Before the
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION

Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers	)	File No. P095416

Comments of Statz, Inc. on Preliminary FTC Staff Report

Cameron Lewis, CEO
Tom Wilson, COO
STATZ, INC.
98 Cuttermill Road, Suite 370
Great Neck, NY 11021
516.570.100
info@statz.com

Glenn B. Manishin
DUANE MORRIS LLP
505 9th Street, N.W.
Suite 1000
Washington, DC 20004
202.776.7813
gbmanishin@duanemorris.com

Counsel for Statz, Inc.

Dated: February 18, 2011

Statz, Inc. (Statz), by its attorneys, respectfully submits these comments in response to the preliminary staff report (Report), released Dec. 2, 2010 by the Bureau of Consumer Protection of the Federal Trade Commission, on *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*.[1]

INTRODUCTION & SUMMARY

Statz commends the FTC staff for a forward-looking effort to adapt the agency's historic privacy policies to the current commercial environment. Sea changes over the past three decades in industry data collection, use and sale have yet to be matched with comprehensive, effective business and legal protections for consumer privacy. The Report's recommendation that a national United States privacy framework should apply to every entity that "collects or uses" data that can reasonably be linked to a specific consumer or device, including third parties, is a basic concept that unfortunately has yet to be accepted uniformly in the corporate milieu, especially traditional brick-and-mortar industries. As a result, the foundational principles articulated in the Report are destined to be viewed as an important landmark in the evolution of public policy on consumer privacy in this country.

Nonetheless, given the failure of a pure notice-and-choice privacy model to achieve the transparency and consent necessary for consumers to make informed decisions on whether and for what compensation (whether explicit or indirect) to release their private, digital data online[2] — data which is unequivocally owned by consumers, not ISPs, vendors, content and service providers or third party data aggregators — Statz urges the FTC to move beyond the Report's focus on transparency of data practices and their corollary, Fair Information Privacy Practices

---

[1] Available at http://ftc.gov/opa/2011/01/privacyreport.shtm. On Jan. 21, 20111, the Commission extended the deadline for public comment on the preliminary staff report until Feb. 18, 2011 to "encourage full participation by all stakeholders." *See* http://ftc.gov/opa/2011/01/privacyreport.shtm.

[2] Report at iii ("[T]he notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand.").

(FIPPs). There is no longer any valid distinction between digital privacy in the e-commerce and real-world settings. An increasingly interconnected "Internet of things" is collecting and transmitting an unparalleled amount of data on consumer behavior, consumption and product usage autonomously. As the Report correctly summarizes, "[c]onsumers live in a world where information about their purchasing behavior, online browsing habits, and other online and offline activity is collected, analyzed, combined, used, and shared, often instantaneously and invisibly."[3] The risk of consumer harm and deception in this emerging environment arises less from a lack of transparency and information security than from collection and transfer of data that the affected consumer never knows of and has no opportunity to consent to its usage and dissemination, let alone be compensated.

Statz and other firms are at present developing new business models for aggregation and sale of consumer data in transparent marketplaces that will monetize the private information consumers affirmatively decide they wish to sell. This will, essentially for the first time, give individuals the ability to decide, at a granular level, which personal information they want to release and the price at which they are willing to part with such commercially valuable data. We therefore concur with the Report's conclusion that regulators should act cautiously about restricting the exchange and use of consumer data in order to "preserve the substantial consumer benefits made possible through the flow of information."[4] Given this appropriate caution and the simultaneous emergence of both ubiquitous data collection and transparent consumer data marketplace exchanges, the FTC should accordingly direct its privacy enforcement priorities to identifying and sanctioning companies that seek to expropriate consumer data rights by sale of

[3] Report at i.
[4] Report at 35.

consumer information, whether aggregated, de-identified or personally identifiable, without affirmative consent and some form of bartered-for compensation.

We emphasize that compensation need not be explicit or monetary, and for many purposes will be satisfied by the "free" distribution of advertiser-supported services, as is the case with many Web sites and Internet content services today. But explicit consent, and some sort of consideration, are the two fundamental bases on which retailers, content providers *and third-parties* must rest in order to permissibly use and sell private consumer data. Statz believes a Commission enforcement focus on unfair and misleading practices by data mining firms that assert a right to *use* private data without explicit consent by and compensation to consumers is as significant to the development of privacy as the FTC's traditional focus on unauthorized *disclosure* of such information and the Report's recommendation of a "do-not-track" option for online, digital behavioral advertising.[5] Quite apart from FIPPs and privacy practice disclosure, personal data is being collected and sold today by third party companies (sometimes referred to in the Report as "non-consumer-facing entities") with no notice to consumers, no request for individual consent and no offer of compensation. That is a concrete threat to consumer privacy and the continued development of consumer data exchanges — and thus an unfair and deceptive practice — which is at least as great as the length, ambiguity, arcane language and obscure location of online privacy notices to which the Report addresses the bulk of its analysis.

