsibly. If the cost of providing access outweighs the value of the information to a Web site, the site should revisit its' information-gathering practices. Cost benefit analyses of this type are good for privacy and for businesses. Just as industries that can't afford new pollution controls close their old factories, businesses that are incapable of handling information responsibly should close their doors.

2.6 AUTHENTICATION

This Committee was asked to consider not just access to personal information but also security for personal information. This combined mandate was an appropriate one, for there is a very real tension between access and security, one that we address in this section.

Unlike the other Fair Information Practice principles, the access principle sometimes pits privacy against privacy. Simply stated, the problem is this -- On the one hand, privacy could be enhanced if consumers can freely access the information that commercial Web sites have gathered about them. On the other hand, privacy is lost if a security failure results in access being granted to the wrong person – an investigator making a pretext call, a con man engaged in identity theft, or, in some instances, one family member in conflict with another.

How can consumers get the benefits of access to their personal data without running the risk that others will also gain access to that data? The answer is to employ techniques that adequately authenticate consumers – that provide sufficient proof that the consumer is authorized to have access to the personal data. As more and more of our personal information is stored on the Web, like stock portfolios and financial accounts, the need for good online authentication grows ever stronger, and new solutions continue to arrive in the market.

But authentication often involves making tradeoffs between security and ease of access. How should those tradeoffs be made in the context of an access policy? In particular, what kind of authentication techniques should a commercial Web site employ to limit inappropriate access to personal information?

If the consumer must produce three picture IDs, privacy will be protected, but access will be difficult. If an email address is treated as sufficient, access will be encouraged, but the risk of compromise will grow. This section of our report attempts to illustrate the ways in which these competing interests can be addressed. In the end, it will be clear that there is no single answer to the dilemma described above.

As with many of the access issues discussed in this report, the proper level of authentication depends on the circumstances. To take one example, the level of authentication depends in part upon whether the consumer will simply view the information or will correct or amend it as well. Allowing the wrong individual to view someone else's data is a violation of privacy – and may lead to additional harm ranging from embarrassment to loss of employment – but allowing the wrong person to "correct" that personal information can result in equally devastating consequences. For example, in the past, before the Postal Service implemented tighter controls, criminals have gained access to an individual's credit card accounts by filling out a change of address card and diverting the individual's credit card statements to another location. With access to the individual's bank statements and credit card bills, the crook has ample information to impersonate the victim. For this reason, where correction or amendment is provided, an audit trail should, if practicable, be maintained to aid in identifying potential problems.

In judging the proper level of authentication, it is necessary to bear in mind that the risk of liability will heavily influence the Web site's choices. A business runs a risk of liability if it allows the wrong person to access personal information. Although it is not clear what specific remedy an individual might have under existing law, the lack of certainty regarding liability presents a problem for both individuals and businesses. If the liability standard imposed upon business is too strict, businesses could raise the barrier to access very high, burdening individuals' access in an effort to avoid liability. Conversely, if existing legal remedies do not provide sufficient penalties for inappropriate access, individuals' privacy may suffer. How to strike an appropriate balance that spurs good practices, encourages the deployment of robust authentication devices, and does not overly burden access is the challenge at hand.

We noted that efforts to provide consumer access could lead to authentication measures that could erode anonymity on the Internet. Authentication can support access whether the consumer chooses to be anonymous, pseudonymous, or known. So, authentication does not necessarily require consumers to provide personally identifiable information. But as a practical matter the conflict is often direct. For example, technologies such as biometrics may improve authentication but they may inevitably reduce the consumer's ability to remain anonymous.

Similarly, access processes that rely on data held by a third party to authenticate a consumer may increase the proliferation of personal data, bringing into question the privacy policies of third party authentication services. At the same time, third parties – intermediaries – can also play a role in the protection of identity. Currently, several intermediary companies provide anonymity or pseudonymity to individuals on the Internet.

2.6.1 WAYS OF ADDRESSING THE AUTHENTICATION PROBLEM

So, how can Web sites choose an authentication policy? There is no one right answer. In this section we look at two case studies to identify ways in which commercial Web sites might strike a balance in addressing the authentication problem. Often, the solutions chosen will depend on the Web site's relationship with the consumer, as well as the kind of data to which access is provided.

Account Subscribers. Perhaps the fewest difficulties arise where a subscriber establishes an account with a Web site. In many cases, the individual may be given access to information about his or her account if he or she simply provided only the information required to establish and secure the account. But relying on information such as name, address and phone number to authenticate the identity and authorization of an account holder is risky because the information is so widely available. In fact, many of the most common "shared secrets" (such as social security numbers or mother's maiden name) have been so widely shared that it is hard to call them secrets any more.

For this reason, it is common practice both offline and online to require some additional piece of information that is thought to be more difficult to compromise. Many businesses require individuals to use a shared secret (password) to access an account.

