WORLD **PRIVACY** FORUM

Donald S. Clark
Office of the Secretary
Federal Trade Commission
600 Pennsylvania Avenue
Room H-135 (Annex N)
Washington, DC 20580

Via email to behavioralmarketingprinciples@ftc.gov

Re: Comments of the World Privacy Forum concerning FTC's proposed principles, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles.*

April 11, 2008

Dear Secretary Clark:

The World Privacy Forum appreciates the opportunity to comment on the Federal Trade Commission's proposed principles, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*.[1] The World Privacy Forum is a non-partisan, non-profit public interest research and consumer education organization. Our focus is on conducting in-depth research and analysis of privacy issues, including issues related to online privacy.[2]

Our comments focus first on general comments about the proposed principles, and then on aspects of the specific principles.

General Comments

I. Self-Regulation vs. a Mandatory Scheme

The World Privacy Forum thanks the FTC for attending to the issues inherent in behaviorally-targeted advertising and for publishing its proposed self-regulatory

---

[1] Federal Trade Commission, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, December 20, 2007. < http://www.ftc.gov/opa/2007/12/principles.shtm >.

[2] See World Privacy Forum home page, <http://www.worldprivacyforum.org>. See also, eg., <http://www.worldprivacyforum.org/internetprivacy.html>, <http://www.worldprivacyforum.org/calldontclick.html>.

principles. In the course of these comments we do address the proposed principles. However, we would be remiss in not noting that self-regulation in this space is unlikely to be successful.

Due to the past lack of success of self-regulation in this space, we urge the FTC to rely on a mandatory scheme instead of self-regulation, which has been a proven failure. The World Privacy Forum published a report documenting and analyzing various issues regarding the current self-regulatory regime.[3] Instead of reviewing those issues again here, we incorporate the report in our comments by reference and note that the issues documented in the report are largely continuing. One of the primary concerns we have is that long-term patterns of consumer profiling are being ingrained in online activities, business practices, and business processes.

We have no complaint about legitimate advertising; our complaint is with intrusive and difficult- to-detect (or nearly impossible to detect) profiling of consumers that is part of certain kinds of advertising practices. The laxity and opacity of the current dysfunctional self-regulatory system rewards the worst actors, which has had the result of creating an unappealing and unfortunate race to the bottom among some businesses. Now we have come to the point where we are seeing business models built on inappropriate opacity with concomitant highly intrusive consumer snooping. For example, we note the rise of a model where Internet Service Provider (ISP)-level profiling activities have been launched without sufficient transparency regarding which ISPs are allowing the profiling activities, or regarding consumer notice, among other issues.[4]

We have read the various comments of some industry members stating that regulation or a mandatory scheme in the area of online advertising would break the Internet, or somehow restrict or reduce large quantities of compelling content that are currently free to consumers based on advertising support. Again, advertising is not the problem. It is the deep and detailed profiling of consumers that is the problem.

We believe that a much-improved balance may be found in the area of online and other forms of digital advertising. Advertising accompanied by good practices and respect for consumers and their privacy is more than welcome. A better balance will allow advertisers the freedom of commercial speech, and will allow continued support of free content while still providing for the protection of consumers in an area currently lacking in fair play and characterized by uneven, even absent enforcement.

---

[3] World Privacy Forum, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*. Nov. 2, 2007. < http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf>.

[4] We refer in particular to models involving deep packet inspection of transmissions from an ISP. See Peter Whoriskey, *Every Click you Make*: *Internet Providers Quietly Test Expanded Tracking of Web Use to Target Advertising*, Washington Post, April 4, 2008. < http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html >.

II. Enforcement of the Principles

The World Privacy Forum observes that the proposed principles offer the opportunity for a shift in enforcement mechanisms from that of a centralized NAI/Truste model to a model that requires each company to be directly responsible for its own activities under the FTC Act §5.

If the FTC is going to go down a self-regulatory road, then it is our recommendation that the FTC provide expressly for direct consumer enforcement of any self-regulatory principles rather than relying on an industry self-enforcement model.

