

**Request from the**  
**Public Relating**  
**to**  
**Online Behavioral Advertising**

## **Executive Summary**

Before one begins to answer complex questions such as what is needed to address the concerns and needs of an online community, and whether the proposed recommendations are enough to protect a consumer subject to online behavioral advertising, it is necessary to balance the consumer rights to both privacy and security along with the private industry rights to fair regulations. Consumers have a fundamental right to privacy and security (protection) of their personally identifiable information (PII) and every effort should be employed to ensure and enforce these rights, and in all forms of transmission. Honesty is crucial to the customer, and a necessary component of a good business relationship between an informed consumer and the company s/he chooses to do business with, and this relationship should be recognized as a privilege. Consumers have the right to be informed about their rights (up to and including information regarding their information privacy, security and enforcement) of inspection, review, and the correction of information found, and the ability to report violations and collect damages from any and all data breaches from the company and its affiliates. In addition, companies (and thus, industries) have a right to legitimacy, and fraudulent claims must be vigorously prosecuted.

While there exists a number of statutes, regulations and piecemeal laws concerning privacy and security in general, a further interpretation is necessary. Public trust, confidence and values must be tempered with government oversight, accountability and transparency. The problem posed by the Federal Trade Commission (FTC) is that of an information asymmetry. In any situation where one party has an information advantage over another, an information asymmetry is said to exist. To properly address this issue, a number of factors need to be considered, all of which fully engage the issue from all sides.

Already, the FTC has taken steps to address the problem. Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles<sup>1</sup> as well as the Dot Com Disclosures<sup>2</sup> were initial attempts to solve the problem. However, a more comprehensive set of principles or rules should be instituted to further elaborate on the initial conceptual framework established. The following set was developed and further elaborated upon by myself, a graduate student at the University of Michigan School of Information, and serves to further illustrate the need for a broad set of best practices that can be implemented not only within the online realm, but the private and public policy, business, and technology sectors as well.

1 - <http://www.ftc.gov/opa/2007/12/principles.shtm>

2 - <http://www.ftc.gov/bcp/online/pubs/buspubs/dotcom/index.shtml>

The five-point TOPAS<sup>(c) 2008</sup> framework I developed can be utilized to illustrate a robust, comprehensive, and holistic approach towards being able to resolve some of the ethical, legal, political, economical, technological, cultural, competitive, and social consequences of such policy actions. This framework is an acronym for Transparency, Oversight, Privacy, Accountability, and Security. It was developed to assist in assessing policy matters and allows a deeper level of analysis to get at the root of the issues, and can incorporate micro- and macro-analysis levels. What is really useful about the framework is that at any stage of evolution, a whole or parts of the policy, rule or guideline being considered can be readily analyzed for decision-making purposes. Any policy decision created for the benefit of the public should consider the public as their accountability standard and this should be explicitly stated.

#### TRANSPARENCY

Transparency is the two-way mirror model which allows internal and external parties to (re)view the information actions of one another. To protect civil liberties of the stakeholders, this model may benefit from filtering or screening mechanisms to avert or otherwise lessen the effects of full transparency when matters do not warrant such scrutiny. However, controls must be in place to ensure full access is restricted to those with a need-to-know. A minimization implementation is a method of averting full access in the absence of full scrutiny. In addition, issues of power and control can be mitigated by a combination of other models, namely, the oversight model. Full transparency, in of itself, is not useful to fully implement any policy action and must be carefully balanced with the remainder of the framework models. A good balance of full use of all models is needed to fully realize the benefits of the TOPAS<sup>(c) 2008</sup> framework of analysis.

#### OVERSIGHT

Oversight is the authoritative model which allows a party/parties an ability to provide checks and balances, or otherwise interpret and execute the information actions of another. By nature, this role is largely one of enforcement powers, but this effect can be mitigated by the accountability model. This model prevents any one entity from accumulating too much power or control, and ultimately, eliminates monopoly powers of any one entity.

#### PRIVACY

Privacy is the alternate side of the security model, and allows an ability of a party/parties to shield (or protect) one's information actions from another. This is largely a dual-role of each party involved and is therefore, the most broadly applicable model of the five. If privacy is seen as a fundamental or constitutional right, then it is a birthright of every human being. However, if seen as a policy matter, it is subject to the interpretation of the laws at that time. This is, arguably, also one of the most highly controversial models of the five. For the purposes of this model, privacy is ubiquitous and broader in nature than security.

#### ACCOUNTABILITY

Accountability, closely related to oversight, refers to the stakeholders who are affected by the information flows taking place between and among the parties. As such, due to guides, laws, directives, mandates, or regulations, this role may be somewhat mutable and slightly lower (or higher) than expectations due to the acuteness of stakeholder involvement. It can be said that this model follows that of a flowchart in many ways, outlining who is responsible for the actions of (an)other.

## SECURITY

Security is the alternate side of the security model, and as such, is but one half of the whole. This model indicates whether parties believe their information actions are protected from access or use by any others. Due to its wide applicability within the realm of critical information flows, it can be implemented in a wide variety of ways. This, however, can be mitigated by drafting policies that provide foundational guidance, based on best practices. Security could also be understood as narrower than privacy, and but one way to implement or attain private status, although many other options exist and could be substituted. For this reason, security is myopic but ever-important in policy matters.

