Comments on the DOC Green Paper and the FTC Preliminary Staff Report:

Creating a Privacy Friendly Data Policy

Introduction

The FTC Proposed Framework and the DOC Dynamic Policy Framework Green Paper have effectively outlined the laundry list of issues that impact privacy in the online and offline advertising marketplace. The Frameworks' offer recommendations, guidelines, and possible remedies for multiple situations and applications where private data comes into play.

In our response we would like to suggest an enhancement to the Frameworks' that focuses less on the situational usage of the data and more on managing the common cause of the concern – the consumer transaction data itself.

In our opinion a reasonable regulatory treatment of personally identifiable transaction data would serve to supplement and enhance the recommendations of the FTC Proposed Framework and the DOC Dynamic Policy Framework Green Paper. Regulatory treatment of consumer transactions would provide the necessary baseline for consumers and industry on which to build a suite of mutually beneficial remedies. The goals of Privacy by Design and Fair Information Practice Principles would remain entirely relevant serving to codify the objectives of providing the data privacy protections demanded by consumers while supporting the economic realities of the digital economy.

Thesis

With the number of players and varied business models and data mining techniques in the personal data ecosystem, we believe that the proposals rely too heavily on defining a set of privacy guidelines for each situation or delivery channel. As recognized by the DOC and the FTC, this ad-hoc approach would leave the door open for evolving data mining techniques and legal interpretation that would likely circumvent any application-driven policy.

The objectives of the Frameworks' could be more effectively achieved by directing policy initiatives toward regulating the baseline source of the concern – the consumer transaction data itself. Our Privacy Friendly Data Policy (PFDP) recommendation will be detailed in the pages that follow. How PFDP addresses the Frameworks' summarized objectives will also be addressed:

- Protecting First Party marketing rights that exist between the consumer and vendor.
- Effectively defining the metrics associated with sensitive vs. non-sensitive information, permissible use, and retention periods.
- How to guard against linking of data - reconnecting de-identified data with the consumer.
- The misapplication of Privacy Policies as a legal defense.
- The practicality of workflows around Opt-out and Opt-in.
- The impact of a "Do Not Track" policy.

By addressing the privacy of the data at a lower level in the marketing ecosystem we believe that many, if not most, of the specific privacy issues and remedies proposed in the reports' become practical and enforceable. We also believe our approach would create a more sustainable business and privacy friendly environment.

Applying our Privacy Friendly Data Policy for dealing with all consumer transaction data would streamline the privacy infrastructure, eliminating the need for interpretation of consumer facing choice such as opt-in or opt-out, and potentially improve the overall business performance of both offline and online marketing programs.

We are suggesting a data usage policy that protects all consumer transaction data all of the time.

Under our Privacy Friendly Data Policy all "consumer transaction data" would become part of a new class of "permissible use only - private data". Consumer transaction data would be defined as a consumer transaction of any distinct product or service which is captured and recorded by a selling party or their agent for customer support and future internal use.

Consumer transaction data would be treated differently than census results, directory data, compiled demographics, voting history or property records. Each of these data collections represents examples of what is often considered publicly available data. Consumer transaction data that is not publicly available would be considered private by default.

A key component of this proposal is to provide privacy predictability and confidence among consumers. PFDF would structurally curtail consumer transaction data from being applied in any manner beyond the expectations of the consumer – vendor relationship. Under a PFDP policy a company or their agents would be restricted in their ability to redistribute, broker, or otherwise resell their consumer transactions information to third parties in its raw form. There would be two guidelines that frame the policy for the treatment of consumer transaction information:

1. FIRST PARTY RIGHTS: Unrestricted internal usage of consumer information would accrue as part of the First-Party relationship that exists between the company and the consumer. A First-Party relationship would be defined by a purchase transaction, product registration, a website registration, or a cookied browser.

    - We believe that it is critical for businesses to be able to nurture and develop customers who have voted with their wallets or clearly opted-in for the product or service that the company offers.
    - First-Party rights would also extend to cookied visitors to a website provided that any cookie being set for the purposes of retargeting expires within a session or within a period consistent with the sales cycle of the product – never more than a week. Cookies would have to be specific to the product or to the offer and can never be transferred or resold in

raw form to a third party (i.e. to Data Brokers).

2. PREDICTIVE MODEL DRIVEN PROSPECT DATA: Organizations put together marketing programs every day to identify "prospects" as part of normal customer acquisition programs. Marketers acquire mailing lists, emails or cookied browser links in their raw form from companies, list resellers, and data brokers who have collected this information. They purchase "leads", but no FIRST PARTY relationship exists between the prospect and the original company. We are recommending that the acceptable use and transfer of the raw "consumer transaction data" be limited to sample data sets. These sample data sets would be restricted in size by a prescribed formula where they can only be used for analytical purposes. Wholesale transfer or resale of customer transaction data to third-parties would no longer be permissible.