The importance of robust and timely access to consumer complaints

One difficulty with the current centralized model is that industry's designee for enforcement provides no significant enforcement oversight. If this model is followed again, we can expect the same kinds of outcomes, one of which is that the central organization is not required to make public consumer complaints or enforcement actions. If a self-regulatory organization does share those complaints, there is no guarantee the company names will be left in the complaints, and there is no promise that the complaints may be seen as often as desired by the public.

The World Privacy Forum believes that consumer complaints regarding any self-regulatory scheme needs to be directed to the FTC's Consumer Sentinel database, where those complaints can be requested by the public at any time. Another benefit is greater transparency and the potential for greater longevity and meaningfulness in terms of metrics. It is important that the FTC have the ability to directly monitor the effectiveness of any self-regulatory scheme.

Any enforcement plan should incorporate these principles:

- **Transparency of consumer complaints**: The public must have unrestricted access to consumer complaints.

- **Completeness of consumer complaints**: Consumer complaints must be maintained in a complete form, and given to the public with minimal redaction, i.e., redaction of consumer information, but with all company information included and all complaint and date information included.

- **Independent, public audits**: Independent audits of any scheme must be conducted by independent organizations with credible auditing capabilities. The audits should be published in a timely manner and with enough detail to assure the public of the quality and effectiveness of the audit and the independence of the auditor. The company chosen to conduct the audit should provide transparency about the resources used for the audit, including costs.

- **A yearly report to the FTC**: As part of enforcement, companies under a mandatory or self-regulatory scheme should provide a detailed report to the FTC of their activities for oversight purposes, which the FTC can then relay to the public in aggregate form.

- **Widespread publicity for complaint mechanisms**: any regime must require the regulated companies to publicize the chosen complaint mechanism. For example, there needs to be a *direct* link to an FTC complaint form, along with the notice of the privacy practices of the company, on appropriate web pages. In this way, consumers will have an improved opportunity to learn that they may provide feedback to the FTC about their experiences with the companies, and consumers will have an improved ability to navigate to that feedback opportunity.

The importance of simplifying and unifying enforcement in a fractured market

In the past decade, advertising technologies have become much more sophisticated and the targeting of consumers is more refined. It is no surprise, then, that the corresponding business models built in part or in whole on these technologies are in flux, which creates a certain amount of policy "churn." A good example comes from newer entrants to the marketplace that profile consumers at the ISP level.[5]

While the NAI has been the primary centralized entity that manages various aspects of the current self-regulatory regime to date, other self-regulatory regimes exist. It is not unlikely that additional new regimes will appear on the horizon and gain momentum. While the display of interest in self-regulation by industry is welcome, having multiple self-regulatory frameworks creates enforcement challenges, among other practical issues such as the temptation to comply with the weakest self-regulatory regime. We want to avoid a race to the bottom.

The FTC should enforce any self-regulatory scheme directly

Direct enforcement by the FTC of a mandatory scheme and direct FTC collection of consumer complaints is the only realistic way of encouraging a single, simplified enforcement framework and a unified enforcement mechanism applicable to all players. It is crucial that enforcement does not become a victim of a patchwork quilt of self-regulatory efforts, which could compete with each other in unproductive ways and potentially contribute to lax or missing enforcement.

The World Privacy Forum urges the FTC to move any enforcement of mandatory or self-regulatory principles to the FTC directly, and to make each company directly responsible for its own actions under FTC Act §5. This will accomplish many productive goals, including accommodating rapid changes in technology, a variety of business models, and

[5] See note 4.

the variety of platforms (web, mobile web, email, and so on), that are extant. There is no reason that any company acting in the best interests of consumers should have a problem with this shift in enforcement.

III. Request for a Separate Rulemaking Regarding Sensitive Medical Information

The World Privacy Forum respectfully requests a separate and formal rulemaking procedure regarding what constitutes sensitive medical information. Medical information is a complex topic area with non-trivial regulatory overlaps with HIPAA and with FDA oversight.[6]

Current efforts underway at the Department of Health and Human Services and elsewhere focusing on electronic medical information need to be played out without premature intrusion by network advertisers that do not understand the complexity of the health care field and its regulatory structure, and do not understand the breadth of the negative impact an improper definition of this can have on consumers.

