Consumers Union
Nonprofit Publisher of Consumer Reports

February 18, 2011

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Comments of Consumers Union to the Federal Trade Commission
on
A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

INTRODUCTION

Consumers Union (CU),[1] the non-profit publisher of *Consumer Reports*®, supports the Federal Trade Commission's (FTC) increased focus on protecting the privacy of consumer data. As noted by the FTC, consumer information is more important than ever in today's digital economy. Every day, new technologies are developed that enable companies to collect, analyze, combine, use and share information about consumers' activities and habits, both online and offline. Many such companies manage consumer information responsibly, and use it to enhance consumer experience online by quickly connecting individuals to relevant products and services. Arguably, consumers benefit when they receive truthful advertisements and offers tailored to their specific interests.

[1] Consumers Union of United States, Inc., publisher of *Consumer Reports*©, is a nonprofit membership organization chartered in 1936 to provide consumers with information, education, and counsel about goods, services, health and personal finance. Consumers Union's publications and services have a combined paid circulation of approximately 8.3 million. These publications regularly carry articles on Consumers Union's own product testing; on health, product safety, and market place economics; and on legislative, judicial, and regulatory actions that affect consumer welfare. Consumers Union's income is solely derived from the sale of *Consumer Reports*©, its other publications and services, fees, noncommercial contributions and grants. Consumers Union's publications and services carry no outside advertising and receive no commercial support.

While respecting the utility of such innovative tools, however, we must pay close attention to individuals' need and desire for privacy – "the right to be let alone." Many consumers are deeply troubled by the extensive collection, sharing, and compilation of data about them, in spite of the benefits such practices may offer. A December 2010 Gallup poll shows, for example, that when individuals were asked whether advertisers should be allowed to match ads to their specific interests based on past web pages visited, 67% answered 'no.'[2]

Allowing companies to collect, compile, and share vast quantities of online and offline information about consumers' preferences and behaviors could result in not only benefits to consumers, but also certain harms. As noted by Chairman Leibowitz,[3] it is disturbing to contemplate the prospect of a health insurer raising an individual's rates based on the purchase of a deep-fat fryer, or a bank turning a consumer down on a refinancing application because it knows that the consumer has bought the book *The Winner's Guide to Casino Gambling*. It is unclear whether companies have already adopted such practices; however, as more and more consumer information is collected, shared, and compiled in an unregulated manner, such troubling information uses become both possible and likely.

Consumers Union agrees with the FTC's proposal to develop a comprehensive privacy framework that would apply broadly to online and offline consumer data collection practices. CU believes that any such framework must be grounded in statute and implemented and enforced primarily by the FTC, an independent agency with a focus on protecting consumer rights. So far,

---

[2] Lymari Morales, "U.S. Internet Users Ready to Limit Online Tracking for Ads," Gallup.com, December 21, 2010. < http://www.gallup.com/poll/145337/internet-users-ready-limit-online-tracking-ads.aspx >.

[3] Jon Leibowitz, "FTC Chairman: 'Do Not Track' Rules Would Help Web Thrive," U.S. News & World Report, January 3, 2011. < http://www.usnews.com/opinion/articles/2011/01/03/ftc-chairman-do-not-track-rules-would-help-web-thrive-jon-leibowitz >.

voluntary industry self-regulatory initiatives, based primarily on the notice-and-choice system, have proven difficult and unwieldy for consumers, and have done little to restore confidence in the system.

We are particularly pleased with the Commission's "privacy by design" approach, which would build privacy protections into companies' every day business practices. For far too long, consumers have carried the entire burden of online data privacy by being forced to read and understand complex privacy policies drafted more with an eye towards legal compliance than consumer understanding. Requiring companies to incorporate substantive privacy practices into their day-to-day activities will hopefully redistribute that burden, so that it is shared by both companies and consumers alike.