Even a password requirement, with all its inconveniences and costs, may suffer from security flaws. Many consumers use the same password at multiple places, or leave themselves reminders on yellow stickies, or use obvious passwords that are easily guessed, for example, one of the most commonly used passwords is “password”. All of these risks can compromise the integrity of the authentication system. Authenticating identity has become a far more complex endeavor than it once was.

Even when an account already requires a password, it may be appropriate to require something more than the password before allowing access. This could be a physical object (something the consumer owns), or some unique physical attribute (e.g. some a biometric characteristic), or information passed to the consumer in a separate channel, such as a special code provided with the customer’s last statement or information about recent account activity.

We discussed the feasibility of using authentication devices as a method for obtaining consumer access to personal data. Some Committee members said that authentication solutions are available today that solve the password 'problem' described above. They pointed to hardware tokens that may be used like an ATM card and software tokens that can be downloaded to a PC, PDA or cell phone. Other members on the Committee argued that such solutions are still too costly or cumbersome and may not reliably prevent misuse and misappropriation.

Subscriber Access – An Authentication Case Study

A subscriber opens an email account with a free mail service. Establishing the email account does not require the subscriber to disclose personal information. However, the service uses preference data provided by the user to target advertisements. The subscriber is assigned an email address and asked to establish a password to protect the account. If the subscriber requests access to personal information held by the service, how should the service determine whether to authorize access? What level of authentication should be required?

Options:

a. Require the same information for access (account name and password). This approach errs on the side of ease of use for the account holder. But in doing so it relies upon one token (account name) that is frequently shared with others (email address for example) and another token (password) which is (as our discussions indicate) relatively easy to compromise.

b. Require account name, password, and some additional information (e.g., IP address). This approach provides additional protection against the compromise of the account password.

c. Require account name, password, and some dynamic information (e.g., information about recent account activity). This method adds some protection against unauthorized access. By asking for information that is dynamic and therefore less likely to be permanently compromised, it adds some additional protection.

d. Require any of the above sets of information and send the requested information to the account.

e. Require account name and password in order to trigger the sending of a one-time access code through a separate communication channel. The code would be used to gain access to the personal information. This approach would build in an additional precaution against unauthorized use. By requiring the request to come from the account (similar to credit card authorization that must come from the registered phone of the account holder) and returning a one-time access key to the account the system could further limit unauthorized access. This feature might cause a minor delay, but it does not require the individual to remember additional pieces of information.

Cookies, identifiers, and partially personalized data

A harder authentication problem arises if the Web site seeks to provide access to data that is not tied to an individual subscriber's account. Sometimes, data is gathered about a consumer's activities through the placement of a unique identifier such as "cookie" on the consumer's computer. But such data maybe only partially personalized -- the computer may have more than one user. The consequences of disclosing information about an individual's use of a Web site or clickstream data to another person (family member, co-worker, other) could be damaging.

The Committee notes that this problem is not limited to the online environment. Consumers are familiar with the problem in other contexts. To take one example, a home telephone number is only "partially personalized." It may be used by anyone who enters the house. Thus, an itemized phone bill may reveal information about one family member's calling behavior to another. For telephone billings, we accept over-disclosure. And despite nearly a century of experience with telephones and telephone billing, new privacy issues continue to arise in this context (e.g., disclosure of use of 900 numbers). Based on this experience, the problem of partially personalized information will remain a thorny one for the foreseeable future.

In such circumstances, how can a service authenticate that the individual is the person to whom the data relates? Can Web sites provide access in a fashion that reflects the potential adverse consequences of disclosing information to someone other than the subject of that information? Should the level of access authorized be lowered due to the complexities of connecting the user to the data? Are there other policies that would address the privacy interest and have a lower risk of unintentionally disclosing data to the wrong individual? Does this concern vary from Web site to Web site?

Again, there is no single answer to these questions, as our case study shows.

Cookies – An Authentication Case Study

A Web site assigns each visitor a unique identifier – a cookie – that is used to track and retain data about the visitor's activities at the site. The Web site does not request or gather information about specific visitor's identities. A visitor requests access to information that the Web site has about her use of the site. How should the Web site proceed?