[5] This conclusion is implicit in the Report's observation that companies which collect consumer data often "share the data with multiple entities, including affiliated companies as well as third parties that are many layers removed from, and typically do not interact with, consumers." Report at 23.

DISCUSSION

Statz is an emerging growth company in the business of providing consumers with a platform to establish and extract fair value for data created by, for and about them.[6] The company recognizes the necessity of data flows to support product development and fuel economic growth. At the same time, certain private data, specifically information that relates to individual behavior, product usage and personal environments, is under legal precedent dating to English common law owned by the consumer.

In order to redress imbalances in bargaining power and equity in the transfer, sale and trade of that information, Statz delivers a "board of trade" commercial platform which provides a secure privacy framework, allowing individual and corporate consumers to (a) securely store and control their private consumption and usage data, (b) manage data access and control privacy at a granular level and, most importantly, (c) participate fully and explicitly in an efficient, auction-type market for data and information exchange.

The recent development of transparent exchanges and other forums in which individuals can authorize collection, aggregation and sale of private data arises from a revolution in the ubiquity and intrusiveness of consumer data collection that already dwarfs the online privacy issues addressed in the Report. Statz therefore commends the FTC's staff for its articulation of the landmark principle that that a national United States privacy framework should apply to every entity that "collects or uses" data that can reasonably be linked to a specific consumer or device, whether online or in traditional brick-and-mortar industries.

As explained further in these comments, however, given this simultaneous emergence of ubiquitous data collection and transparent consumer data marketplace exchanges, the FTC

[6] The Statz data marketplace and privacy policies, currently in beta trial, are available at http://www.statz.com.

should direct its privacy enforcement priorities to identifying and sanctioning companies that seek to expropriate consumer data rights by sale of consumer information — whether aggregated, de-identified or personally identifiable — without consent and compensation. Just as the Commission has recently stressed that data security obligations extend "downstream" to third-parties data resellers,[7] so too should data privacy protections extend to third-parties which unfairly and deceptively expropriate the value of private consumer data without notice, consent or consideration. The Report's recommendation that a single privacy framework apply to "all commercial entities that collect consumer data in both online and offline contexts, *regardless of whether such entities interact directly with consumers,"* is an important first step in the establishment of such a privacy enforcement priority.[8]

I. CONSUMER DATA OWNERSHIP IS A FUNDAMENTAL AND INALIENABLE LEGAL RIGHT

With antecedents going back to English common law, ownership of personal data — including identity, personal behavioral data, product usage and personal environments — rests with the individual who generates that data. The rights to use that data, incidentally and longitudinally, require specific terms and consent in the form of economic compensation (barter, fiat or trade). This form of personal data equity is well-established in consumer research programs, Internet barter-for-service agreements and affinity programs, to name a few examples.

The exchange of value-for-value, based on either fiat or trade, suggests a market equilibrium that we believe requires more transparency for, and participation by, the individual to ensure efficiency and the generation of fair economic value. That is the purpose of the Statz Data Marketplace and similar business concepts being developed by our competitors. Building

---

7 *E.g.*, http://business.ftc.gov/blog/2011/02/data-resellers-liable-downstream-security-failures.

8 Report at 42 (emphasis suplied).

on the principle that the individual consumer owns all data generated by and about their consumption, product usage and online activities, Statz provides a vehicle for individuals to monetize the commercial exploitation of their personal information through a voluntary, opt-in, for-consideration marketplace.

The reality, however, is that the economic function of an efficient market is largely lacking in two areas: first, the choice by consumers to provide private data to a vendor or service provider in the first instance; and second, the ability of consumers to receive monetary value (whether explicit, as in financial compensation, discounts or rebates, or implicit, as in advertiser-supported services such as Web content and social media networks) for the authorized sale of their data. The Report focuses principally on the first of these. Statz is a business dedicated to the second because, in a broader societal context, data privacy today is in some respects more of an economic than a legal issue.