We also agree that in order for consumers to have real control over the way their data is used, they must be presented with simpler and more meaningful choices regarding practices that are of greater concern. Within this context, Consumers Union strongly supports the FTC's concept of a universal "Do Not Track" mechanism that would allow users to persistently opt out of certain online tracking and information sharing. In addition, CU supports the Commission's proposed heightened protections for sensitive data and sensitive users.

Finally, we support the Commission's focus on helping companies increase the transparency of data practices by providing consumers with reasonable access to stored data, by simplifying privacy policies, and by educating consumers about data collection practices and the choices available to them. Innovative technologies such as location-based services and behaviorally-targeted advertising can certainly yield many benefits, but we must ensure that

consumers understand how the information is used and have sufficient control over it, so they can decide to bypass the benefits of the technology, should they choose to do so. The Commission's privacy report takes an aggressive stand for consumer choice in commercial data collection and use.

A. SCOPE

Consumers Union supports the scope of the framework, which encompasses all entities that collect or use consumer data, both offline and online, as long as the data can be reasonably linked to a specific consumer, computer, or other device.[4] CU agrees with the Commission that the scope should not be limited to entities collecting traditionally-defined personally identifiable information (PII), as the distinction between PII and non-PII is increasingly losing its significance. Companies are often able to re-identify consumer information, even when such information is deemed "anonymous." In addition, business practices that are harmful to consumers, such as discriminatory pricing based on browsing history, can be carried out without use of PII.[5] In such cases, the individual is targeted through the specific device he or she is using, and entities do not necessarily need to connect that device to an identifiable individual. Limiting the scope of collection and use of only PII would not address such harmful practices.

[4] These comments are not intended to apply to the newly emerging health information exchanges (HIEs). CU hopes to address any privacy concerns related to HIEs in a separate discussion.
[5] For information on "dynamic pricing," see the recent article in *Washington Post* by Annie Lowery, "How Online Retailers Stay a Step Ahead of Comparison Shoppers." Dec. 12, 2010. < http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121100143.html >.

CU does not believe that any business that collects or uses consumer data should be exempt from strong privacy requirements. All businesses must understand the importance of setting in place sound privacy protections, regardless of size or amount of data stored. However, CU does agree that the way in which the framework is implemented can be tailored to suit the needs of entities that collect a limited amount of information from a limited number of users, or collect no sensitive information at all.

B. PRIVACY BY DESIGN

Consumers Union strongly agrees with the Commission's "privacy by design" approach. This approach encourages companies to incorporate substantive privacy and security protections into their everyday business practices and to consider privacy issues systemically, at all stages of design and development of their products and services. This approach ensures that consumers are not made to bear the entire burden of protecting their privacy online by reading and understanding lengthy, complex privacy policies. Such documents are more frequently geared towards meeting legal requirements and preventing litigation than towards helping consumers make meaningful choices about the privacy of their information. Companies should engage in sound data security, data minimization, data retention, and data accuracy practices, thus providing consumers with automatic privacy and security protections.

Data Security

Almost every day, new data breach incidents lead to identity theft, lost revenue, and decreased consumer confidence in the way their personal information is handled in the

marketplace. The incidents often occur through inadvertent disclosures, physical loss of stored paper or electronic records, data theft by company insiders, and data breach by third parties through hacking or malware. Sometimes, these incidents affect ten or twenty consumers. Other times, the private information of hundreds of millions of consumers is compromised.

In order to address this issue, CU supports the adoption of a comprehensive commercial data security breach law that would apply both to online and offline records. CU hopes that such a robust measure would include notification provisions, strict data security protocols, and requirements that entities responsible for a data breach provide periodic credit reports or pay for a security freeze in order to protect consumers from harm.

Legislation should not include a risk threshold in order to trigger the notice obligation. If necessary, the legislation could include an exemption for documented instances of breaches that pose no significant risk. Through the threshold approach, entities would not come under the requirements of the law unless there is some risk (reasonable or significant) that the information could be used to commit identity theft or harm the consumer. This particular framing is problematic because companies could simply say they do not know if the data breach presents any risk of identity theft, thus avoiding the law's requirements. CU would prefer the exemption approach, under which all entities involved in a data breach are covered by the law's requirements, but where an exemption is available for entities that determine the data breach presents no significant risk of identity theft or harm. As a result, a company could not easily escape the requirements of the law by simply claiming they do not know whether a risk exists or not. Any risk determinations by the company should be submitted to the FTC.