There is a risk that a rush toward advertising using medical records or other health care information will fatally undermine consumer willingness to adopt greater use of information technology for medical information. See the recent World Privacy Forum report, *Personal Health Records: Why Many PHRs Threaten Privacy*.[7]

To list just a very small selection of ongoing activities:

- The Secretary's Advisory Committee on Genetics, Health, and Society is currently studying and deliberating on the issue of direct-to-consumer advertising of genetic tests. This Committee has already worked to recommend and facilitate the publication of a key joint FTC – CDC - FDA consumer alert about advertisements containing misleading claims regarding direct-to-consumer genetic tests, *At Home Genetic Tests: A Healthy Dose of Skepticism May be the Best Prescription*.[8]

  In its most recent draft report on this issue from winter 2007, the SACGHS notes:

  > **Direct-to-consumer advertising of genetic tests and consumer-initiated genetic testing have the potential for adverse patient outcomes and cost implications for the healthcare system.** There is a gap in knowledge concerning the extent of this impact. SACGHS recommends an examination of these issues:

[6] To note just one example, the FTC and the FDA have concurrent jurisdiction over weight loss products.

[7] < http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf>.

[8] Joint FTC, FDA, and CDC consumer alert, July 2006, < http://www.ftc.gov/bcp/edu/pubs/consumer/health/hea02.pdf>.

> HHS should step up its efforts through collaborations among relevant Federal agencies (e.g., FDA, CDC, NIH, and FTC), States, and consumer groups to assess the implications of **direct-to-consumer advertising** and consumer-initiated genetic testing, and as necessary, **propose strategies to protect consumers from potential harm.** Any additional oversight strategies that may be established should be attentive to cost and access issues that might prevent consumers from gaining benefits of wider access to genetic tests. [Bold added for emphasis.] [SACGHS Draft Report at line 6100.]

- The National Committee on Vital and Health Statistics has offered recommendations arrived at through a long deliberation and formal hearing process regarding health care data outside of HIPAA, and requirements for its handling.[9]

- At the state level, the California Privacy and Security Advisory Board, composed of a multi-stakeholder group, is the first official state-level group to formally begin the process of determining and setting a code of best practices for handling medical information held outside of HIPAA, including sensitive medical information.

Genetic information and the definition of sensitive medical information

To explore just one example of the difficulties a hasty decision could create in this area, the NAI has proposed new sensitive medical information guidelines that include cancer as sensitive medical information, but the guidelines do not, for example, include genetic information or genetically linked diseases as sensitive. Given all the state legislation establishing criteria for the use and disclosure of genetic information, this choice is transparently self-serving. It preserves the ability of advertisers to collect and traffic in information about every individual and tries to avoid the issue by proposing narrow protections for the subject of individuals with cancer.

Although health care professionals use genetic testing for the treatment of patients, technological and commercial developments have already begun to take some genetic testing out of the realm of health care professionals and into the currently unregulated commercial marketplace. Direct-to-consumer genetic testing and advertising is already here and is already recognized for its potential for abuse.[10]

However, this area has not fully matured. Imagine a time when genetic testing for all or a significant part of the human genome costs only a few dollars. We cannot predict when

---

[9] See <http://www.ncvhs.hhs.gov/071221lt.pdf>.

[10] Joint FTC, FDA, and CDC consumer alert, July 2006, < http://www.ftc.gov/bcp/edu/pubs/consumer/health/hea02.pdf>..

this might happen, but it seems inevitable that the cost of genetic testing will continue to drop dramatically.

Data profilers may find that they can make a profit by offering free or low-cost testing for consumers. The profits could come from the sale of a consumer's genetic profile to marketers during the course of the consumer's lifetime. Most genetic findings are likely to be relevant for the consumer's entire life and to have some relevance for blood relatives. The stream of income from data sales over many years may support a significant upfront cost to acquire the core data.

We observe, unfortunately, that it has not proven difficult for unregulated commercial ventures to obtain personal information from unsuspecting consumers through a variety of schemes and pretexts, or in exchange for a product, convenience, or opportunity that may have little value. It is quite possible that many consumers would sign up for free genetic testing in the same way that some have filled out online surveys about diabetes and other conditions, surveys which have landed these consumers on the kinds of marketing lists that can be readily found on list marketing web sites such as DirectMag's List Finder.[11]

Existing privacy oversight and regulatory mechanisms may be wholly irrelevant because of their limited applicability to parts of the health care world. The FTC should not casually assume that federal or state health privacy laws will help in the arena of genetic privacy. If a marketer or profiler obtains detailed genetic health information about a consumer, no existing regulation is likely to limit the maintenance, use, or disclosure of the information.