As the Report recites, the Fair Credit Reporting Act of the 1970s articulated ground-breaking concepts about the collection and accuracy of consumer financial data.[9] But that era was far different from today, as the development of scaled, low-cost, instantaneous technological means to populate massive electronic databases with immensely valuable consumer data has overwhelmed the practical ability of consumers to share in the value derived from their personal information. At the same time, no one would dispute that an individual's medical and drug history under the Health Insurance Portability and Accountability Act (HIPAA), for instance, or securities trading activity under the Gramm-Leach Bliley Act (GLB), as another example, represent forms of information in which health care professionals and information processing companies, like registered broker-dealers and financial institutions, can assert no valid claim to

[9] *See* Report at 3-6.

ownership.[10] That is why, in these and other privacy statutes, the focal point has been on procedures for authorization of transfer of data *by the individual consumer* as a precondition to commercial use of such private information.

The protection of ownership as it pertains to the artifacts, including data, of our daily lives was documented in the United States as early as the 1890s in the seminal privacy paper by Professors Warren & Brandeis.[11] While individual ownership of personal information and data has received little direct challenge, the advent of the Internet has dealt inequitably with the relative power of consumers, merchants, content providers and data aggregators to profit from the dissemination, sale and transfer of that data. The established models of economic value call into immediate question the capability some businesses, based on technologies that harvest individual data and sell it without the explicit consent or compensation of the individual, to engage in such practices. They are equally problematic under the FTC's privacy initiatives, as the concept of unfair and deceptive trade practices embodied in notice-and-choice privacy inherently includes compensation to the consumer — in an amount and form satisfactory both to the individual and the overall market supply of data — as part of the principles of notice, choice, access, security and enforcement animating current FTC privacy policy.[12]

Statz does not disagree that consumer consent for the collection and transfer of information incidental to purchases, what the report calls "commonly accepted practices," such as product fulfillment, should typically be inferred.[13] But it is no more permissible or fair for a grocery chain to sell data on individual purchasing habits to third parties without offering customers the explicit opportunity to consent to the exchange of data for in-store discounts than

---

[10] Report at 3-6.

[11] Warren, Samuel D. & Brandeis, Louis D., "The Right to Privacy", 4 Harvard L. Rev. 193 (Dec. 1890), http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[12] *See* Report at 7.

[13] Report at 44-49.

it is for a bank to sell the balances of an account holder's assets without consent and compensation. At the very least, because data about a consumer's product and service usage is owned by the customer, not the vendor, the bargained-for consent of the former is a precondition to the right of the latter to commercialize that data, through transfer to third parties or otherwise.

II. FAIR INFORMATION PRACTICE PRINCIPLES ARE PLAINLY INADEQUATE TO PROTECT DATA PRIVACY IN TODAY'S ENVIRONMENT OF UBIQUITOUS AND INSTANTANEOUS INFORMATION COLLECTION

As a business matter, there is no substitute for empirical data that measures personal behavior, product (or service) usage and personal environments for effectively targeting advertising. But just as no one in government, in 1970, foresaw the impact of databases on the collection and distribution of personal information relative to FCRA practices, today we are on the brink of a similar sea change in personal data harvesting and dissemination. The proliferation of cell phone applications that measure consumer behavior, and forthcoming sensor networks that will add granularity and ubiquity, need to be reckoned with now to assure personal privacy is safeguarded before, rather than after, it has been compromised.

The transition to what some have called an "Internet of things" in which embedded sensors and actuators collect, analyze and transmit data from and about consumers and their products is a startling illustration of the power of silicon-based technologies.[14] Vinton Cerf, recipient of the National Medal of Technology and the Presidential Medal of Freedom, and

[14] Iera, A.; Floerkemeier, C.; Mitsugi, J.; Morabito, G.; , "The Internet of things [Guest Editorial]," *Wireless Communications, IEEE* , vol.17, no.6, pp.8-9, December 2010, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5675772&isnumber=5675766; Lane, N.D.; Miluzzo, E.; Hong Lu; Peebles, D.; Choudhury, T.; Campbell, A.T.; , "A survey of mobile phone sensing," *Communications Magazine, IEEE* , vol.48, no.9, pp.140-150, September 2010, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5560598&isnumber=5560574; "Internet of Things", *NetworkWorld*, September 16, 2010, http://www.networkworld.com/newsletters/lans/2010/091610-internet-of-things.html; Savage, Neil, "Cycling Through Data", *Communications of the ACM*, September, 2010, http://delivery.acm.org/10.1145/1820000/1810898/p16-savage.pdf?key1=1810898&key2=5056508921&coll=DL&dl=ACM&ip=68.196.119.201&CFID=9338567&CFTOKEN=66555951.

widely recognized as one of the "fathers of the Internet", noted just today during an interview that one of the next major consumer uses of the Internet[15]

> … will be this Internet of Things where we start managing collections of devices for our benefit.