CU also supports providing periodic free credit reports or payment of security freeze fees to consumers whose personal data has been involved in a security breach. Consumers should not have to bear the costs of securing personal information when a data breach is caused by a company's inadequate data security practices.

State Attorneys General should have enforcement authority over the provisions of such legislation. In addition, CU prefers that a federal law set a floor rather than a ceiling, allowing states to implement more robust security requirements to protect their consumers.

CU believes that a national security breach standard would provide industry with clear guidelines regarding the proper way to safeguard consumer data, as well as actions to take in case of a breach. This bill could also have the added effect of inducing companies to impose data minimization processes and data retention limits, in order to ensure that they are not collecting more data than they absolutely need.

Data Minimization & Data Retention Limits

As the Commission noted in its report, the limitations of the notice-and-choice model have become increasingly apparent, as privacy policies are generally long and incomprehensible to consumers, and few entities offer consumers any control over the way their data is collected and used. As a result, Consumers Union supports the implementation of substantive privacy principles, such as data minimization and data retention limits, which do not rely solely on consumer participation to function. Including these principles in the framework will require companies to carry out an honest assessment of the types and amounts of information they actually require to do business, as well as how long they need to retain those records. Fewer

privacy concerns will arise if only necessary data is collected and stored for a limited amount of time. A privacy framework that allows a company to collect an infinite amount of data and hold onto it indefinitely as long as that company is transparent about its practices would be a troubling one indeed.

Consumers Union also believes that data retention limits for information collected specifically for behavioral targeting purposes should be relatively short. Consumer preferences, collected through online tracking mechanisms, will change as time goes on. As a result, collected information will lose value as it ages, and can lead to irrelevant and ineffective advertising. CU believes there is no demonstrable business need for companies to store this information indefinitely. Continually collecting and aggregating information about consumers would ultimately allow entities to create extremely detailed profiles of their users, and to potentially put that information to new, unrelated uses. In addition, the more information a company stores, the more information it could inadvertently reveal in a data breach.

CU also agrees that data retention and minimization requirements can be scaled based on the size of the company, the amount of information it collects, and the sensitivity of the information.

Comprehensive Privacy Programs

CU agrees that every covered entity should institute comprehensive privacy programs to ensure these privacy principles are carried out. Such programs should focus on accountability, employee training, and constant assessment of the impact of new data practices on consumer privacy. Should Congress adopt a comprehensive data privacy framework, grounded in the FIPPs

and enforced by the FTC, we believe companies would have sufficient incentives to develop privacy programs in order to ensure they are complying with the law because otherwise, they would risk facing possible sanctions and civil penalties.

C. Simplifying Consumer Choice

Consumers Union agrees with the Commission that the key to empowering consumers is to give them meaningful notice and choice. Privacy policies that span over several pages and use legal jargon are often incomprehensible to consumers, and do not result in meaningful consumer participation. In addition, seeking affirmative consent for every single use of information would be annoying and unwieldy, causing consumers to ignore the substance of the privacy notice altogether.

As a result, we believe it makes sense to differentiate between "commonly accepted practices" and practices that are not commonly accepted, and to treat the two in separate ways. This approach recognizes the fact that consumers have different expectations vis-à-vis entities that they voluntarily establish relationships with, as opposed to unknown entities that obtain their information surreptitiously. Limiting consumer choice to only those practices that are not "commonly accepted" and which consumers would not expect allows individuals to more meaningfully participate in the way their information is collected and used.