While the aforementioned types of micro-analysis can be used within the framework, they are but one methodology of use; in fact, higher-level analysis could be done, as well. In fact, whole sections of policies, laws, guidelines, and reports could be dumped into the framework for analysis to find flaws and begin corrective actions. As an example, I took entire sections of the IRTPA law and input them into the framework. While this type of analysis is too broad for the purposes of this paper, it does serve to illustrate the framework is robust and scaleable to the needs of the audience. [Table B].

### The TOPAS<sup>© 2008</sup> Approach

The TOPAS<sup>© 2008</sup> approach seeks to be a holistic, comprehensive, and robust tool of analysis to discover discrepancies, strengths, and to identify flawed self-assessments and lessons learned through compare and contrast to understand, resolve, and respond to defective information flows for the purposes of public policy matters. Combined with a view of the micro-level and macro-levels described in Table A, it is useful and can be applied broadly or narrowly defined for analysis purposes.

MYOPIC	HOLISTIC
local or national approaches	global approaches
intra-agency communications (information flows)	inter- and intra-agency communications (information flows)
industry (domain) specific protections of information	adoption of best practices applied to <b>all</b> information flows

TABLE A – Micro- or Macro-Analysis

<b>TOPAS <small>(c) 2008</small> Framework</b>	<b>Policy, Law, or Guideline of Interest: Behavioral Guidelines</b>
TRANSPARENCY	Consumers want to know what is being done with all of their information being collected; want to know what is being collected and for what purpose(s) – what information is voluntary? what information is mandatory?
OVERSIGHT	Consumers want to know if they are able to find redress if any information is illegally obtained, and whom to contact for enforcement purposes if such breach occurs, along with contact information
PRIVACY	Consumers want to know that their information is being protected; some may want to know in what ways, and whether or not third-party affiliates who have been outsourced this information are their data stewards and thus, responsible for any inaccuracies, breach notifications, and enforcement action
ACCOUNTABILITY	Consumers need to feel that they are valued, and thus, there is a point of contact that is accountable to them if something goes wrong (along with that contact's information to reach them if they are harmed in any way – this is a single point of contact in the industry, or company*). The consumer must be made to feel as if their worth is valued and the industry or company is ultimately responsible to them.
SECURITY	Consumers want to know that all of their information is being protected, and why they should trust anyone other than the initial collector of their information with it

TABLE B – Perspective of the Consumer

<b>TOPAS <small>(c) 2008</small> Framework</b>	<b>Policy, Law, or Guideline of Interest: Behavioral Guidelines</b>
TRANSPARENCY	Industry wants to know if they are required to disclose all policies, procedures, or rules to the consumer and what information they can protect/filter/withhold legally
OVERSIGHT	Industry wants to know they are not being singled out and that each company is being treated equally, along with who(m) is/are the oversight agent(s), and what business practices are under scrutiny
PRIVACY	Industry wants to be able to protect their proprietary information/intellectual property and does not want to provide unnecessary information to oversight or accountability agents, including the customer as it may not included as a cost of doing business due to regulation/law/statutes/directives in place at the time of the request
ACCOUNTABILITY	Industry wants to know if they have an advocate who is accountable to them and perceives their interest as valued
SECURITY	Industry wants to protect their information that is collected legally, and wants to know if they can be assured of providing protection to customer data if they have followed appropriate laws, guidelines, rules, or directives

TABLE C – Perspective of the Industry

### ANALYSIS - Transparency

Of course, any policy that is implemented must take into account information from both the perspective of the consumer as well as industry. In this case, as in others, there are various motivations for the disclosure (or filtering) of information to suit different purposes. Under the transparency model of the framework, the consumer would like to be able to review all of the information being collected and for what purpose(s), while industry would like to retain some information as private, particularly if there are business practices that give them a competitive advantage to that proprietary information. For this reason, a transparency policy would seek to take a middle approach, giving neither side an information advantage over the other, and could look something like this:

#### Consumer -

Any information voluntarily provided will be collected for the purposes of \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_ by [company] and its affiliates: [named] who agree to provide this information upon request of the customer.

\_\_\_\_\_ is voluntarily collected, while \_\_\_\_\_ is mandatory information needed for business purposes.

Mandatory information collected is handled in this way: \_\_\_\_\_

#### Industry -

What information is absolutely necessary to provide to the customer and what information is exempt?

How often will we need to contact the customer should circumstances change?

Each industry and/or company would decide if there should be an opt-in or opt-out voluntary collection process by the consumer

### ANALYSIS – Oversight

While the consumer wants to know who is watching industry with their information, they also want to know who(m) and how to contact someone should harm befall them, industry wants to know if they are being treated fairly and what business practices are under scrutiny. For this reason, a policy that takes a middle ground approach and gives neither side an information advantage over the other may look something like this:

#### Consumer -

Should a breach occur, a consumer may contact [name], at this telephone number [ ], email [ ], fax [ ], and street address: [ ] who is responsible for the industry/company in question

Also, what constitutes the definition of breach in my state: \_\_\_\_\_

#### Industry -

Provide updates to consumers if laws have been changed from initial educational literature

What other industry statistics on this type of issue being analyzed?