Options:

a. **Require only the identifier (the cookie).** This would make it quite easy for the user to get access to personal data; but if the identifier is tied to an imperfect proxy for the individual (such as a computer) it is possible that other individuals may gain access to the individual's personal information. For this reason, the identifier alone may be insufficient to grant access, particularly when the information may be sensitive (visits to disease-specific medical sites, for example).

b. **Require the individual to open an account and allow access to data collected from this point forward**. This certainly sounds more secure, but it may not limit inappropriate access. For example, if the account is browser-based and there are several individuals who use the browser, unless special precautions are taken, this option could allow one individual to access all the data and prevent the others from accessing any.

b. Require the identifier but limit the scope of access. This option acknowledges the risk of inappropriate access and it seeks to mitigate the harm by limiting the information provided. For example, a Web site could provide categories of information it has collected rather than the actual information. (Note that at this point the Web site is providing something more like notice than access.).

c. Delete or disassociate the data from the requester's identifier This option provides something other than access. Where the data is maintained in the aggregate, this option recognizes the site's commercial interest in utilizing the data. Where deletion is provided, it protects the consumer's general interest in their privacy.

d. Require no identifier but provide only a general description of the kinds of data collected. This solution also provides notice rather than access. In response to an access request, it provides notice of the kinds of data that the site gathers.

3 SECURITY

We examined how to ensure the security of personal data held by commercial Web sites. This section first describes competing considerations in computer security. After then looking at some possibilities for regulating computer security in online systems, it discusses the importance of notice and education as supplements to standards for protecting personal data. It presents competing options for setting Web site security standards and recommends a specific solution to protect the security of personal data.

3.1 COMPETING CONSIDERATIONS IN COMPUTER SECURITY

Most consumers – and most companies – would expect commercial Web sites that collect and hold personal data to provide some kind of security for that data. Identifying the most effective and efficient solution for data security is a difficult task. Security is application-specific and process-specific. Different types of data warrant different levels of protection.

Security – and the resulting protection for personal data – can be set at almost any level depending on the costs one is willing to incur, not only in dollars but in inconvenience for users and administrators of the system. Security is contextual: to achieve appropriate security, security professionals typically vary the level of protection based on the value of the information on the systems, the cost of particular security measures and the costs of a security failure in terms of both liability and public confidence.

To complicate matters, both computer systems and methods of violating computer security are evolving at a rapid clip, with the result that computer security is more a *process* than a *state.* Security that was adequate yesterday is inadequate today. Anyone who sets detailed computer security standards – whether for a company, an industry, or a government body – must be prepared to revisit and revise those standards on a constant basis.

When companies address this problem, they should develop a program that is a continuous life cycle designed to meet the needs of the particular organization or industry. The cycle should begin with an assessment of risk; the establishment and implementation of a security architecture and management of policies and procedures based on the identified risk; training programs; regular audits and continuous monitoring; and periodic reassessment of risk. These essential elements can be designed to meet the unique requirements of organizations regardless of size.

In our advice to the FTC, we attempt to reflect this understanding of security. Our work, and this report, reflects the various types of on-line commercial sites, and the fact that they have different security needs, different resources, and different relationships with consumers. The report reflects this understanding and seeks to identify the range of different possibilities for balancing the sometimes-competing considerations of security, cost, and privacy.

3.2 DIRECTING COMPUTER SECURITY – PRELIMINARY CONSIDERATIONS

Before turning to the options, it is worthwhile to comment on several issues that we considered but did not incorporate directly into its list of options.

First, we considered whether self-regulatory guidelines or government-imposed regulations on security should contain some specific provision easing their application on smaller, start-up companies or newcomers to the online environment, but we ultimately determined that new entries should not receive special treatment when it comes to security standards. In part, this is because organizations that collect personal data have an obligation to protect that data regardless of their size. In part, this is because we concluded that any risk assessment conducted to evaluate security needs should take into account the size of the company (or, more appropriately, the size of a company's potential exposure to security breaches). In many cases (but not all), a smaller Web site or less well-established company will have fewer customers, less data to secure, and less need for heavy security. A smaller site may also have an

easier time monitoring its exposure manually and informally. And of course, even a small site may obtain security services by careful outsourcing.

Second, we noted that several of the proposed options depend on, or would be greatly advanced by inter-industry cooperation and consultation on appropriate and feasible security standards. Often, there are significant barriers to sharing information about adverse events, including fears of anti-trust actions and liability exposure. In the past, the government's willingness to provide clarity on anti-trust rules to allow useful cooperation among firms has been helpful. Similar guidance that will encourage industry members to cooperate in the development or enforcement of security standards and procedures without fear of anti-trust liability will be helpful here.

Third, it is vital to keep in mind that companies need to protect against internal as well as external threats when considering solutions designed to secure customers' personal data. Many companies have already implemented information security policies that protect sensitive corporate data (i.e., compensation information) by limiting access to only those employees who need to know. Companies need to implement similar measures that protect customer data from unauthorized access, modification or theft. At the same time, mandated internal security measures can pose difficult issues. For example, it is not easy to define "unauthorized" employee access; not every company has or needs rules about which employees have authority over computer or other data systems. And many companies that have such rules amend them simply by changing their practices rather than rewriting the "rule book." Even more troubling is the possibility that internal security requirements that are driven by a fear of liability could easily become draconian – including background checks, drug testing, even polygraphs. We should not, without serious consideration, encourage measures that improve the privacy of consumers by reducing the privacy of employees.