A consumer who casually agrees to disclosure of genetic information may find it impossible to retrieve the information. Once the information is out, the consumer who discovers that he or she has become uninsurable as a result of a disclosure made without adequate disclosure of the consequences may be powerless.

The commercial marketplace includes no shortage of unfair, deceptive, misleading, and fraudulent activities that rely on personal information or that exploit other consumer weaknesses. The consequences for genetic information are worse because inappropriate disclosures of consumer information in this area can impact the consumer for his or her life span.

We have just scratched the surface for issues surrounding genetic information, and genetics are just one aspect of sensitive medical information. It should be clearer now why we called for a separate rulemaking for sensitive information.

We are generally concerned industry's disregard for the consumer perspective about sensitive medical information. In comments to the FTC regarding the proposed principles, a commenter noted that individuals conducting an Internet search on the term

[11] <http://directmag.com/resourcecenter/listfinder/>.

HIV would not be revealing anything about their health status, and that consumers could be potentially surprised if they did not see ads for HIV. Individuals certainly expect to see search ***results*** that match their queries, but they do not necessarily expect to see ***ads***. They don't expect that their searches will be added to personal profiles and used to potentially assess health status and interests in the future. Additionally, examples such as this tend to omit the impact of bad actors on this issue. While a good actor may put forward a legitimate advertisement, plenty of fraudulent actors seeking to benefit inappropriately from the information may well put forward an advertisement as a lure to unsuspecting consumers.

Some suggest that a search query does not reveal a health status. Search queries cannot be evaluated fairly in isolation. As the AOL data breach made painfully clear, a collection of queries can be quite revelatory. So much so, in fact, that in regards to the AOL data breach, anonymous AOL searchers were able to be identified by name using their search queries alone. Given that searches can take place on many types of web sites and may even be embedded in certain applications, the collection of sensitive medical information in these and other online contexts poses significant threats to uninformed consumers.

After consumers' medical information has been collected, the proverbial Pandora has left her box, and mischief in uses of the information can occur with little or no recourse or oversight. Most, if not all, of the medical information disclosed or inferred is available under current law for use and redisclosure without limit.

Companies with a strong commercial interest in maximizing advertising dollars should not be the sole deciders about what constitutes medically sensitive information. There is a significant array of other interests in the health care sector including clinicians, vendors, payers, providers, patient groups, and other key players. All will want to and deserve to weigh in on what constitutes medically sensitive data, and it is important that all stakeholders should have the opportunity to do so.

A number of serious, deliberative regional and national processes are already underway looking at electronic medical information. The World Privacy Forum strongly encourages the FTC to conduct an entirely separate rulemaking on this matter, one which incorporates much more input from the private health care sector, the public health care sector, including HHS, CMS, and others, and draws from a much broader set of business and interest groups. To do less than this will jeopardize the policy work being done right now in this area.

It is unlikely that a definitive agreement could be reached on collection and use of medically sensitive data if the definition is not set. However, that being said, the World Privacy Forum notes that some information, such as information on genetically-linked diseases which have the potential for impact on blood relatives beyond the individual making the initial data disclosure, should not be collected at all.

IV. Comments on the Scope of the Proposed Principles

The World Privacy Forum believes that the proposed principles provide a starting place, but do not provide a complete protective scheme for consumers. We request that the principles be expanded to incorporate the full cohort of Fair Information Practices as articulated by the OECD. We know that the FTC is aware that the eight principles of Fair Information Practices are acknowledged nearly world wide, and we will not repeat the entire set of FIPs here.

However, we note that consumer access to all data being held about them by companies, correction rights, purpose specification, collection limitation, and the rest of the FIPs are all highly relevant to behavioral advertising and should all be included in any future set of principles.