As the Report explains, data privacy has historically been premised on both "notice-and-choice" and "harm-based" models, more generally referred to as Fair Information Practice Principles, or FIPPs. Yet both notice-and-choice and harm-based approaches, including FIPPs, eventually break down due to their sheer complexity. Faced with substantial volumes of forms, jargon, disclaimers and legal language, consumers largely tend to ignore privacy statements and warnings, making notice-and-choice ineffective.

Professor Cate identified as early as 2006 that FIPPs were failing their fundamental mission of consumer protection.[16]

> FIPPS have increasingly been reduced to narrow, legalistic principles (*e.g.*, notice, choice, access, security, and enforcement). . . . As theoretically appealing as this approach may be, it has proven unsuccessful in practice. Businesses and other data users are burdened with legal obligations while individuals endure an onslaught of notices and opportunities for often limited choice. Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice.

Equally important to note are the failures of the credit reporting industry spawned as a result of the FIPPs-based Fair Credit Reporting Act. Far from making individual credit scores and reporting something readily understandable and controllable by the individual consumer, FCRA has effectively drawn a veil of secrecy around both the calculation of credit scores and the

---

[15] Cerf, Vinton G., "Future of Internet doesn't include an IPV7", *NetworkWorld*, February 18, 2011, http://www.networkworld.com/news/2011/021811-vint-cerf-ipv7.html.

[16] Cate, Fred H., "The Failure of Fair Information Practice Principles," in *Consumer Protection in the Age of the Information Economy* (2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972.

distribution of personal information and credit history. What was initially envisioned as a set of consumer protections has resulted ultimately in a highly insulated cartel of three participants with exceptionally unfriendly consumer policies and processes.[17]

Similarly, privacy regulations formulated as part of HIPAA are often touted as a well-functioning example of FIPPs. Yet since its inception, studies have shown that patient confidentiality and privacy afforded by HIPAA has not had a substantive or meaningful impact on the uptake of recommended or even essential medical services. Those with privacy fears still choose to "opt out" or forgo treatment rather than rely on FIPPs-based privacy regulations to preserve their anonymity.[18] And under HIPAA, in one year alone, fraud resulting from the theft of Electronic Medical Records (EMR) grew from 3% to 7%, a 112% increase.[19]

Perhaps the most telling example of the failure of FIPPs as the means of privacy protection in online activities starts with the Commission's May 2000 report to Congress. At that time, fully 100% of the most popular Web sites — and 88% of randomly-sampled sites — had a formal privacy policy statement, despite the absence of any regulatory mandate.[1] Yet notwithstanding this impressive voluntary compliance with the notice-and-choice privacy model, the events of the last decade, and especially of the last 24 months, have taught us that unexpected (and even deliberate) disclosure of personal data by Web companies large and small have unfortunately become all too common.[20]

---

[17] *See* Testimony of Jim Harper, The Cato Institute, before the U.S. Senate Committee on Commerce, Science and Transportation (July 27, 2010), http://www.cato.org/pub_display.php?pub_id=12209.

[18] "EMR Data Theft Booming," *Information Week*, March 26, 2010, http://www.informationweek.com/news/healthcare/security-privacy/showArticle.jhtml?articleID=224200494.

[19] FTC Report to Congress, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (May 2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[20] "Facebook in Privacy Breach: Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds," *Wall Street J.*, Oct. 18, 2010, http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html; "Facebook and Zynga Face Lawsuits over Privacy Breach," *Wall Street J.*, Oct. 19, 2010, http://blogs.wsj.com/digits/2010/10/19/facebook-and-zynga-face-lawsuits-over-privacy-breach/; "Facebook Privacy Fail: Apps Leak Private Info, Report," *PCWorld*,

III. ANONYMOUS OR "DE-IDENTIFIED" DATA IS NO LONGER A SAFEGUARD OF CONSUMER PRIVACY

Statz agrees completely with the Report's astute observation that the dichotomy between personally identifiable information (PII) and "non-PII" data that has been rendered anonymous is "losing its relevance" as a result of technical advancements in data analysis, algorithms and related developments. Report at 35-37. In fact, reliance on anonymization as a privacy safeguard is quixotic because where there is a commercial value to obtaining consumer-specific information, businesses have the incentive and ability to extract that information, however obscure or deep-nested the linkages may be.