Fourth, we are concerned about the risks of regulation based on a broad definition of "integrity." Some concepts of security – and some legal definitions – call for network owners to preserve the "integrity" of data. Data is typically defined as having integrity if it has not been "corrupted either maliciously or accidentally" [Computer Security Basics (O'Reilly & Associates, Inc., 1991)] or has not been "subject to unauthorized or unexpected changes" [Issue Update on Information Security and Privacy in Network Environments (Office of Technology Assessment, 1995, US GPO)]. These definitions, issued in the context of computer security rather than legal enforcement, pose problems when translated into a legal mandate. If integrity were read narrowly, as a legal matter, it would focus on whether a Web site has some form of protection against malicious corruption of its data by external or internal sources. If the definition is read broadly, it could lead to liability for data entry errors or other accidental distortions to the private personal information it maintains.

Authentication and authorization controls for access to information are integral parts of system security. To establish appropriate authentication and authorization, businesses must consider the value of the information on their systems to both themselves and the individuals to whom it relates, the cost of particular security measures, the risk of inside abuse and outside intrusion, and the cost of a security failure in terms of both liability and public confidence. This discussion of security pertains both to information in transition and information in storage.

3.3 NOTICE AND EDUCATION

After considerable discussion, the Committee has developed a wide range of possible options for setting standards for protecting personal data held by commercial Web sites. Before presenting these options, we will address two policy options that the group considered but determined were unsatisfactory on their own. While insufficient standing alone, we concluded that development of programs to educate consumers on security issues and a requirement that companies post notice describing their security measures are approaches that should be examined as possible supplements to some of the options in the Security Options below.

3.3.1 NOTICE

Notice is viewed as an appropriate tool for informing individuals about the information practices of businesses. It is critical to the consumer's ability to make informed choices in the marketplace about a

company's data practices. In the area of security, as in the area of privacy, there is not necessarily a meaningful correlation between the presence or absence of a security notice statement and the true quality of a Web site's actual security. A security notice could be more useful if it allows consumers to compare security among sites in an understandable way. Since it is difficult to convey any useful information in a short statement dealing with a subject as complex as the nuts and bolts of security, most such notices would be confusing and convey little to the average consumer. Further, providing too many technical details about security in a security notice could serve as an invitation to hackers. As was discussed at some length by the Committee, these considerations also mean that it is not possible to judge the adequacy of security at Web sites by performing a "sweep" that focuses on the presence or absence of notices.

Notice is important in triggering one of the few enforcement mechanisms available under existing law. If a posted notice states a policy at variance with the organization's practices, the FTC may exercise its enforcement powers by finding the organization liable for deceptive trade practices. But security notices are ineffective standing alone. At the same time, we believe that they could be useful in conjunction with one of the other options discussed in Section D. The form such notice should take will vary depending upon the option selected.

3.3.2 CONSUMER EDUCATION

In addition to notice, consumer education campaigns are also useful to alert consumers about security issues, including how to assess the security of a commercial site and the role of the consumer in assuring good security. Regardless of what security solutions the FTC decides to recommend, it would be extremely valuable for the FTC, industry associations, state attorneys general, and others to sponsor consumer education campaigns aimed at informing Internet users about what to look for in evaluating a company's security. In addition, no system is secure against the negligence of users, so consumers must be educated to take steps on their own to protect the security of their personal data.

3.4 OPTIONS FOR SETTING WEB SITE SECURITY STANDARDS

The Committee has identified two sets of options for those seeking to set security standards. In essence, these options address two questions: How should security standards be defined? And how should they be enforced?

The question of how security standards should be defined requires consideration of the parties responsible for the definition as well as issues of the scope and degree of flexibility and changeability of the standards. The entities that could be responsible for setting security standards explicitly include government agencies, courts, and standards bodies. Furthermore, it could be left up to Web sites themselves to develop security programs (perhaps with a requirement that each site develop some security program), or it could be left to market forces and existing remedies to pressure Web sites into addressing security at an appropriate level.

In this section, we set forth five options for setting security standards that fall along a continuum from the most laissez faire to the most regulatory. Each of the proposals reconciles the three goals of adequate security, appropriate cost, and heightened protections for privacy in a different manner. For each option, we have presented the arguments deemed most persuasive by proponents and opponents of the option.

3.4.1 SECURITY OPTION 1: RELY ON EXISTING REMEDIES

Before requiring any particular security steps, wait to see whether existing negligence law, state attorneys general, and the pressure of the market induce Web sites that collect personal information to generate their own security standards. It is worth noting that the insurance industry has started to insure risks associated with Internet security. The emergence of network security insurance may force companies to seriously address security issues, as the presence or absence of adequate security will be taken into account in the underwriting process utilized to determine rates for premiums.