Commonly Accepted Practices

Consumers Union agrees with the Commission's proposed list of "commonly accepted practices." When an individual visits a specific webpage, he or she establishes a voluntary

relationship with that entity. As a result, the consumer is likely to know and expect that his or her personal information could be used for product and service fulfillment, internal operations, fraud prevention, or first-party marketing. A consumer who shops on Amazon.com, for example, would expect the company to share their name and address with the shipping company delivering the purchased product, and will most likely know that Amazon may target them with advertisements about other Amazon products, based on their purchase. The key distinction here is that the individual knowingly establishes a relationship with a trusted entity. As a result, we believe requiring consumers to give consent for each of these practices would be more burdensome than beneficial, and may result in a deluge of notices that consumers will eventually ignore altogether.

The Commission's definition of "first party marketing," referring to the party with which the consumer interacts directly, is also appropriate. Entities can have hundreds of business affiliates that it would consider "first parties," but consumers are often unaware of such business relationships. Restricting first party marketing in this way ensures that only the party with which the consumer has voluntarily established a relationship can use that information for marketing purposes, something a reasonable consumer would expect.

Commonly-branded affiliates could be considered first parties only if in the same line of business as the first party with which the consumer directly interacts. For example, a bookseller could share information with other commonly-branded affiliates that also sell books, but not with affiliates selling clothing, cars, or furniture. In such a situation, the sharing of information would

only be "commonly accepted" if the commonly-branded affiliate used it in a manner closely related to the primary purpose of information collection.

In regards to data enhancement practices, Consumers Union does not believe that companies need to offer consumers a choice as long as the enhancement occurs only for product or service fulfillment purposes, or for fraud prevention. However, if the data enhancement practices are undertaken in order to create a consumer profile used for marketing purposes, consumers should be notified and given the possibility to opt-out.

Finally, Consumers Union strongly believes that "deep packet inspection" should be classified as an "unanticipated use" of information. This practice is particularly troubling, as it involves the monitoring of all or substantially all the consumer's online activity across websites, and allows ISPs to create highly detailed profiles of individuals. Consumers would not expect that profile to be shared or sold for marketing purposes, and CU agrees that such a collection and use of information should be considered an "unanticipated use" and subject to heightened protections.

Practices That Require Meaningful Choice

Consumers would probably not expect that the sites they are visiting are collecting and sharing their PII with a data broker, or allowing a third party advertiser to collect and compile their online activity information. Such uses of information are rightfully denominated in the Commission's report as "unanticipated uses," and CU agrees that websites should provide clear, concise, and streamlined notice at the moment when the consumer yields his or her personal data or accepts a product or service, and obtain affirmative consent. The manner in which the notice is

delivered and consent obtained will probably be different for different contexts, depending on the manner in which the entity collects the information. Any consumer choice obtained in this manner should be durable and not subject to repeated additional requests from the particular merchant.

We certainly appreciate that in recent months, industry has developed a new self-regulatory initiative that places a link on each targeted ad, allowing consumers to see who delivered the ad and to opt out of behavioral targeting altogether. However, this program is voluntary and not all entities have chosen to participate. In addition, we believe that consumers should be given control over their information *before* it is used in unanticipated ways, not only after the fact, when the PII has already been shared and the ad has been delivered. Providing a simple, clear, and streamlined "just in time" notice on the site before the information is collected will allow consumers to make informed choices at the beginning of the process, when they are deciding whether to input information.

We also do not believe that it is appropriate for companies to offer choice as a "take it or leave it" proposition. The ability to share one's PII only with specific trusted entities should be a basic consumer protection principle. Behavioral advertising should be offered to enhance a consumer's experience online. If consumers wish to forgo this benefit and restrict the sharing of their PII with unknown third parties, they should not be punished for that decision.

The collection and use of sensitive information should require affirmative opt-in consent, even when first party marketing is involved. Sensitive information generally refers to information that could harm or embarrass the user, or lead to identity theft or discrimination

against the user. As a result, sensitive information should be afforded the highest level of protection possible, and should only be used for the express purpose for which it was collected unless affirmative opt-in consent has been obtained from the user.