V. Request for a Consumer Advisory Board

The World Privacy Forum requests that the FTC convene an independent consumer advisory board tasked with a focus on behavioral advertising. The consumer board should include consumer representatives from national, state, and local non-profit groups, representatives from privacy-focused non-profit groups, state representatives from either consumer protection bureaus or representatives of state Attorneys General offices, and neutral technical experts who have privacy and security technical-side expertise but who do not have a financial stake in the outcome.

The board should receive detailed reports from regulated companies regarding compliance for review, and should be able to hold formal or informal hearings or sessions where they can learn more about various topics of interest and applicability.

One of the functions of the board should be to assist in keeping any scheme up to date with current trends, and to provide a means of communicating to the public regarding various issues in this arena.

VI. Request for Increased Specificity

It will be difficult to move forward with any scheme without a precise definition of what constitutes personally identifiable information, behavioral targeting, and so forth. Without precise definitions, it will be too easy for industry players to bend or ignore the rules.

Regarding the definition of personally identifiable information, the World Privacy Forum supports the definition arrived at by a consensus of consumer groups in 2007:

> **Personally Identifiable Information** — Personally identifiable information (PII) consists of any information that can, directly or indirectly:

> (1) identify an individual, including but not limited to name, address, IP address, SSN and/or other assigned identifier, or a combination of unique or non-unique identifying elements associated with a particular individual or that can be reasonably associated with a particular individual, or
>
> (2) permit a set of behaviors or actions to be consistently associated with a particular individual or computer user, even if the individual or computer user is never identified by name or other individual identifier. Any set of actions and behaviors of an individual, if those actions create a uniquely identified being, is considered PII because the associated behavioral record can have tracking and/or targeting consequences.

Non-Personally Identifiable Information — Non-Personally Identifiable information (Non-PII) is:

> (1) aggregated data not associated with any individual or any individual identifier, or
>
> (2) any individual level data that is not PII.[12]

The inclusion of IP address in the definition of personally identifiable information (PII) is important. After hearing from a range of industry and consumer representatives, the EU Article 29 WG has interpreted the EU Data Privacy Directive as including IP address in the definition of PII. IP addresses are already being used and are likely to become the tracking tool of choice for advertisers and behavioral trackers.

It is an important decision which highlights the need to recognize at a regulatory level the increased identifiability of information that was previously regarded as aggregate or non-identifiable. This is just one part of a larger trend toward increased indentifiability or targeting of individuals, a topic that needs further exploration in the context of behavioral advertising.[13]

---

[12] *Consumer Rights and Protections in the Behavioral Advertising Sector*, October 31, 2007. Signatories include CDT, Consumer Action, CFA, Cryptorights Foundation, EFF, Privacy Activism, PIR, Privacy Journal, Privacy Rights Clearinghouse, World Privacy Forum. <http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf>.

[13] An important National Academies of Science report about identifiability and regulation explores this and other key issues in depth. The report discusses the following issues: (1) When is information sufficiently identifiable so that privacy rules apply or privacy concerns attach? (2) When does the collection of personal information fall under regulation? and (3) What rules govern the disclosure of personal information? The discussion of these issues in particular appears at Appendix A in the NAS report, *Putting People on the Map: Protecting Confidentiality with Linked Social-Spatial Data* (2007) <http://books.nap.edu/catalog.php?record_id=11865>.

VII. Comments on the "Harm" Approach to Consumer Privacy

The FTC's approach is largely based on the "harm" model. Many industry comments likewise focus on harm, with an emphasis on a perceived lack of consumer harm in the area of behavioral advertising.

The World Privacy Forum understands the reasons a harm model has been accepted by the FTC in some areas. We believe, however, that in information privacy, that more innovative approaches to consumer policy are necessary that move beyond the harm approach and evolve toward a more preventive approach. Consumers have interests in the processing of their personal information by third parties, and those interests do not only arise when a specific harm can be demonstrated.

Consumer harm may sometimes be obvious. In the case of revelations of consumers' sensitive medical information tied to their name and other highly identifiable information in commercial mailing lists such as the "Ailments, Diseases, and Illness Sufferers," it is profoundly obvious there is the potential for harm. In this marketing list, which is simply one among hundreds or thousands of similar lists, 172 million individuals are identified by ailment type, age, income, ethnicity, gender, homeownership, marital status, and other factors.[14] When a consumer's name, address, email, disease, medications, and more show up on a marketing list, these consumers face potential negative consequences regarding employability and insurability. Waiting for an actual victim to meet some artificial harm standard is unfair. The right approach is to recognize the rights and interests of consumers first and not to protect the commercial interests of those who seek to exploit consumers and their data often through methods hidden from consumers.

