

Online Access & Security Committee
Access Subgroup One:
Degree of Access, and Terms & Conditions of Access

I. Degree of Access (what information, if any, should consumers have access to)

a) **Categories of Personal Information** - The Subgroup has organized policy options by several different data categories previously discussed by the Online Access & Security Committee (OA&S Committee). These policy options are followed by arguments in favor and against providing consumer access to the specified data category. By breaking down the policy options in this manner, the Subgroup decided to provide a very inclusive range of options that could be explored by the full OA&S Committee. The categories are: non-personally identifiable information (non-PII), non-PII that may be linked to PII, account & transactional data, interactive data, computer information (including IP number, GUID or LUID, cookies, etc.), navigational or click stream data, derived data, PII merged from other databases, distribution of data, and all PII. After each of the categories are discussed, two overarching general policy options about the scope of access are listed: whether or not consumers should have access only to certain categories or information, and whether or not consumers should have access to all information that is collected about them. Finally, the Subgroup included two policy options regarding data relevancy and data retention.

- i) **NON-PII.** Companies should not have to provide access to non-personally identifiable information (non-PII).
 - (1) Pros
 - (a) Reduces costs to businesses
 - (b) Non-PII poses a limited threat to privacy
 - (c) Access to non-PII might otherwise create an incentive to aggregate PII with non-PII (thereby creating an incentive to sell or disclose such information)
 - (2) Cons
 - (a) Non-PII may pose a threat to privacy
 - (b) Non-PII may be linked to PII information by others

- ii) **NON-PII LINKED TO PII.** Companies should not have to provide access to non-PII, as long as such information is not linked to PII. Once linked, consumers should be provided access to this information.
 - (1) Pros
 - (a) Reduces costs to businesses
 - (b) Non-PII poses a limited threat to privacy
 - (2) Cons
 - (a) Companies may not know when some information is linked
 - (b) Imposes responsibilities on companies to follow data
 - (c) By definition, when non-PII data is merged with PII, that data can become PII.

iii) **ACCOUNT & TRANSACTIONAL DATA.** Companies should provide access to account and transactional data (a subset of interactive data)

(1) Pros

- (a) Increased reliability and accuracy of data
- (b) Increases consumer trust and confidence
- (c) May limit information asked to be provided
- (d) Deeper customer relations
- (e) Limit the proliferation of bad data
- (f) Competition advantage versus companies with poor access policies
- (g) Public relations benefit
- (h) Increased customer market

(2) Cons

- (a) Increased business costs (see original access #3 for costs)
- (b) Access implies correction
- (c) Potential legal liability
- (d) Increases security threats

iv) **INTERACTIVE DATA.** Companies should provide access to all interactive data (data actively generated from or reflecting explicit transactions with a service provider through a site – such as queries to a search engine, responses to surveys, logs of account activity, or purchases made)

(1) Pros

- (a) Access to interactive data demonstrates the give and take of the particular experience of the consumer with the company

(2) Cons

- (a) Will present additional costs
- (b) Showing one side of an interaction may be like recording half of a telephone conversation
- (c) Showing both the consumer side and company side of a transaction may pose proprietary considerations
- (d) Extremely difficult to administer by companies, particularly with decentralized data collection systems
- (e) It is difficult to define “derived data” (e.g. does it include inferred and observational data?)

v) **COMPUTER INFORMATION.** Companies should provide access to computer information (including IP number, domain name, browser type, and operating system), GUIDs and LUIDS, and information contained in state management systems (such as cookies)

(1) Pros

- (a) Consumers will know what companies are storing on their computers
- (b) Consumers will know the extent of tracking or profiling by companies