We also believe that the collection and use of information about teens should be subject to heightened protections. Teens between the ages of 13 and 17 make up a large portion of Internet users today. At the same time, they are more vulnerable to inappropriate uses of their personal information online, especially because many of them do not understand the potentially detrimental consequences of freely sharing personal information. Congress has already addressed the privacy of children under the age of 13 by passing the Children's Online Privacy Protection Act (COPPA), which seeks to place parents in control over the type of information collected from their young children online. We hope the Commission will support heightened protections for teen users as well. Sites aimed at adolescents, for example, should provide greater controls, transparency, and limits on information collection. In the social networking context, entities that have reason to believe a user is a teen should restrict options, for example, by not allowing that user to share information with "Everyone."

Do Not Track

Consumers Union supports the concept of a "Do Not Track" mechanism, which would provide consumers with a universal, transparent, and durable means to opt-out of information collection and use for marketing purposes. We also agree that one simple way to implement this mechanism would be to provide a browser setting that a consumer could turn on in order to signal to websites that the consumer wished to remain anonymous on the web. We believe that a

browser-based mechanism would be preferential to the present industry cookie-based opt-out, since consumers are constantly encouraged and reminded to delete their cookies and browsing history in order to protect their privacy online. Deleting cookies also deletes the privacy setting in the current cookies-based opt-out system.

A "Do Not Track" option would also allow consumers to express their preferences once, without having to undergo the onerous task of opting out of every site or ad network. In addition, such a mechanism would address the complex matter of data brokers, who may find it difficult to provide "just in time" notice to consumers at the point of collection, since they do not interact with the consumers directly.

Consumers Union would also not be opposed to a behavioral targeting opt-out system that allowed consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them. Such a system may actually prove more effective for marketing purposes because, instead of relying on inferences made in reliance on a person's web activity, companies could target consumers based on expressed preferences and interests. This practice would be likely to cut down on irrelevant and ineffective ads by showing consumers products or services in categories in which they have already shown an interest.

Any such "Do Not Track" mechanism would have to be grounded in statute and enforced by the FTC. Without significant and robust enforcement, such a requirement would be essentially meaningless, as companies could easily choose to disregard the consumer privacy choice expressed by the browser.

Consumers Union also encourages the Commission to look beyond the browser-based system when implementing "Do Not Track." With the rise of smart phones and tablet computers, the "app" model is becoming increasingly ubiquitous. When using such devices, consumers often do not access web sites through browsers, but rather through specific applications. Any persistent, universal opt-out mechanism should also address this ever-increasing method of accessing the web.

D. TRANSPARENCY

Privacy Policies

Transparency can be enhanced through the use of clear, concise, and streamlined privacy policies. As outlined in the FTC report, current privacy policies are often written in order to satisfy legal obligations, not to facilitate consumer understanding. The number and complexity of current privacy policies is overwhelming to the average consumer and cannot provide meaningful notice of a company's privacy practices.

Consumers Union believes that a simple, streamlined privacy policy must be developed that allows consumers to easily compare and contrast companies' privacy practices. These streamlined privacy policies could be industry-specific and could be developed through a collaboration of stakeholders representing industry, consumer groups, and government. Such privacy policies should use clear, simple language and sentence structures, and use an easy-to-read format like bullet points or charts. The privacy policies should be as concise as possible, allowing consumers to quickly scan them and understand the most important pieces of

information. The privacy policy could certainly include links to more detailed discussions and explanations of individual sections of the policy, but the main page should be geared towards helping the consumer understand how the company will be collecting and using his or her data, not towards fulfilling legal requirements. Finally, the privacy policy should be easily accessible and readily available to the consumer *before* the consumer has to reveal any information to the site.

Transparency will also be promoted if the links to the privacy policies are placed prominently on the website and not hidden at the bottom of the page in tiny, inconspicuous print. This could possibly be achieved by creating a uniform button that can be prominently placed on all sites where commercial data is collected.

Transparency-enhancing techniques need to be adapted to fit the different forms of media from which websites can be accessed. Different media include computer screens, tablet screens, and mobile phone screens. A privacy policy for a given site thus should be modified in terms of presentation depending on whether it is accessed from a computer or a mobile phone.