We would like to offer an example that highlights this issue. We have already discussed some of the issues surrounding direct- to- consumer genetic testing and advertising. Looking further at the issue of requests for genetic testing, we note that intensive internet searches for a service that provides genetic tests for Huntington's disease could provide information on testing subjects to advertisers and web portals. If a consumer was identifiable to a web portal and his or her behavioral profile at that portal was expanded to include genetic information, could the consumer find out about this inclusion? What other entities would find out about this aspect of the profile? Could the consumer delete the information if he or she so desired?

Regrettably, genetic information – even merely the request for certain kinds of genetic tests -- can have potentially deleterious consequences for a consumer. A profile of an individual with even just a potential for having a genetically linked disorder could be valuable to some companies or marketers. In weighing the relative interests of consumers and marketers, any reasonable person would find that the potential risk to consumers is

---

[14] DirectListFinder 2.0, Ailments, Diseases & illness sufferers data card, Nextmark ID # 102585. Data care last viewed April 11, 2008 at < http://listfinder.directmag.com/market;jsessionid=CE0945748C65721DC5CDD0CBD063D20A?page=research/datacard&id=102585>.

high and that marketer's interest in selling consumer information as many times as possible at ten cents a name is low.

Although this kind of approach represents a modulation of the FTC's current approach, we request that the FTC consider newer ways of approaching these complex and challenging issues. We do not believe a pure harm-based approach will be a sure enough guide in this area, and the stakes are too high for failure.

Comments on Specific Proposed Principles

VIII. Comments on Principle 1: Transparency and Consumer Control

The World Privacy Forum supports this principle in the broadest sense. We have additional suggestions to refine the principle.

The World Privacy Forum supports privacy policies. We believe they are crucially important for both businesses and consumers for a number of very good reasons. Any regime the FTC considers should require a disclosure of privacy policy. However, we also acknowledge that despite their importance and utility, privacy policies are problematic when used as the sole vehicle for consumer notice.

Minimum disclosure data sets for policies

Given the complexity of this field and the opacity of the language industry sometimes uses to describe fairly invasive data collection practices, we believe a privacy notice should have a bare minimum standard that is met, and this standard should be consistently applied across all business models. We suggest the adoption of ***minimum disclosure data sets*** to assist in this.

The idea is that a minimum disclosure data set will set a baseline standard of disclosure across the regulated industry. The data set will allow for a flexible yet standardized approach that allows consumers the ability to more easily and readily comprehend and compare actual practices of companies. This will go far to correct the hazy language currently extant in some of the privacy policies of behavioral marketers. It will also serve to reward companies who are attempting to be good actors and working to protect consumer privacy. To date, an effective consumer tool for privacy comparison has been lacking in this space.

Minimum disclosure data sets should contain the following mandatory elements:

- **Disclosure of all entities collecting data at a web site, portal, or other relevant digital medium:** This should be inclusive of Web 2.0 materials, which can have embedded applications and interactions from third parties. If data is being collected, then the collection should be disclosed.

- **Disclosure of what data is being collected**: There needs to be a precise disclosure of what is being collected from consumers.

- **Disclosure of the why the data is being collected**: For what purpose will the data be used? Will the data be used to determine a price point for an item, or interest on a line of credit? This needs to be disclosed to the consumer, so as to allow consumers who have received offers based on profiling activities to find the best possible offer or to request the best possible price available, regardless of profile, geography, or other factors.

- **Disclosure of what other businesses or entities will be using or receiving the data:** One of the difficulties with many current behavioral advertising policies is that the policies describe secondary data use in glowing but nebulous terms such as "business partners," "marketing partners," and so on. Businesses need to disclose what other businesses are getting the data.

The importance of consumer access in transparency and consumer control

Transparency will be greatly assisted by meaningful, complete consumer access to data held on them by companies. The EU Article 29 WG decision regarding search engines interprets the EU data protection directive as granting consumer access to all profiling information held on consumers by search engines, including data merged with other profiling data.