- (c) Such information may be used to target certain consumers
 - (d) If companies are required to provide access to such information, they may be less likely to collect and store such information if they don't have a reason to do so. Dissemination of such data may pose security threats in the future (older less secure systems / operating programs).
- (2) Cons
- (a) Such information poses limited privacy threat
 - (b) Consumers often can find out this information on their own
 - (c) May increase security risks
 - (d) May force companies to store such information in a way that is identifiable by name
 - (e) Content may not be understandable to a consumer without a lot of explanation
 - (f) Companies may incur additional costs in translating such information into a readable format
 - (g) Translation may pose additional privacy threats
 - (h) Costly and difficult to administer
- vi) **NAVIGATIONAL OR CLICK STREAM DATA.** Companies should provide access to navigation or click stream data
- (1) Pros
- (a) Consumers are worried about being tracked
 - (b) Access may provide incentives for companies to eliminate unnecessary tracking
- (2) Cons
- (a) Potential cost of providing access
 - (b) May affect web software architecture design
- vii) **DERIVED DATA.** Companies should provide access to derived data about consumers
- (1) Pros
- (a) Derived data may have a life impact
 - (b) Derived data shows what is truly being communicated about consumers
 - (c) Consumers may expect to know why decisions are being made about them
 - (d) Access to derived data may limit incentives for companies to "redline" groups of customers
- (2) Cons
- (a) Derived data may include proprietary information
 - (b) Companies should be able to make private decisions about who they target for marketing, etc.
 - (c) May increase litigation
 - (d) Very difficult to administer, particularly where there is qualitative data/information

- viii) **PII MERGED FROM OTHER DATABASES.** Consumers should be given access to all PII merged from other databases
 - (1) Pros
 - (a) Consumer profiles pose a unique privacy threat
 - (b) Potential life impacting decisions made with merged data
 - (c) Data may be acquired by subpoena
 - (2) Cons
 - (a) Companies sell such information as a product

- ix) **DISTRIBUTION OF DATA.** Host companies should give consumers access to all recipients of data transferred by that host company
 - (1) Pros
 - (a) Informs consumers of likely users of data
 - (b) Informs consumers of likely uses of data
 - (c) Provides an efficient audit mechanism for consumers (a road map for consumers)
 - (2) Cons
 - (a) Brings into question what responsibilities host companies have for information practices of data recipients
 - (b) Difficult to decide how far the data trail should be traced by the host company
 - (c) Raises issues whether or not host companies must disclose data transmissions to affiliated companies

- x) **ALL PII.** Should companies provide consumers access to all PII
 - (1) Pros
 - (a) Gives consumers the greatest access rights
 - (b) Helps ensure accuracy of data
 - (c) Likely to promote consumer confidence in privacy of personal information
 - (d) Competitive advantages versus companies with poor access policies
 - (2) Cons
 - (a) Likely to increase costs
 - (b) May require consumers to provide more information to gain access to PII in some circumstances
 - (c) Security concerns / need to enhance authentication to ensure appropriate access
 - (d) Potential centralization / linkage of data that may not have been linked otherwise

- b) ***Overall Policy of Basing Access Upon Categories.*** After a discussion of the pros and cons of providing access to individual categories, the Subgroup decided to discuss the “category” approach generally.
 - i) **ACCESS BASED UPON CATEGORIES.** Companies should provide different access rights depending upon the type or category of information.

- (1) Pros
 - (a) Not providing access to all information may reduce costs
 - (b) Limiting access to some types of information may pose less of a security threat
 - (c) Limiting access to some types of information may pose less of a threat to proprietary information
 - (d) Some information may not be usable by the average consumer
 - (e) May reduce potential liability
 - (f) May reduce consumer confusion with clear categories/standards and rights attached.
- (2) Cons
 - (a) Consumers may want to see all information collected about them
 - (b) Companies may be able to manipulate categorical definitions to limit access rights
 - (c) Consumer ability to correct / delete information may be limited
 - (d) Consumer awareness and trust may not be enhanced to the fullest extent
 - (e) Companies may not limit their data collection as much

c) **Overall Policy of Providing Access to All Consumer Information.** The Subgroup noted that a logical alternative to discussing access based by category is simply to allow consumers to have total access to all information (PII, non-PII, etc.) that is collected about them, regardless of category. This approach would likely encompass all of the costs and all of the benefits associated with each of these categories. Reference is made to the costs and benefits outlined by the original access costs and benefits subgroup (subgroup # 3).

i) **TOTAL ACCESS RIGHTS.** Consumers should be provided access to all information that is kept on them.