One recent outgrowth of HIPAA has been the advent of companies, including major healthcare providers, pharmaceutical manufacturers and independents such as First DataBank, building businesses based on de-identifying and then EMR and related medical data, all fully within the current scope of HIPAA and its implementing regulations. In some cases, even government agencies, such as the State of Texas,[21] have engaged in the sale of "de-identified" EMR information.

As companies like AOL, Netflix and others have learned over the last decade,[22] however, seemingly de-identified data can be used to undo protections and re-identify specific individuals within a population. In many cases, even without the inclusion of any directly personally identifiable data element, re-identification is still possible. Worse still, the "safe harbor" defined

---

Oct. 18, 2010, http://www.pcworld.com/article/208058/facebook_privacy_fail_apps_leak_private_info_report.html; "LexisNexis Warns 300,000 of Possible Data Theft," *PCWorld*, April 13, 2005, http://www.pcworld.com/article/120426 lexisnexis_warns_300000_of_possible_data_theft.html.

[21] DuBois, Shelley, "Electronic Medical Records: Great, but Not Very Private." *Fortune*, Oct. 6, 2010, http://money.cnn.com/2010/10/06/technology/electronic_medical_records_safety.fortune/index.htm.

[22] Ohm, Paul, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," Univ. of Colorado Law Legal Studies Research Paper No. 09-12 (Aug. 13, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

by HIPAA may not be so safe after all. In their prescient ACM paper, Arvind Narayanan and Vitaly Shmatikov conclude that:[23]

> The PII fallacy has important implications for health-care and biomedical datasets. The "safe harbor" provision of the HIPAA Privacy Rule enumerates 18 attributes whose removal and/or modification is sufficient for the data to be considered properly de-identified, with the implication that such data can be released without liability. This appears to contradict our argument that PII is meaningless. The "safe harbor" provision, however, applies only if the releasing entity has "no actual knowledge that the information remaining could be used, alone or in combination, to identify a subject of the information." As actual experience has shown, any remaining attributes can be used for re-identification, as long as they differ from individual to individual. Therefore, PII has no meaning even in the context of the HIPAA Privacy Rule.

As a pointed example, there is a 0.04% chance that data de-identified according to HIPAA standards could be re-identified down to the individual level when compared with voter registration records.[24] More simply put, if a database de-identified using HIPAA standards comprised one million names, then 400 people could be readily re-identified. If data from other sources —including public records, commercial databases, the Internet or private records — were then cross-correlated with the de-identified HIPAA data, the number of possible re-identifications would increase.[25]

In sum, this exploded myth of the anonymity of de-identified data, and the failing of even the "safe harbor" provision of HIPAA, clearly shows that traditional notice-and-choice and harm-based models for structuring personal privacy and anonymity have been outpaced by the proliferation of data sources and the growth of Internet data collection and access.

---

[23] Narayanan, Arvind and Vitaly Shmatikov, Vitaly, "Privacy and Security: Myths and Fallacies of 'Personally Identifiable Information,'" *Communications of the ACM* (June 2010), http://portal.acm.org/citation.cfm?id=1743558.

[24] Sweeney, Latanya L., "Information Explosion," in CONFIDENTIALITY, DISCLOSURE AND DATA ACCESS: THEORY AND PRACTICAL APPLICATIONS FOR STATISTICAL AGENCIES (Urban Institute 2001), http://privacy.cs.cmu.edu/dataprivacy/projects/explosion/explosion2.pdf.

[25] Gellman, Robert, "The Deidentification Dilemma: A Legislative and Contractual Proposal" (July 12, 2010), http://www.futureofprivacy.org/wp-content/uploads/2010/07/The_Deidentification_Dilemma.pdf.