Proponents of this approach would argue:

1. Consumers who suffer harm as the result of negligence can typically bring tort actions. There is no reason to think that consumers who are harmed by a breach would lack a remedy for any specific injury they may suffer.
2. Damages are often quantifiable (e.g., credit card charges or lost work time due to identity theft). And even when they are not quantifiable (disclosure of embarrassing medical data, for example), the problem is no more difficult for juries to resolve than similar intangible wrongs routinely resolved by juries today (e.g., libel damages or "false light" claims).
3. It is therefore reasonable to wait for such litigation and to correct any gaps that may emerge in the law when and if the lack of a remedy has been demonstrated.

Opponents of this approach would argue:

1. This approach does nothing proactive to advance good practices in the marketplace, and will result in a long delay before security issues are addressed and consumers are protected. Consumers are often the last to know about security breaches and have limited resources to bring court action on their own. It will take some time before litigation based on existing negligence law results in judgments. And it will take time for the market to respond to this, if that even happens at all
2. If relying on existing remedies fails to work, we will be in the same or worse position then as we are now, and many more consumers will have had their privacy violated due to security breaches.
3. In the meantime, businesses that would welcome guidance from experts may be left to flounder and face lawsuits because of a lack of awareness, even if they are well intentioned.

3.4.2 SECURITY OPTION 2: MAINTAIN A SECURITY PROGRAM

Require all commercial Web sites that collect personal information to develop and maintain (but not necessarily post) a security program for protecting customers' personal data. This option could take one of two forms:

The contents and methodology of the security program could be specified, and businesses could be required to post a brief notice indicating their compliance.

The requirement could be limited to a simple mandate that the Web site adopt a security strategy without specifying the details or requiring that it be posted.

Proponents of this approach would argue:

1. A security program is necessary for a commercial Web site of any size that collects personally identifiable information and wishes to keep the information confidential.
2. The scope of the program may vary depending upon the size of the company. In the case of a very small business, one person may be able to effectively handle security on a part time basis. However, just as marketing, human resources, and accounting are considered essential business functions for companies of any size, maintaining a security program is also critical to any company's operations.
3. Security professionals believe that any effective program, even if managed by only one person part time, should involve the elements of risk assessment, implementation of controls based on the risks, testing and monitoring of controls, and periodic re-assessment of risks.
4. A statement that the company maintains a security program that assesses risks and implements appropriate controls to address the risks need not be incomprehensible to consumers or too burdensome for businesses to comply with and insures consumers and businesses that security has been considered in the system design.

Opponents of this approach would argue:

1. Developing and maintaining a program -- but not testing it or otherwise verifying or assuring that the organization is complying with the program -- will only result in an illusion of security.

2. The costs of developing, testing, verification, and assurance (especially to small or not technically savvy businesses) will be significant, diverting resources from the main business purpose. Many firms would not know where to turn or how to take the first step in developing such a program.
3. If the plan description is posted, much of it may both be incomprehensible to non-technical users and all-too-clear to technically savvy attackers.

3.4.3 SECURITY OPTION 3: RELY ON INDUSTRY-SPECIFIC SECURITY STANDARDS

All businesses operating online that collect personal information could be required to adhere to security standards adopted by a particular industry or class of systems. There are three quite different options for how the standards are developed:

- A government-authorized third party could develop standards through a process that encourages public participation (notice and comment) and may include governmental review.
- The standards could be established by any third-party but the FTC or another applicable agency could require that the standards address specific topics (e.g. access, data integrity, notice, authentication, authorization, etc.).
- The standards could be developed by any third-party as long as the identity of the standard-setting organization is revealed to consumers (this is in effect a security "seal" program).

Proponents of this approach would argue:

1. No government agency is smart enough or fast-moving enough to set network security standards for a particular industry. Industry-specific standards should be set by industry because each sector has different computer security needs and methodologies.
2. Industry groups will have a strong incentive to avoid setting too low a bar. Every company with a brand name is held accountable for the products sold under that name. So too with security standards-setting organizations; those that are associated with serious security breaches will lose the confidence of the public.
3. The three options presented under this heading are quite different, and c) is significantly better than the others. It associates a security standard with a "brand name" so that consumers can decide whether security at the site is sufficient. Option b) simply adds a requirement that the standards address certain issues. In most cases this will be unnecessary and in other cases insufficient. Option a) requires that the government license standard-setting organizations; it also requires notice and comment and perhaps government review for such standards. This option is nearly indistinguishable from requiring government-written standards and will require that the FTC or some other body make hundreds if not thousands of individualized decisions about what security practices should be required in which industries, decisions that will have to be remade every three months as security standards and challenges evolve.