- (1) Pros
 - (a) Benefits to consumers (See original access subgroup #3)
 - (b) Benefits to businesses (See original access subgroup #3)
- (2) Cons
 - (a) Costs to consumers (See original access subgroup #3)
 - (b) Costs to businesses (See original access subgroup #3)

d) **Data Relevancy Issue.** The Subgroup discussed whether or not those who collect data should question why they are collecting the information in the first place. One member queried: is it being collected because the technology makes it easy to do so and so “more is better”, or because the information is relevant to the purpose for which it has been acquired.

i) **DATA RELEVANCY.** Companies should limit the collection of information to what is relevant to the purpose for which it has been acquired or as required by statute or regulation

- (1) Pros
 - (a) This may translate into cheaper costs for the company collecting the information

- (b) May increase consumer confidence that companies are protecting privacy by limiting information collection
 - (c) Less information stored poses less of a danger of incorrect information
 - (2) Cons
 - (a) One piece of information may have many purposes
 - (b) Companies may define their purposes for collection very broadly to avoid any uses being questioned
 - (c) Relevance is difficult to define
- e) **Data Retention Issue.** The inclusion of data retention options were also discussed by the Subgroup for many of the same reasons as data relevancy. The question is whether information that is less current should have an “expiration” date on it. Information can become stale and out of date. The Subgroup debated whether or not procedures should be put in place for the destruction of such information.
- i) **DATA RETENTION.** Companies should delete information after a specified period of time or as allowed by regulation.
- (1) Pros
 - (a) If there is a set end date for information that has been gathered, the information is more likely to remain current / accurate
 - (b) If old information is periodically destroyed, less likely to have negative consequences for consumers
 - (c) This may translate into cheaper costs for the company storing the information
 - (d) May increase consumer confidence that companies are protecting privacy by limiting information stored
 - (2) Cons
 - (a) Difficult to decide how long information is necessary across different industries
 - (b) Many companies are required to store information for regulatory and auditing purposes
 - (c) Companies may need such information to protect themselves from persons questioning their information practices
- f) **Access Depending Upon Use / Purpose of Information.** In keeping with an opinion raised by an earlier subgroup and by the OA&S Committee, the Subgroup strongly believes that the use of information should be an integral part of considerations of access. Of particular concern is individuals' ability to access information used to make decisions about them, and questions of commingling data from various sources.
- i) **PURPOSE BASED ACCESS.** Consumer access should depend upon the purpose for which the information will be used
- (1) Pros
 - (a) Access for some purposes may already be covered under current law (e.g. FCRA)

- (b) If consumers make a decision that information sharing in notice is okay, access serves less of a purpose
- (c) Access could depend upon the type of decision a company will make about the consumer
- (d) Access could depend upon the likely consequences of any adverse decision

(2) Cons

- (a) Consumers will not be able to check whether information is used for its stated purpose
- (b) Places more of a burden on self-regulation organizations or government to verify if companies are doing what they say
- (c) Difficult to define for which purposes access is required
 - (i) Information used to determine eligibility for credit, employment, or insurance
 - (ii) Information used to decide whether or not a service is offered
 - 1. Pros - Consumers will know why they are rejected
 - 2. Cons- Companies may have a right to make these decisions privately
- (d) Consumer access should be independent of purpose.

- ii) **ACCESS LIMITATIONS.** Consumers should not have access to information that is used for internal purposes such as auditing, billing, fraud detection, etc.

(1) Pros

- (a) Consumers may not expect to access such information

(2) Cons

- (a) Consumers may want access to such information
- (b) Such information could be further disseminated

g) ***Who Decides the Scope of Access Rights / Sensitivity of Consumer Information.***

The Subgroup believes that it is important for the full OA&S Committee to consider what type of access rights should be provided. However, the Subgroup was left with the question of who most appropriately should make decisions about what personal information is important to access. One option discussed was providing consumers the ability to decide what information they want to access. The other option was allowing some other entity (industry, self-regulatory organization, or government) to decide what information is most important, or most “sensitive.” Under this option, companies could feasibly provide access to all “sensitive information” while limiting access to other non-sensitive information. Both approaches lead to numerous questions.

- i) **CONSUMER CHOICE.** Consumers should be able to choose what personal information they can access.