IV. MARKET SOLUTIONS ARE AVAILABLE TO ENHANCE AND PROTECT CONSUMER DATA PRIVACY WHILE PRESERVING THE ABILITY OF BUSINESS TO ACQUIRE AND UTILIZE SUCH INFORMATION FOR PRODUCT DEVELOPMENT, INNOVATION AND COMPETITION

The flow of electronic consumer information, including personal demographic and behavioral data, product preference and usage, has become essential to not just sustaining but growing our free market-based economy in the United States. Billions of dollars spent annually on product development, market research and advertising would suddenly be set adrift without the guidance of verified and validated consumer inputs if the FTC, Congress or other government institutions prevented the aggregation, acquisition and use of consumer and product research data.

Simply shutting off the flow of data through legislative mandate would have a significant and detrimental impact on Internet commerce specifically, and on the U.S. economy in general. Many Websites today rely heavily on targeted ad sales to sustain their existence and subsidize audience services. Reduction of advertising revenues as a result of consumer "opt-out" will negatively impact these businesses. Other than putting up pay walls, there are no other existing generally accepted Internet revenue models.

The increasing popularity of "opt-in" rules for particularly "sensitive" data and "opt-out" initiatives by privacy advocates and grassroots social media campaigns represents a clear attempt to reassert consumer control within the constraints of the traditional FIPPs notice-and-choice model. Apart from the potential impact to the economy at large, such an all or nothing approach is incapable of dealing with the richness of personal data and its myriad and often beneficial uses.[26] With opt-out as the only alternative, consumers will effectively either have to divorce

[26] Report at 60-62.

themselves from participating in the economic marvel of electronic commerce, or else remain unrewarded and passive participants, as they largely are today.

We believe that an individual's privacy is directly correlated with his or her ability to exercise control over personal information and data, in a manner and at a granular level that is consistent with each individual's own personal and objectives. As Jim Harper of The Cato Institute testified to the Senate last July:[27]

> In his seminal 1967 book *Privacy and Freedom*, Alan Westin characterized privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." A more precise, legalistic definition of privacy in the control sense is: the subjective condition people experience when they have power to control information about themselves and when they have exercised that power consistent with their interests and values. The "control" sense of privacy alone has many nuances. . . . Importantly, privacy is a subjective condition. It is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be.

Research further suggests that by giving consumers a granular level of control that allows them to choose which aspects of their personal and behavioral data are used for targeting, rather than simply whether or not their data are used at all, the resulting advertising performance may not suffer at all. In fact, advertising effectiveness could actually improve,[28] driving economic growth through increased sales.

A system that provides for individual control over personal data would likewise provide transparency into who was purchasing your data, when it was purchased, how frequently it was purchased and what other data was purchased by the same company. Interestingly, this transparency and participation could also result in a new form of brand loyalty (based on consumer to business selling) that advertisements alone cannot possibly achieve.

---

[27] *See* note 15 above.

[28] Tucker, Catherine, "Social Networks, Personalized Advertising and Privacy Controls," NET Institute Working Paper No. 10-07 (Sept. 29, 2010), http://ssrn.com/abstract=1694319.

Ultimately, therefore, consumer information privacy is, at its core, an economic issue. Despite fears over identity theft and public disclosure of embarrassing or potentially harmful personal information, most people would likely agree that product and behavioral information, when used properly and under the construct of bargained-for value exchange, has been helpful to the development of electronic commerce and overall advancements in economic welfare. New products and services, improved designs and implementations of existing products and services, as well as advances in technology and especially in healthcare, medical procedures and treatment, are all attributable in part to the disclosure and use of personal and behavioral information. If concerns about privacy, anonymity and personal control can be addressed, then what is left is purely an economic issue, *i.e.*, delivering fair and equitable value-for-value.

So, how do we arrive at fair and equitable compensation? In the physical world, if someone uses real property that belongs to me, then that act is generally accompanied by some remuneration in the form of cash, barter/trade or future liability. The use of personal information and data in the digital world should not be treated any differently.

The precedent for data ownership and participation in value comes from decades of consumer research and statutory rights in several specific categories. More recent is the barter for service formula of Web services. In both cases the exchange of value is predicated on the consumer offering personal data as the medium for exchange. The consideration given by businesses to consumers in exchange for personal data is a transaction involving the individual consumers' possession of valuable information, with the price or other consideration representing the fair market value of the right of use of that data.

Consider the following example. A car dealership, which conducts business through a traditional brick-and-mortar storefront as well as online, purchases a listing of local residents

living within a 25-mile radius of its location. The dealer correlates this demographic data with online tracking information acquired through the use of Web "cookies" regarding visitors to their dealer site, purchases additional online data from advertising information brokers and develops a profile of people shopping its Website for particular vehicle configurations. Based on that data, the dealer orders several vehicles in specific colors and with specific options, and then runs a focused *online* sales campaign, potentially including specific product and service discounts, directed at its target audience.