In discussions of the topic of consumer access to data companies hold on them, companies usually object strenuously without addressing the interests of consumers whose profiles they maintain. We see no fundamental difference in the need for transparency of behavioral profiles and credit reports. Both influence how consumers are treated in the marketplace.

If decisions about a consumer are being made based on a profile, then consumers need to know what the contents of that profile are should they desire to see it.

The importance of transparency regarding collection technologies and methods

In our report on the failure of the current self-regulatory scheme, we noted that Flash cookies, Silverlight cookies, and other mechanisms exist to circumvent current technological-based means of opting-out.[15] Those mechanisms still exist, and more will follow. Any means in use of collecting information from consumers needs to be readily transparent to that consumer.

---

[15] World Privacy Forum, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*. Nov. 2, 2007. < http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf>.

IX. Comments on Principle 2: Security and Data Retention.

Regarding data retention, we urge the FTC to indicate a specified duration of time for data retention, which should not exceed six months. We have heard the industry arguments regarding the need for longer data retention periods, but they make little sense. At present, there is a lack of balance between consumer interests and industry interests in this area. Shorter retention periods will restore some of the needed balance in favor of consumers.

X. Comments on Principle 3: Affirmative express consent for material changes to existing privacy promises.

The World Privacy Forum supports this principle strongly. One of the salient weaknesses with privacy policies as a consumer protection mechanism is the ability of a company to change the policy in the blink of an eye. We agree, however, with the FTC that there are good reasons that businesses may have to occasionally update and change a privacy policy. This proposed principle is balanced between consumers' interests in reliable protection and business' interests in flexibility.

The only comment we offer is in regard to consent and withdrawal of consent. We are aware that the FTC is familiar with the myriad problems of consent, particularly as mediated electronically, through its enforcement of the Fair Credit Reporting Act (FCRA). In light of the mischief that can occur around consumer consent, we urge the FTC to spell out specific guidelines regarding consent.

The situation we want to avoid is the proverbial pre-checked box at the bottom of an email or web page, or any other consent mechanism that is vague, confusing, misleading, not readily visible, or leads the consumer to a predetermined course of action toward consent without having adequate or fully accurate facts. We also are disinclined to accept as meeting the definition of express consumer consent a mere statement of consent on a privacy policy, eg, "if you use this web site, you have consented to ..."

We also request that the FTC incorporate the right for consumers to withdraw their consent. This right can be implemented in the electronic medium, as we have seen with the implementation of the FCRA. There is no reason that consumers cannot be offered the ability to withdraw consent. A consumer should be able to formally withdraw consent using a comparable mechanism that was used to obtain the consent in the first place. Neither consent nor withdrawal of consent should be mediated through a cookie.

XI. Comments regarding Principle 4: Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising

We have commented in large part on this principle in our request for a separate formal rulemaking on medically sensitive information in the "general comments" section of this document. We do have some additional specific comments on this proposed principle.

In the explanation listed under the "Issue" section, the FTC notes that some consumers find it helpful to see ads based on particular medical conditions. This may well be true, but the missing piece here is the presence and in some cases prevalence of bad actors, and the highly deleterious impact bad actors can have in this area.

We point to fraudulent weight loss advertising as an example of the problems that can occur. It is fair to state that not all weight loss advertisements are helpful to consumers.

The FTC has been active regarding this issue. The FTC has issued "Red Flag" guidelines to media to encourage media companies to avoid running misleading weight loss ads.[16] The FTC has also levied significant and plentiful enforcement actions against bad actors in this area, with its first enforcement action coming in 1927, and its most recent in February 2008.[17] The FTC has published a thorough report exploring advertising and weight loss, *Weight-Loss Advertising: An Analysis of Current Trends*, and has held a workshop that illuminated the myriad challenges with fraudulent advertising in this area.[18]

Something to consider here is that some weight loss advertisers compile consumers' information and make additional money from the sale of the information to the list marketing world. On a search of DirectMag's ListFinder, we found 2,311 lists containing the keywords weight loss. The lists ranged from people who had expressed interest in weight loss products, bought weight loss pills, and/or responded to online surveys, among other things. Millions of identifiable consumers are on these lists.