Reasonable Access

Consumers Union supports the requirement that consumers be able to access the information compiled about them and correct it, if it is erroneous. However, we agree that this requirement should be proportionate to the sensitivity of the information and its potential harm to the consumer.

In addition, we believe that consumers should be notified when information about them complied by data brokers is used to make an adverse decision about them. Although the Fair

Credit Reporting Act (FCRA) already applies to consumer information to be used for credit determinations and certain other purposes, such as employment decisions, the existence of vast and unregulated databases of consumer information, including preferences, interests, and online browsing habits creates an opportunity to evade FCRA. CU is particularly concerned about the possibility of insurance companies and banks using such data from information brokers to make significant decisions about consumers. Consumers should, at the very least, be given notice of adverse decisions and be permitted to access and correct any erroneous information in their consumer file.

Material Changes to Privacy Practices

When companies use consumer information in an unanticipated manner that was not disclosed at the time of collection, they should be required to provide notice to consumers and obtain opt-in affirmative consent. In order to develop consumer confidence in the online economy, consumers must be able to believe that a company will behave in the way it has stated it will. Companies should not be able to lure consumers into disclosing PII by ensuring them that their information will be securely protected, only to then turn around and alter their privacy policies in an unanticipated manner. Consumers should be able to trust that the entities they do business with will keep their word and respect their privacy promises, or else obtain authorization for any other information uses.

Consumers Union
Nonprofit Publisher of Consumer Reports

D. CONSUMER EDUCATION

Consumers Union agrees that there is a great need for consumer education regarding data collection and use, as well as the privacy implications associated with these practices. The FTC roundtable discussions reveal that many consumers are simply unaware that their behavior is being tracked and used to create consumer profiles, which are then used for marketing purposes. In addition, even if consumers are aware of such practices, they are ill-equipped to effectively balance the benefits of behavioral targeting with its potential harms. Consumers Union looks forward to working towards raising consumer awareness of these issues and encourages all stakeholders to accelerate efforts to do the same.

CONCLUSION

Consumers Union commends the FTC for exploring the privacy issues and challenges associated with 21st century technology and business practices, both through its privacy roundtables and through this report. CU supports the FTC's proposed framework for addressing the commercial use of consumer data, which we believe should be grounded in a Federal statute and implemented and enforced by the Commission.

We believe that the adoption of a "privacy by design" principle will be the key to the success of the data privacy framework. Companies cannot claim they are protecting consumer data when, in reality, they are merely relying on consumers reading and accepting complicated and lengthy privacy policies. The current "notice and choice" system does not allow consumers meaningful choice. Instead, companies must seek to incorporate substantive privacy practices

Consumers Union
Nonprofit Publisher of Consumer Reports

into their day-to-day activities, and must evaluate every data collection and use practice in order to understand its effects on consumer privacy.

In addition, we agree that consumers can provide meaningful consent most easily when they are presented with simple, streamlined choices. As a result, distinguishing between commonly accepted practices and those practices requiring affirmative consent will be essential in implementing this privacy framework. Any practice classified as an "unanticipated use" and not "commonly accepted" should trigger opt-in, affirmative consent. In addition, granting consumers a simple, persistent means to protect their privacy, such as a proposed "Do Not Track" mechanism, could go a long way toward ensuring consumers have meaningful participation in the way their information is used online, thus enhancing consumer trust.

Combined, the above-mentioned factors and recommendations will help protect consumer privacy and increase consumer confidence in the Internet, while also giving businesses clear guidelines, so that they can grow and innovate with confidence.

Thank you for the opportunity to comment on this important initiative, and we hope to work with you in the future in order to support and implement the proposals discussed.

Sincerely,

Ioana Rusu
Regulatory Counsel
Consumers Union – Washington, D.C. Office

Consumers Union
Nonprofit Publisher of Consumer Reports

1101 17th Street, N.W.
Suite 500
Washington, D.C. 20036
Tel: (202) 462-6262
Fax: (202) 265-9548
irusu@consumer.org