   - Limit companies in their ability to resell or redistribute any First-Party consumer transaction information – the crux of the privacy issue. Companies would now only be able to resell or transfer a "random sample of their client base" not to exceed 5% to 10% of the total number of transaction in a file – 5% to 10% is a statistically significant sample an adequate in size for analytic purposes.
   - Using today's technology, prospects would be statistically de-coupled from the consumer transaction data, preserving privacy and any targeted intrusion. The targeted marketing lists that are created from, but do not include, the 5% of the people in the sample, must be based on predictive analytical models and/or demographic selection criteria mapped against publically available data sources.
   - A Company privacy policy and website would certify in Privacy Statement that details that the consumer's name, address, email or browser data will not be distributed or resold to any third party except as part of a random sample totaling no more than 5% of the customer base. In the event the customer name is transferred, that name will automatically be excluded from any promotional distribution list that is derived from that sample.
   - Prospect lists that are a product of the statistically valid analytical processes are typically considered of higher quality than raw consumer transaction files which inherently provide only limited coverage. Ironically marketing campaigns and business performance would likely improve because the policy would encourage the marketing ecosystem to seek the improved coverage provided by more holistically qualified prospect lists.
   - Data brokers and resellers of data would be required to comply with the same rules as companies. They could acquire or license a 5% sample of any given customer base, but only for the purpose of developing a predictive model or creating a profile that would be used to determine selection criteria for a prospect lists against a compiled file. Data brokers and resellers of data would be able to resell the model or selection-qualified lists to other third parties for marketing acquisition purposes in the same way they resell consumer transaction lists today.

In Practice

There are four use cases that best illustrate the practical implementation of our Privacy Friendly Data Policy;

1. INTERNAL USAGE OF DATA: A First-Party relationship exists when a consumer makes a purchase from a company that is recorded either offline or online. A consumer could go to a department store and acquire a business suit which they pay for with a Store Credit Card. They could also go online and purchase the suit and have it delivered through the mail. In addition, in our proposal a First-Party relationship is established when the consumer elects to make themselves known to the Company through a visit to a site, registration on that site, or a response to an acquisition mailing.

    - The company is permitted to access and use the customer identity because as part of the initial transaction a First-Party relationship was established – the consumer has knowledge of the company, and the consumer has elected to share their identity with the company.
    - The consumer responds to an acquisition mailing, or registers for more information online or offline but elects not to transact. In our proposal the act of response and registration by the consumer identifies themselves and this creates a First-Party relationship.
    - The consumer visits the company website and/or abandons a shopping cart. In our proposal the consumer has demonstrated an indication of interest. In this case the consumer can be cookied for purposes of near term re-targeting. The cookie can be used by the company for a period of time determined by the active browser session or the likely sales cycle of the product – but never more than 5 to 7 days.

2. OFFLINE DIRECT MARKETING: Companies generate Direct Mail and Email campaigns and purchase or rent demographic and consumer data to support customer acquisition programs that target the best available prospects. In the offline world the normal pattern is to rent compiled data which includes contact information, demographics, behavioral and psychographic data. Most of the core demographics that are used to select the audience such as income, net worth and ethnic profiles are modeled from samples in order to achieve the broadest possible coverage of a qualified audience.

    Today these compiled files may also contain First-Party consumer transaction data in raw form. The data capturing the consumer transaction of known buyers and the products they bought are often licensed by the First-Party Company for resale by date resellers. Companies licensing their customer transaction lists through data brokers do so to generate royalties by having these lists resold to other third parties. This is a relatively minor revenue stream for most companies.

    The practical issue with licensing consumer transactions to list brokers or resellers is that in spite

of privacy statements and opt-in or opt-out forms consumer is rarely aware that logging onto their online banking account or purchasing a product online could trigger an event where their identity or consumer behavior is being resold. Records of these transactions can live on for years on a reseller's database - as long as it has marketable value.

- The research clearly indicates that when given a choice consumers will opt-out of providing personal information for resale. It is our belief that consumers should not have to navigate legal policy statements or make a determination whether an opt-in or opt-out is best for them. In our Privacy Friendly Data Policy companies would be limited in their ability to participate in the direct data resale or brokerage of their consumer transactions as raw data. Companies would be required to maintain a confidence of privacy with consumers regardless of whether the consumer provides permission to use their names.
- In our Privacy Friendly Data Policy a customer's transaction data can only be used without restriction internally by a company if there is a First-Party relationship in place. However, instead reselling raw consumer transaction data for a royalty, companies could elect to relicense their "model-driven" lists. They could transfer a 5 to 10% sample of their customer to a third party – data broker, reseller, compiled file vendor, or analytic shop for modeling purposes. The product of the models, or scored lists, could be redistributed but cannot contain the 5%-10% source consumer transactions.
- A survey of the consumer transaction lists being resold reveals that the coverage of a typical list of consumer transactions is a small percentage of the potential consumer base for any given product. As a practical matter the limited coverage of most consumer transaction lists is usually too limited in coverage to be effective for marketing acquisition purposes. Offline marketers are familiar with this challenge and use Modeling and Profiling to supplement and aggregate enough potential prospects to meet ROI needs for a campaign.