Opponents of this approach would argue:

1. Allowing industry to develop (and police) itself invites lax standards and under-enforcement. Self-regulatory organizations that are comprised solely of the industry at issue will not develop robust standards because doing so may subject its members to additional implementation costs and expose them to greater liability.
2. The insular nature of the standard setting process does not adequately assess and address the needs and values of other parties – other industries, the public, and policy makers. In the absence of other stakeholders industry will fail to address important concerns or craft proposals that undercut other important public policies.
3. The standard setting process lacks public accountability. It is inappropriate to develop substantive policy through entities and processes that lack institutional mechanisms for ensuring public accountability and oversight.
4. Opponents will find that options a-c do not address their general concerns with industry-generated standards. However, opponents may find that proposal "a" partially responds to criticisms 1 and 2

because it constructs a process for soliciting public and policy maker input and review and to a limited extent addresses concerns about industry capture and stakeholder participation. However, because it does not permit other stakeholders to participate in the formulation of the standards, it is unlikely to fully ameliorate these concerns. In addition, since the item to be protected, personal information, is likely to be considered less valuable by the business than individuals, the concern about lack of representation is heightened. Opponents may find that proposal "b" (while weaker than "a") provides some restraint on the standard-setting process by allowing outside interests to decide what issues must be addressed. Option "c" will garner the greatest opposition from opponents as it fails to address any of the concerns outlined above.

3.4.4 SECURITY OPTION 4: "APPROPRIATE UNDER THE CIRCUMSTANCES" - STANDARD OF CARE

Require all commercial Web sites holding personal information to adopt security procedures (including managerial procedures) that are "appropriate under the circumstances." "Appropriateness" would be defined through reliance on a case-by-case adjudication to provide context-specific determinations. As the state of the art evolves and changes, so will the appropriate standard of care. An administrative law judge of the FTC or another agency or a court of competent jurisdiction could adjudicate the initial challenge.

Proponents of this approach would argue:

1. This approach allows for an assessment of security tied directly to considerations of circumstance and knowledge. It is impossible to summarize in any detail the balance that must be struck between security and usability; even for the most sensitive data, such as medical information, it may be necessary to lower security standards in order to assure prompt treatment for the injured.
2. The creation of a general standard that is informed by the security practices of others similarly situated at a certain date and time allows for flexibility and growth while encouraging ongoing progress. A similar approach is found in judging medical treatment – doctors are not regulated by an elaborate rulebook but rather by the requirement that they practice medicine in accordance with accepted professional standards. The law leaves definition of those standards to the particular case.
3. This approach is designed to encourage increasingly strong security practices. If a bright line rule is adopted, there is little doubt that the pace of technical change will leave the adequacy of regulation in the dust, and what was intended to be a regulatory floor will become a ceiling in practice. Rising tides do raise all boats, except those that are anchored to the bottom.

Opponents of this approach would argue:

1. In the absence of clear minimum-security standards, courts and companies will lack guidance, because there are no universally accepted security standards.
2. For consumers, the absence of any clear definition of what is sufficient security may put their personal information at risk from companies who do not share the same risk assessment about what is "appropriate under the circumstances."
3. For commercial Web sites, there are also disadvantages to this approach; their security precautions will not be judged until after a breach has occurred, which means that the precautions are more likely to be viewed as inadequate in hindsight.
4. An after-the-fact security standard could lead many Web sites to ignore security until they are sued.

3.4.5 SECURITY OPTION 5: REQUIRED SLIDING SCALE OF SECURITY STANDARDS

Require commercial Web sites that collect personal information to adhere to a sliding scale of security standards and managerial procedures in protecting individuals' personal data. This scale could specify the categories of personal data that must be protected at particular levels of security and could specify security based upon the known risks of various information systems. In the alternative or as part of the standard, there could be minimum-security standards for particular types of data. The sliding scale

could be developed by a government agency or a private sector entity and could incorporate a process for receiving input from the affected businesses, the public, and other interested parties.

Proponents of this approach would argue:

1. A sliding scale allows for the matching of consumer protection risk to data source, thereby allowing companies to develop a more efficient compliance and technology infrastructure.
2. A sliding scale provides commercial flexibility in the way Web sites comply with security standards.

Opponents of this approach would argue:

1. This option will embroil the agency or private sector entity in trying first to gauge the sensitivity of numerous, different types of data and then to match the sensitivity with particular security measures. It is an impossible task, and the results will be a mess.
2. If the sliding scale is produced at a high level of generality, it will be unenforceable and probably incomprehensible; if it is made specific enough to enforce, it will be a straitjacket for many businesses and a series of loopholes for others.
3. Even if it could be prepared properly the first time, a sliding scale would have to be updated almost constantly, tasks for which bureaucracies are illsuited.