(1) Pros

- (a) Consumers would be able to decide for themselves what information they wish to access

- (b) Consumers might limit their access requests to only that information which is important to them, reducing the overall volume of responses to access requests
- (2) Cons
 - (a) Allowing consumers to decide what they can access creates a major database architecture problem.
 - (b) Consumers may not understand the range of information collected about them and therefore may not ask for all categories of information that they would otherwise find important
- ii) **NON-CONSUMER DEFINED ACCESS**. Companies should provide access to all “sensitive data,” as defined by the industry, self-government organization, or government
 - (1) Pros
 - (a) Sensitive data poses greatest privacy threat
 - (b) Consumers want to ensure accuracy
 - (c) Data may have an impact on life impacting decisions
 - (d) Access may already be proscribed under existing law
 - (i) European Union Directive
 - (ii) Fair Credit Reporting Act
 - (2) Cons
 - Difficult to define “sensitive data”
 - (i) EU definition (financial, health, religious, sexual)
 - (ii) Definition proposed by original Access Group #4
 - 1. Publicly available
 - 2. Available to the casual observer
 - 3. Known to close acquaintances
 - 4. Privileged information
 - (b) Sensitivity may depend upon use
 - (c) This will result in increased costs that may be spread among all consumers.
 - (d) Sensitivity standards are subjective and would be difficult to define, possibly resulting in differing standards across industries



II. Terms and Conditions of Access

- a) **Access Fees.** The Subgroup decided to discuss the range of fee options for providing access: from providing access for free to charging consumers for the actual costs of providing access. The Subgroup recommends that the OA&S Committee look to existing regimes, such as the Fair Credit Reporting Act and the BBB Online policies, to help frame the debate.
- i) **FREE ACCESS.** Consumers should be provided access for free at all times
- (1) Pros
- (a) Consumers may not otherwise exercise choice
 - (b) Businesses may limit costs by limiting the amount of information collected
- (2) Cons
- (a) Access results in costs – some should be borne by consumers (Free access may result in higher product costs and indirectly affect all customers; ie., a few inquiry-happy customers may drive up costs for all customers)
 - (b) Repeated access may be either frivolous or a purposeful attempt to hurt a business (this will drive up costs)
- ii) **FREE ACCESS INVOLVING CREDIT, EMPLOYMENT, OR INSURANCE.** Consumers should be provided free access whenever a credit, employment, or insurance decision is made about them
- (1) Pros
- (a) May be required under current law
 - (b) Consumers should have a right to see information that may not be correct
- (2) Cons
- (a) May force aggregation where it is not currently required
- iii) **FCRA BASED FEES.** Fees should be guided by a regime similar to the Fair Credit Reporting Act in some states
- (1) Pros
- (a) Providing initial free access would not discourage consumers from accessing information
 - (b) Charging a fee for requests thereafter may discourage frivolous requests
 - (c) Dollar limits under FCRA are reasonable for consumers
- (2) Cons
- (a) Companies may not be able to recoup access costs
 - (b) Free initial access may encourage too much access for businesses to cope with
- iv) **USER BASED FEES.** Fees should be user based fees similar to the BBB online practices
- (1) Pros

- (a) Would require some limitation on fees for consumers
 - (b) \$15 maximum fee may not be too burdensome
 - (2) Cons
 - (a) Companies still may not recoup costs
 - (b) Fees are not weighted by how much information is provided
- v) **ACTUAL COST FEES.** Companies should charge fees reflective of actual costs
- (1) Pros
 - (a) Businesses could recoup costs
 - (b) Could limit frivolous access requests
 - (2) Cons
 - (a) Could prevent consumers from exercising access
 - (b) Could become a disincentive to reducing access costs
- b) ***Frequency Limitations.*** The Subgroup seemed to be in agreement that overly repetitious access requests could result in needless costs to companies. However, the specifics of any particular limitations on access rights remain an item for consideration.
- i) **OVERLY REPETITIOUS REQUESTS.** Companies should be able to refuse access to overly repetitious requests
- (1) Pros
 - (a) Reduces costs
 - (b) Eliminates potential for abuse
 - (c) System performance for all users is degraded by overly repetitive / aggressive requests
 - (2) Cons
 - (a) How is overly repetitious defined, who defines it
 - (b) Companies could amend practices after request quotas are reached
- c) ***Temporal Limitations.*** While instantaneous access may be easiest for consumers, several members of the OA&S Committee indicated that providing instantaneous access to personal information may pose real costs on companies. Some information may be so sensitive that proper authentication of the requestor's identity may require delayed access.
- i) **REAL TIME ACCESS.** Consumers should be given real time access to information
- (1) Pros
 - (a) Consumers can instantly ascertain a company's information collection practices
 - (b) Consumers may gain confidence about the company they are doing business with immediately, promoting more commerce
 - (2) Cons
 - (a) Real time access poses tremendous costs
 - (b) Real time access poses increased security risks