3. ONLINE BEHAVIORAL TARGETING: Internet Advertising and the use of behavioral targeting through the application of cookies is considered one of the main areas of concern when it comes to privacy. Online campaigns that use behavioral targeting techniques increasingly include the purchase or rental of consumer transaction data. It is our position that similar, if not identical, policies should exist for the treatment of online advertising as they would exist under point #2 above for offline advertising.

    - The policies of First-Party relationships would exist and extend to the placement of a cookie on a browser of the consumer. Online First-Party relationships exist when the consumer has an account with the company, has registered for information, or has interacted in a material way with the company website. In all these cases the cookie would have to expire at the end of the browser session or within a typical sales cycle – but no longer than 5-7 days. The theory is that if a First-Party relationship exists, the consumer will return and the cookie would be refreshed. This would be consistent with industry standards for banking

relationships, email vendors and other frequently visited company sites by the registered user.

- Commercial Banks, Electronics Retailers, Auction Sites, Online Bookstores, Browser vendors or Email providers no longer would have the right to broker their cookied customer lists to ad networks, ad agencies, or data brokers in raw form. In our opinion consumers who have had their browsers cookied have not explicitly opted-in to this practice and they have not agreed to have their contact information redistributed. If a consumer's bank, social network, flight mileage program or online book buying behavior are being resold and redistributed for targeting purposes clearly the rights provided to the vendor by the consumer through any existing first-party relationship has been broken. Privacy policy forms and opt-in screens are inadequate or misleading tools for addressing privacy at this level – they are designed primarily to limit liability while achieving the revenue objectives of the seller. This is not what is in the best interest of the consumer – and ironically not in the best interest of the advertiser.
- Under our Privacy Friendly Data Policy companies would, however, be able to provide third parties and ad networks with a 5 to 10%% sample of the cookied consumer transactions for analytical purposes. These consumer transactions could be combined with contextual reference data from the sites and offline demographic profiles in order to create predictive targeting models. The models could be used to score the location, the context, and/or the core demographics – gender, age, education, income, etc., variables supported as selection criteria by most of the ad networks in order to build a sufficiently large qualified prospect audience.

4. DO NOT TRACK: The FTC's proposal of a "Do Not Track" policy where browser providers and ad networks agree, as a default, not to track consumers is a technological option which we believe would have unintended negative consequences. It is our opinion that the Do Not Track policy proposed by the FTC Commission may be unnecessary if the consumer transaction data is limited and regulated.

    - If one of the main objectives of the FTC Staff Framework is to define privacy initiatives that both protect consumers and enhance business effectiveness, we believe a "Do Not Track" policy would run counter to this objective. If browsers were set by default to block cookies, – First-Party relationships would be negatively impacted. Recalling sign-in information for your email, banks, credit cards, bill paying, online newspapers, fantasy football, etc., are all part of the normal traffic and behavior pattern of users with First-Party relationships. A voluntary "Do Not Track" policy would actually force people into accepting tracking in order to make the web experience less frustrating.

5. PRIVACY FRIENDLY CONSUMER TARGETING: All parties agree there is a need to protect a user's privacy, however, the execution of any policy needs to address commercial impact. There are alternatives that support commercial objectives yet technologically control unwarranted

distribution of private information. It would seem entirely consistent with the objectives of the FTC, DOC and commercial entities to provide a way to move toward Privacy Friendly Standards for linking online prospects with prequalified advertising offers online. We are recommending that this linkage be made through a persistent metadata cookie or Universal Ad Key attached to an individual browser. This metadata score would be a hash of flags containing only references to publicly available demographic variables that are currently addressable through most ad networks: age range, gender, income range, education, day part and possibly ethnicity. Data would exist only as ranges of information and would be impossible to reverse engineer or link to an individual. Identifying a specific browser would be at the "segment level" not individual level. There are typically between 500 to 600 unique combinations of these core demographic variables. Each of these combinations of variables to produce segments, could be used by marketers as core selection criteria or in combination with an advertisers specific predictive model score. The product of the predictive models built offline would provide the criteria that prioritizes the appropriate consumer segments addressable on the browser. In effect, targeting would be derived from models that are built by advertisers from their known, First Party, relationships and applied to privacy protected prospects.