3.5 SECURITY RECOMMENDATION

The great majority of the Committee believes that the best protection for the security of personal data would be achieved by combining elements from Options 2 and 4. (Of course, existing remedies would not be supplanted by this solution.) We therefore recommend a solution that includes the following principles:

- Each commercial Web site should maintain a security program that applies to personal data it holds.
- The elements of the security program should be specified (e.g., risk assessment, planning and implementation, internal reviews, training, reassessment).
- The security program should be appropriate to the circumstances. This standard, which must be defined case by case, is sufficiently flexible to take into account changing security needs over time as well as the particular circumstances of the Web site -- including the risks it faces, the costs of protection, and the data it must protect.

4 OTHER CONSIDERATIONS NOT FULLY ADDRESSED

4.1 ENFORCEMENT ALTERNATIVES

The Committee was asked to provide its views on access and security in the context of the Fair Information Practice principles and industry self-regulation. We did not examine legislative or enforcement options in any detail, but it was difficult to address some of the access and security issues without giving some thought to the question of enforcement. As part of the security discussion, in particular, we assembled a range of representative options for enforcement of security principles. Some of these options are consistent with self-regulation, and others would require government intervention. We record them here, not for the purpose of recommending any particular course of action but to show the range of possibilities open to industry and government.

Rely on Existing Enforcement Options - Many of the options include the publication of the Web site's security procedures or its adherence to particular standards. Such postings are subject to traditional FTC and state enforcement if the statements are false. It is also of course possible for consumers to bring their own actions for fraud, false statements, or underlying negligence in the handling of the data.

Third-Party Audit or Other Assurance Requirements - Rely on independent auditors to ensure compliance with standards. This structure could require security standards to be verified by an external body and public disclosure of the findings. This option would provide more flexibility and could adjust faster to the changing threat environment. It would, however, introduce an additional cost and overhead that may not be justified by all industries and for all levels of risk exposure. It might, on the other hand, introduce a neutral, objective assessment of a company's security infrastructure relative to its industry.

Create Express Private Cause of Action - Congress could establish a private right of action enabling consumers to recoup damages (actual, statutory, or liquidated) when a company fails to abide by the security standard established through one of the options set out above.

Government Enforcement Program - The FTC or another agency could enforce compliance with standards using its current enforcement power or using newly expanded authority. The enforcement could establish civil or criminal fines, or both and other equitable remedies. (This option is, in some respects, modeled after the regulations governing the financial services industry as enforced by the Federal Financial Institution Examination Council (FFIEC). The FTC could establish a similar enforcement regime for other industries.)

4.2 ADVANCING TECHNOLOGIES

We live in the middle of an information revolution where new opportunities for the use as well as the protection of personal data appear daily. Significant new technologies raise questions about privacy that will have to be addressed. For example, with new wireless technology, a unique identifier heretofore not linked to a specific individual may now be linked to an individual identified with a phone number, location information, or other identifier. And wireless communications can be intercepted in an undetectable manner. Similarly, communicating appliances will have the potential to share personal data that may be linked to an individual.

The privacy implications of new technologies may be profound. We have attempted to pro vide options and our recommendation in a manner independent of these new technologies. However, the FTC will have to monitor developments in these areas closely to stay abreast of the privacy and security implications that new technologies may bring.

4.3 SECURITY INCIDENT DATA – INDUSTRY SHARING WITH THE GOVERNMENT

None of the security options discussed by the Committee addressed the issue of industry sharing security incident data with the government. However, during a Committee meeting this issue was raised. Because this issue is not raised by the security options, the Committee did not examine the question of

whether or not the Freedom of Information Act (FOIA) is a barrier to the sharing of security incident data between industry and government. The Committee expresses no opinion on this issue.

4.4 Regulatory Standards – Extant and Emerging

The Committee recognized at several points in its discussions that for some industries, standards for access and security may be set by government regulatory bodies charged with supervision of a given sector (e.g. the Comptroller of the Currency or the Federal Reserve for the financial services industry). The Committee did not examine such standards in detail.Non-Profit & Government Web Sites

4.5 Non-Commercial and Government Web Sites

The Charter of this Committee limits our responsibilities to considering the practices of "domestic commercial Web sites." However, there was considerable sentiment among the members that access and security issues are hardly limited to commercial sites. Non-profit organizations that run sites for commercial purposes, government sites and others were cited as those with enough similarity to commercial sites that their practices should be subject to the same scrutiny and potential production of advice and recommendations for alteration or improvement of practices. For these reasons, we recommend a careful consideration of the issues raised in this report by non-profit organizations and government agencies.

5 CHARTER OF THE FEDERAL TRADE COMMISSION ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY

Official Designation

The Federal Trade Commission Advisory Committee on Online Access and Security

Scope and Objectives

The purpose of the Advisory Committee is to provide advice and recommendations to the Commission regarding implementation of certain fair information practices by domestic commercial Web sites - specifically, providing online consumers reasonable access to personal information collected from and about them and maintaining adequate security for that information. The Advisory Committee will consider the parameters of reasonable access to personal information and adequate security and will present options for implementation of these information practices in a report to the Commission.