- ii) **DELAYED ACCESS FOR SENSITIVE INFORMATION.** Companies should be able to provide access within different intervals based on the sensitivity of such information
 - (1) Pros
 - (a) Different time periods could provide greater security
 - (2) Cons
 - (a) Consumers may want information immediately to make online privacy choices

- iii) **ACCESS WITHIN A DEFINED REASONABLE PERIOD.** Companies should be able to provide access within a “reasonable period,” as defined by the industry, self-regulation organizations, or by the government
 - (1) Pros
 - (a) Reasonable period may give smaller businesses more time to comply based on their infrastructures (especially with legacy systems)
 - (b) Reasonable period is already a useable standard
 - (c) Reasonable period would be sensitive to how much information is to be accessed
 - (2) Cons
 - (a) Reasonable period doesn’t provide businesses with a clear standard
 - (b) Different persons may have different ideas of reasonableness

- d) ***Other Terms & Conditions.*** The Subgroup identified several other items that are important access considerations for consumers, including: how consumers can exercise their access options, how consumers should be notified of and explained their access options, and how personal information should be presented. Additionally, the Subgroup reviewed some issues that may be particularly important to some companies operating on-line, including: whether business shall be required to aggregate data for access when the data is being aggregated by another entity, how long companies shall store information to fulfill access requests, and whether or not companies should update older systems to allow for consumer access. Finally, the Subgroup reviewed different considerations that may be important to persons with disabilities.
 - i) **FORM OF ACCESS REQUESTS.** Companies should not require consumers to request access to online information through the mail or by telephone
 - (1) Pros
 - (a) Promoting online access is the easiest for consumers
 - (b) Consumers may otherwise not request access
 - (2) Cons
 - (a) Companies may want to make access to some types of information more difficult for security reasons

 - ii) **PROPER NOTICE.** Companies should clearly define terms and conditions of access in notices to consumers
 - (1) Pros
 - (a) Promotes consumer knowledge

- (b) Consumers would not otherwise know how to evaluate information that is accessed
 - (c) Promotes enforcement
- (2) Cons
 - Potential legal liability
- iii) **INFORMATION PRESENTATION.** Companies should provide information in a format that is easily understandable
 - (1) Pros
 - (a) Consumers may not otherwise be able to evaluate the information collected by them
 - (b) Companies might otherwise make information difficult to understand to reduce access requests
 - (2) Cons
 - (a) Translating information increases costs
 - (b) Difficult to define readability or understandability
- iv) **AGGREGATION FOR ACCESS.** Companies should not be required to aggregate data if it is not being aggregated by them or anyone who receives such information
 - (1) Pros
 - (a) Aggregation may pose additional privacy threats
 - (b) Aggregation imposes additional costs on businesses
 - (2) Cons
 - (a) Companies may limit consumer access to information that is used by others in aggregated form
 - (b) Difficulties in determining aggregation and who is aggregating
- v) **UPDATE OF LEGACY SYSTEMS.** Companies should modify “legacy systems” to reflect new access decisions
 - (1) Pros
 - (a) Avoids unfair advantages to companies that are not structured to provide access
 - (b) Consumer rights should not be determined by companies who choose adverse access policies
 - (2) Cons
 - (a) Modification of legacy systems may pose tremendous costs
 - (b) Marketplace forces may push companies into newer systems gradually
 - (c) Smaller businesses may not have the capital to modify systems, whereby larger business may
- vi) **STORAGE LIMITATIONS.** Companies should make all temporal information available to consumers
 - (1) Pros
 - (a) Companies may make decisions about persons based on information and then destroy such information

(b) Consumer access rights may be skirted by companies that destroy data quickly

(2) Cons

(a) Requiring companies to permanently store temporal data creates new privacy and security risks

(b) Longer storage of information may increase costs

(c) Difficult to define “temporal”

vii) **ACCESS FOR PERSONS WITH DISABILITIES**. Companies should provide special access policies for persons with disabilities

(1) Pros

(a) May be required under current law (reasonable accommodation)

(b) Promotes a societal good

(2) Cons

(a) May present additional costs