- Users would have the option to edit their metadata or turn it off in the browser options. The consumer would have control to change or eliminate the targeting parameters of their metadata cookie. As a result of the process of modeling the user segment identity is completely shielded from the advertisers by the user.

- The hidden benefit in this approach is that a broader selection of consumers would get relevant promotions and Advertisers would be able to reach more qualified audience than they currently reach with behavioral targeting methods. Given that that average click through rates for online for behavioral targeted advertising today are between .02% and .025% we believe our modeled data solution will actually improve results. Instead of serving online advertising to a small subset of identified consumers who have a cookie (comScore notes that only 30-35% of a potential audience is cookied at any given time) 100% of the of a qualified audience would be available to marketers for each campaign.

Precedent

The FCRA legislation of 1970 re-classified how an individual's credit data could be used in marketing. The individual data itself became restricted due to its perceived level of sensitivity. Redistribution was limited to permissible purpose only. Whenever credit data was used the marketing organization was required to make a firm offer of credit as part of the data usage agreement.

FCRA restrictions increased the cost associated of using credit data, so market forces took over and spawned alternatives that served similar purposes but were less costly and restrictive. Options like Zip+4 summary credit data and ITA Credit (Invitation to Apply) evolved to circumvent the regulatory

requirements. ITA solutions in particular leverage predictive models to derive similar conclusions as credit data, without in fact, ever accessing any of the sensitive restricted credit information.

Under a Privacy Friendly Data Policy the objectives of the FTC, DOC and industry would be best served by moving to restrict the core data that is truly sensitive –consumer transaction data that links an individual with a product or service. Allowing the marketplace to develop a privacy friend proxy for the transaction data will benefit consumers and companies. We believe that the product of predictive models combined with publically available data in the form of a metadata cookie supports the targeting objectives of the marketer while providing a long term solution for consumer privacy.

Conclusion

The most objectionable part of the Privacy issue is the knowledge that our banks, internet browser vendors, online auction houses, book clubs, airline mileage programs, travel sites, and online newspapers may all be re-selling our visits and buying history to whoever wants to pay for it. There is no data to support the idea that consumers would ever knowingly opt-in to this behavior. So, clearly when account information is resold to third-party marketers without permission, there is a violation of trust.

Finding an adequate and practically enforceable solution to the consumer privacy issue is important to both the private sector economy and the individual consumer. The Framework needs to effectively address the consumer privacy issue and at the same time not damage the marketing services industry in the process.

Simple is better. With a Privacy Friendly Data Policy in place the DOC and FTC's objectives are accomplished by simply following the precedent of FCRA - make all private consumer transactions part of a new class of restricted use data. We believe restricting the data will eliminate the necessity for an opt-in/out infrastructure, solve the re-linking of the data problem, and by-pass the need for "Do Not Track". If reselling of transaction data was restricted to a 5 to 10% samples, and every browser had the option of a metadata cookie that placed users into anonymous but targetable user segments, it would simplify the transition for companies, ad networks, data resellers, data brokers and agencies who will all be able to navigate this change and enjoying the benefits of more robust and defensible long-term business model.

If privacy concerns continue without being adequately addressed, direct marketers and businesses will suffer. We believe that it is very important for consumers and for the economic priorities of the direct marketing industry that an unambiguous framework be agreed to that eliminates the privacy concerns of the consumer in a manner that is trusted and understood.

Thanks you for your consideration.

Ray Kingman

CEO
Semcasting, Inc
300 Brickstone Square Suite 701
Andover, MA 01810
978-684-7580
rkingman@semcasting.com

Background

Semcasting, Inc. in Andover, Massachusetts has been actively involved in the compilation, aggregation, and creation of targeted consumer data for the last five years.

We provide a service for the development of analytical models and the creation of targeted campaign data based on our relationships with our clients and resellers. Our scored households for propensity are used in their direct mail campaigns and for online display advertising.

Our client base includes medium to large businesses in retail, travel, entertainment, financial services, and political campaigns. Fulfilling over one hundred marketing campaigns a month, we have a high degree of familiarity with online and offline direct marketing, and with the specific dynamics surrounding privacy in the creation, application, and distribution of data.

In addition to managing marketing campaigns for first party clients, we also compile household data from publicly available sources. Our technology is used to build analytical modeled data variables that serve to define household affluence, life style, affiliations, or buying behavior as projected values. An example of these core data variables would be projected values for Income, Discretionary Income, Recession Sensitivity and Net Worth. Many of these data variables are licensed and resold by the larger compiled file data providers. These attributes are modeled projections or propensities created from a small sample of First Party data that have been projected to approximately 95% of the U.S. population.