On the surface, this appears to be a straightforward and entirely equitable series of events, wherein the consumer ultimately receives the benefit of immediate availability and potentially favorable pricing on the vehicle they are seeking. But, consider the individual data transactions themselves.

1. The dealership purchases the list of local residents from an information broker, who has likely compiled the data by integrating public records, such as property ownership and voting rolls, with other data sources to provide a basic demographic profile as well as detailed identity information.

2. The dealership uses Web browser cookies to track online shoppers and has an online privacy policy that includes an "opt-out" option. Both the privacy policy and the opt-out option are buried in the Website footer. In addition, users who opt-out cannot view the latest online inventories or make queries about specific vehicles. Users who do make an inquiry are automatically "opted in," regardless of any previous selection.

3. The online tracking data purchased by the dealership is collected from directed advertising placements on a variety of automotive related Websites, and does not include an "opt

out." Data is collected surreptitiously, without notice or consent of consumers, and compiled for sale.

No permissions were given by individuals on any of these lists and no consumer benefit has accrued until someone actually buys a vehicle. The original list might have included more than 100,000 names and addresses, plus associated demographic data such as age and household income. Internal and external online tracking databases might represent a cross-correlated set of 10,000 names, and based on predicted purchasing profiles the campaign targets 500 individuals for direct marketing, in hopes of selling 25 new vehicles.

Assuming that the campaign meets its objectives, then arguably the 25 people who purchase a new vehicle receive compensation — in this case in the form of availability, special pricing or other incentives. But those 25 people represent a mere 0.025% of the original 100,000. Yet all 100,000 consumers contributed their data, along with additional online data from at least 10,000 of those same people. All of that data went into developing the profile which targeted 500 individuals and closed 25 new sales. Of course, the fact remains that no one other than the people who purchased a vehicle received any economic compensation for the use of their data.

This imbalance between the sources of consumer data and the recipients of the value of its beneficial use in business can and is being remedied by transparent data marketplaces such as Statz. Clearly, the only equitable way to compensate those who contributed data to developing this campaign is at the point of the data transaction itself. More importantly, the chance to consent or not, defined by notice-and-choice privacy policies, should not itself be seen as an economic benefit or consideration for such data transactions. By establishing a public and efficient market for the sale and purchase of consumer data, Statz and its competitors are

launching a new era in privacy in the United States, one in which the value of consumer information can and will be transferred by the acquiring businesses to consumers themselves in a form, monetary consideration, that historically has been available only to select product reviewers and Nielsen television survey households.

CONCLUSION

Given the failure of a pure notice-and-choice privacy model to achieve the transparency and consent necessary for consumers to make informed decisions on whether and for what compensation (whether explicit or indirect) to release their private, digital data online — data which is unequivocally owned by consumers — Statz urges the FTC to move beyond the Report's focus on FIPPs and the transparency of data practices. The recent development of commercial marketplaces and other forums in which individuals can authorize collection, aggregation and sale of private data arises from a revolution in the ubiquity and intrusiveness of consumer data collection that already dwarfs the online privacy issues addressed in the Report.

The historical safeguards of data anonymity and non-"personally identifiable" information are no longer adequate in today's environment of huge databases and powerful algorithms. Only by using its statutory enforcement powers to attack corporations that unfairly expropriate private data without offering substantive consideration to the consumers whose information is purchased, used or sold can the FTC adequately protect consumer privacy in an era when the distinction between online and offline information is already almost entirely irrelevant. Just as the Commission has recently stressed that data security obligations extend "downstream" to third-parties data resellers, so too should data privacy protections extend to third-parties and data mining firms which unfairly and deceptively expropriate the value of private consumer data without notice, consent or consideration.

Respectfully submitted,

STATZ, INC.

Cameron Lewis, CEO
Tom Wilson, COO
STATZ, INC.
98 Cuttermill Road, Suite 370
Great Neck, NY 11021
516.570.100
info@statz.com

Glenn B. Manishin
DUANE MORRIS LLP
505 9th Street, N.W.
Suite 1000
Washington, DC 20004
202.776.7813
gbmanishin@duanemorris.com

Counsel for Statz, Inc.

Dated: Feb. 18, 2011