What types of matters typically fall under business practices of interest for my industry?

### ANALYSIS – Privacy

The consumer wants to know if all of their information is being protected, while industry is concerned about minimization effects, and what is absolutely necessary protection measures that they need not disclose to the consumer (accountability) or oversight agents. Such a policy may look something like this:

Consumer -

What information do you protect (and in what ways) – [on the part of industry, this second part may be an opt-in for this information]

If you do not provide protection on behalf of your affiliates, why should I trust either of you with my information?

Industry -

[to the regulators] What is the minimal information that I must provide by law/regulation and under what circumstances am I responsible for affiliate mishandling of consumer information I/we provided? How often do I report this information to you, and whom do I contact if there are questions? [this should be a single point of contact, \*not necessarily a person, but perhaps an office or department]

ANALYSIS – Accountability

Consumer –

You are accountable to me, therefore, you will tell me if there are [any] problems with the handling of my information.

Industry –

[to regulators as oversight agents]: At what level(s) of mishandling of consumer information must I disclose to the consumer? For instance, would it be intrusive to consider every mishandling or just those that constitute the level of actual breach?

ANALYSIS – Security

Consumer -

Is all that the information I provide being protected equally, or are some forms of information protected differently, and do all of your affiliates provide the same level of protection? If not, why should I allow you access to all of my information (why should I do business with you...or them)?

Industry -

If I follow the rules, guidelines, directives, regulations, etc., am I liable for data breach? What about information I outsource or my affiliates; how responsible am I for their InfoSec practices?

A second level of analysis that can be taken could include a micro-analysis of the policies already proposed by placing them inside the framework to find inconsistencies or omissions. This analysis can provide another method to compare/contrast the principles being considered to see if all aspects of the framework are being utilized.

**TRANSPARENCY**

Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option; As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.

**OVERSIGHT**

FTC staff seeks additional information about the potential uses of tracking data beyond behavioral advertising and, in particular: (1) which secondary uses raise concerns, (2) whether companies are in fact using data for these secondary purposes, (3) whether the concerns about secondary uses are limited to the use of personally identifiable data or also extend to non-personally identifiable data, and (4) whether secondary uses, if they occur, merit some form of heightened protection.

PRIVACY	Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising. FTC staff seeks specific input on (1) what classes of information should be considered sensitive, and (2) whether using sensitive data for behavioral targeting should not be permitted, rather than subject to consumer choice.
ACCOUNTABILITY	Industries/Companies are accountable to their consumers, therefore, knowledge of business use of information collection is needed (notification, minimization, secondary use, non-disclosure, data accuracy, inspection & review; ongoing education; redress; and information security, integrity, and accountability)
SECURITY	Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need. FTC staff commends recent efforts by some industry members to reduce the time period for which they are retaining data. However, FTC staff seeks comment on whether companies can and should reduce their retention periods further.

### FULL ANALYSIS

The resolution of this problem is as any information asymmetry problem in that there must be incentives in place to ensure that consumers and industry are well protected from harm of the information they provide freely and voluntarily. There must be points of contact clearly identifiable and secondary means of contact available should there be questions; it should be clear what information provided is mandatory and what information is voluntary, and how these differ in level of Information Security, if any. It should be clear that trust is established between a company and its affiliates, as it is very difficult to prove a business case to a consumer if there is no assurance that the information being transmitted is being protected and secured in some reliable way. In addition, there must be an advocate on both sides of the matter to ensure no one side feels unduly pressured or ill-advised by the other. For this reason, there should be public debates on the merits of any of these issues where both sides can speak at length on the matter and dis/prove their points. Independent oversight is a key to this, as well as clear points of contact and enforcement agents for both parties.

Fair information practices can be used as a standard guide towards the methods in which information is handled, up to and including collection, storage, transmission, security, and secondary uses. Incentive-centered and user-centric design principles can also be put into place for both industry and the consumer to ensure that there is fair use of all information provided; no one wants to provide unnecessary information to anyone else. One incentive for industry/companies could be to provide some type of legal protection should breach occur, if these principles are in place and being used, while

for customers this could be a minimal allowable amount from which to sue (and whom to sue) should information be mishandled. Because we live in the age of information proliferation, it is necessary to provide some types of controls as to what is being collected; why it is being collected; who is collecting it; where it is being collected/stored, as well as duration; and perhaps, how it is being collected/protected. Gathering information from industry and consumers is a mandatory step towards finding relevant solutions to these problems.

Control of information is big business, and these questions must be answered in light of the tradeoffs that exist to satisfy the two sides of the issue. While it may be unrealistic to believe that both sides can be fully satisfied, the goal of completing an honest information analysis of the issue can be attained if we answer the questions using frameworks such as TOPAS<sup>(c) 2008</sup> to get at each of the issues at hand.