The question is: how many consumers know they are on these lists, and does their presence on one or more of these lists impact insurability or other high-impact life decisions being made about the consumer?

For weight loss products, the answer may be no in terms of impacts on insurability. But for other diseases, such as Huntington's, a serious genetically linked disorder, the answer

---

[16] FTC, *Red Flag Bogus Weight Loss Claims*, < http://www.ftc.gov/redflag/>.

[17] See Cleland *et al*, Federal Trade Commission, *Weight-Loss Advertising: An Analysis of Current Trends* < http://www.ftc.gov/bcp/reports/weightloss.pdf >; See also *FTC Sues Sellers of Weight-Loss Pills for False Advertising*, Feb. 8, 2008, < http://www.ftc.gov/opa/2008/02/zyladex.shtm >.

[18] Cleland *et al*, Federal Trade Commission, *Weight-Loss Advertising: An Analysis of Current Trends* < http://www.ftc.gov/bcp/reports/weightloss.pdf >; Workshop web site < http://www.ftc.gov/bcp/workshops/weightloss/index.shtml >.

could be quite different. A self-regulatory regime that leaves it to industry to behave well in matters relating to information of this magnitude and level of potential consequence for consumers is not desirable.

We reiterate that in particular, the definition of medically sensitive data needs a separate and formal rulemaking process that is much more deliberative, involves significantly more stakeholders from the public and private aspects of the health care sector, and takes into account the deliberative activities taking place on this very issue at other agencies.

What constitutes express consent?

We offer a comment about collection of sensitive information with consumer consent. We reiterate our concerns about what constitutes express consent, discussed elsewhere in these comments. We are concerned that consent will be nothing more than a click-through that most consumers do not notice. In matters of sensitive information where there is the potential for life-consequences, express consent needs to be carefully and clearly defined, and should be mandatory, not voluntary.

Trafficking in consent

There should be express prohibitions of trafficking in consumer consent where one company acquires consent and then transfers the consent to others (subsidiaries, affiliates, or others).

The issue of disallowing certain data collections

The FTC asked whether or not sensitive data should not be used at all for behavioral targeting. If data is determined to be in a sensitive category, then it should be unavailable for any kind of targeting due to the significant concerns it raises and the high potential for life-impacts the secondary uses of the data could pose. We believe curtailing use after collection is not realistic, and therefore we side with not collecting it in the first place.

We reserve a final decision about what constitutes medically sensitive information until more information and facts are brought forward, with the exception of genetically linked disease, which is a category we believe should not be collected at all due to the high risk potential and due to the fact that blood relatives can be implicated as well as the consumer.

XII. Comments regarding "Next Steps: Request for Comment"

The FTC asked for comment on costs and benefits for offering choice for behavioral advertising. We find in reviewing the harms that have already come to consumers in the area, for example, of fraudulent weight loss advertising, and the potential for harms that can come to consumers in the area of genetically linked profiling and tracking, that the benefits outweigh the perceived costs to an extraordinary degree. If the experience of

weight loss advertising is replicated only in part with a broader set of consumer products and services, the losses to consumers could be staggering and could outweigh any legitimate commercial benefits.

XIII. Conclusion

We thank the FTC for grappling with these issues and for working to address consumer protections through the proposed principles. We appreciate the difficulty of what the FTC is attempting with this, and we support the FTC's efforts to find a new path in this area.

We reiterate our request for a separate rulemaking regarding medically sensitive data, for reasons already discussed. We add that as the National Health Information Network and other digital health information exchange activities are launched under various schemes – both regulated and not -- there will be many intriguing intersections between these activities and the work of the FTC. It will be important for all parties to weigh in.

We also reiterate the cornerstone position that consent and the mechanics of consent will play in any scheme moving forward. We note that if consent mechanisms and procedures are not strong, then a number of contemplated protections fall apart at the seams. We are relying on the FTC to provide more specific guidelines in this area, and to also look at the potential for withdrawal of consent. Finally, we observe that any actions taken in this realm must recognize and incorporate all Fair Information Practices. Notice and consent alone are grossly insufficient to address the rights and interests of consumers.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org