The Advisory Committee will consider, among other things, whether the extent of access provided by Web sites should vary with the sensitivity of the personal information collected and/or the purpose for which such information is collected; whether the difficulty and cost of retrieving consumers' data should be considered; whether consumers should be provided access to enhancements to the personal information obtained directly from them, such as inferences about their preferences and information about them derived from other databases; appropriate and feasible methods for verifying the identity of individuals seeking access; whether a reasonable fee should be assessed for access, and if so, what a reasonable fee would be; and whether limits should be placed on the frequency of requests for access, and if so, what those limits should be.

The Advisory Committee will also consider how to define the standards by which the adequacy of measures taken by Web sites to protect the security of personal information collected online may be judged; what might constitute reasonable steps to assure the integrity of this information; and what managerial and technical measures should be undertaken to protect this information from unauthorized use or disclosure.

Duration

The Advisory Committee will conduct its work from February 4, 2000 through May 31, 2000.

Reporting Relationship

The Advisory Committee will report to the Designated Federal Officer, David Medine, Associate Director for Financial Practices, Bureau of Consumer Protection, Federal Trade Commission.

Support

The Federal Trade Commission will provide the necessary support services for the Advisory Committee, including a court reporter, transcripts of meetings, and photocopying.

Duties

The duties of the Advisory Committee will be solely advisory. The Advisory Committee will provide advice and recommendations in the form of a written report to the Commission describing options for implementing reasonable access to, and adequate security for, personal information collected online, and the costs and benefits of each option, by May 15, 2000.

Costs

The operating cost of supporting the Committee's functions is estimated to be $138,000. Members of the Advisory Committee will not be compensated, and must bear the cost of their own travel-related expenses. It is estimated that 1.5 FTE will be required to support the Committee.

Meetings

It is anticipated that the Advisory Committee will meet four times. Subgroups of the Advisory Committee will likely meet more frequently.

Date of Termination

The Committee will terminate on May 31, 2000.

Charter Filing Date

January 5, 2000.

By direction of the Commission.

Donald S. Clark
Secretary of the Commission

6 APPENDIX B: ADVISORY COMMITTEE MEMBERS

Mr. James C. Allen
eCustomers.com

Stewart A. Baker, Esq.
Steptoe & Johnson LLP

Mr. Richard Bates
The Walt Disney Company

Ms. Paula J. Bruening
TRUSTe

Mr. Steven C. Casey
RSA Security, Inc.

Fred H. Cate, Esq.
Indiana University

Mr. Jerry Cerasale
Direct Marketing Association, Inc.

Steven J. Cole, Esq.
Council of Better Business Bureaus, Inc.

Dr. Lorrie Faith Cranor
AT&T Labs-Research

Dr. Mary J. Culnan
Georgetown University

Mr. E. David Ellington
NetNoir, Inc.

Ms. Tatiana Gau

America Online, Inc.

Alexander C. Gavis, Esq.
Fidelity Investments

Dr. Daniel E. Geer
@Stake, Inc.

Mr. S. Rob Goldman
Dash.com, Inc.

Mr. Robert D. Henderson
NCR Corporation

David Hoffman, Esq.
Intel Corporation

Dr. Lance J. Hoffman
George Washington University

Mr. Josh Isay
DoubleClick, Inc.

Mr. Daniel Jaye
Engage Technologies, Inc.

Dr. John Kamp
American Association of Advertising Agencies

Mr. Rick Lane
U.S. Chamber of Commerce

James W. Maxson, Esq.
Paul, Hastings, Janofsky & Walker

Mr. Gregory Miller
MedicaLogic, Inc.

Deirdre Mulligan, Esq.
Center for Democracy and Technology

Deborah Pierce, Esq.
Electronic Frontier Foundation

Ronald L. Plesser, Esq.
Piper, Marbury, Rudnick & Wolfe LLP

Dr. Lawrence A. Ponemon
PricewaterhouseCoopers, LLP

Mr. Richard Purcell
Microsoft Corporation

Mr. Arthur B. Sackler
Time Warner, Inc.

Dr. Daniel Schutzer
Citigroup

Mr. Andrew Shen
Electronic Privacy Information Center

Mr. Richard M. Smith
Internet Consultant

Dr. Jonathan M. Smith
University of Pennsylvania

The Honorable Jane Swift
The Commonwealth of Massachusetts

James E. Tierney, Esq.
Consultant

Frank C. Torres III, Esq.
Consumers Union

Mr. Thomas Wadlow
Pilot Network Services, Inc.

Mr. Ted Wham
Excite@Home Network

Ms. Rebecca Whitener
IBM Corporation