Public Comment from Abine, Inc., on Consumer Data Privacy Protections in a Networked World

TO: Aaron Burstein
The National Telecommunications and Information Administration (NTIA)
1401 Constitution Avenue NW.,
Room 4725
Washington, DC 20230
Submitted electronically via privacyrfc2012@ntia.doc.gov

FROM: Sarah A. Downey, Esq., Senior Privacy Analyst, on behalf of Abine, Inc., The Online Privacy Company

RE: Public comment on multistakeholder process to develop consumer data privacy codes of conduct

DATE: 3/27/2012

SUMMARY:

Abine, Inc.,[1] is a Boston-based online privacy startup that has been implementing technological solutions to the privacy issues raised in the Administration's privacy framework for several years, including free browser software that blocks targeted advertising and data collection, and a paid service that opts consumers out of having their personal information displayed on data broker websites. As such, we wish to contribute our expertise, experience, and perspective in these areas to the Administration's goal of improved Internet privacy protections.

We begin with background on our company and the privacy matters we address every day. Specifically, these matters of concern are (1), online data collection, especially as it relates to Do Not Track; (2), the data broker industry; and (3) restrictions on developer innovation in the mobile privacy realm. The widespread and largely unregulated collection, sharing, sale, and storage of massive amounts of consumer data are a threat to all of us, particularly because most consumers are unaware of the existence—let alone the scope—of these invasive practices. We strive to offer technological solutions to these problems, but we believe that technology paired with regulation offers the greatest potential to spur significant, positive changes for consumer privacy. We conclude by responding to the NTIA's requests for comment on implementing the multistakeholder process and ensuring that it receives the public attention and input that it requires.

1. Introduction

[1] http://www.abine.com

Now is a critical time for privacy. As our lives become increasingly intertwined with technology, so do our identities: we are the sum of our online and offline parts. Our privacy is just as important on the Internet as it is on the street, in a store, or in a car. And despite having a fundamental liberty interest in privacy in our physical worlds, our protections on the Internet are much hazier.

We applaud the Administration's recognition of the importance of privacy protections in its framework, "Consumer Data Privacy Protections in a Networked World"[2] ("the Framework"). In addition to noting that "Americans have always cherished our privacy" and that privacy "has been at the heart of our democracy from its inception," the Administration described the breadth of privacy's importance: it's "about much more than solitude or secrecy," but the freedom to live life as one wishes, to express oneself without fear of surveillance or repercussions, to associate with others, to "engage in commerce, to participate in the political process, or to seek needed health care."[3] We aren't the same when we're being watched, when everything we do is collected, stored, and sold. Privacy is freedom.

But privacy is being eroded. Privacy violations tend not to be flagrant or undeniable; they are gradual, steady, and creeping. Many are not observable to the average Web user. Approve this application here; sign up for this rewards card there; fail to realize that a website has foisted a less protective Privacy Policy upon you. Most Americans don't realize that we're leaving a digital data trail in our wake, a path that builds up alarmingly detailed profiles about all of us. We're accepting more privacy intrusions each day, sometimes because we don't realize that what we're giving out, other times because we don't feel we have a choice, other times because the harm of this isolated transaction seems so remote. As our collective expectation of privacy shrinks, so do our Fourth Amendment protections.

Through our work on our Do Not Track Plus ("DNT+") browser add-on and other privacy software, we are intimately familiar with the tactics of online tracking and data collection. Invisible advertising networks and tracking technologies follow consumers across the web, building profiles of them and their activities in order to target them with ads. When consumers sign up for online accounts, websites often sell their personal information to third parties. Only one or two out of one thousand Web users read privacy policies, End User License agreements, or Terms of Use, so most consumers are not aware of the tradeoff.[4] Even if they do read these policies, 94% of them use sophisticated language that exceeds the reading comprehension level of a high school education. Even if consumers could understand the policies, they simply lack the time to read them: "reading privacy policies carry costs in time of approximately 201 hours a year, worth about $2,949

[2] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," Feb. 23, 2012.
[3] *Id.* at C3.
[4] Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts* (N.Y.U. Law & Economics Research Paper No. 09-40, October 6, 2009), *available at* http://ssrn.com/abstract=1443256.

annually per American Internet user."[5] FTC Chairman Jon Leibowitz correctly summarized that "[w]e all agree that consumers don't read privacy policies – or EULAs, for that matter."[6]

Once collected, our data ends up in unexpected—and unwanted—places. Spam emails, inclusion in harmful information databases, and identity theft can follow. From Facebook to forums, almost everything consumers do online is bought and sold to the highest bidder. Although the Internet offers wonderful things, much of its "free" content is paid for with the personal information of consumers, people who never knew of or agreed to this trade. Abine's goal is to empower consumers to continue to browse, interact, and shop online while taking control back over their private information.

The privacy goals that the Framework puts forth are commendable, and this moment offers us a terrific opportunity to define our privacy rights for the better. Implementing the Consumer Privacy Bill of Rights depends on input from various stakeholders in the privacy industry, and we are responding to that request for input. We hope that others speak up to say what they'd like the future of privacy to hold.

2. About Abine

Abine is the product of three consumer privacy veterans with over 50 combined years of security and technology experience who thought that the collection, surveillance, and visibility of what used to be private information online had become a concern. Abine's executive team combines talented minds from MIT, Stanford, and Cornell with varied backgrounds in engineering, finance, entrepreneurship, technology, economics, data security, venture capitalism, and consumer-web startups. Our extensive experience in many industries provides a comprehensive, holistic perspective on privacy issues. Abine's technologies have been used by millions, with customers downloading its most recent tool, Do Not Track Plus, more than 750,000 times since its February 2012 launch.

Our software and services provide us with special insight on privacy, particularly as it relates to online tracking and data brokers. Our DNT+ software shows users the invisible tracking devices that are behind almost every website, blocking or opting out of their tracking by default. One of DNT+'s unique features is its blocking of social network tracking through buttons and widgets, such as Facebook's Like and Connect buttons. DNT+ is our attempt to educate and protect users regarding covert Internet tracking technologies. Our DeleteMe service opts customers out of having their information publicly displayed and sold on certain data broker websites. We created DeleteMe to address the privacy, complexity, and time-management concerns that data brokers raise. We also offer Protected Search, an add-on that runs users' Google searches through a proxy server to

[5] Aleecia McDonald and Lorrie Cranor, *The Cost of Reading Privacy Policies,* 4 I/S: J.L. & Pol'y for Info. Soc'y (2008) *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[6] Leibowitz, Chairman, Fed. Trade. Comm'n, Introductory Remarks at the FTC Privacy Roundtable, Dec. 7, 2009, *available at* http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf.

prevent their searches from being tied back to their Google profile. Our privacy offerings continue to grow and evolve with the needs of consumers.

3. Data Brokers

A new privacy concern has emerged and grown in recent years: publicly searchable Internet databases that sell consumers' names, addresses, phone numbers, family members, criminal histories, and more. Intelius.com, Spokeo.com, BeenVerified.com, and WhitePages.com are a few notable examples of these data brokers, commonly referred to as "people search sites." Data brokers "aggregate personal data from multiple sources, often without interacting with consumers at all. Such companies face a challenge in providing effective mechanisms for individual control because consumers might not know that these third parties exist."[7]

Consumers don't have much say in how data brokers display their personal information because the practice is legal. Most data brokers claim that they obtain this information through publicly-available sources, information that's either classified as "public record," such as court records, or content that consumers voluntarily post publicly, such as on social networks. This public records classification, however, is from a pre-Internet era. To obtain a background check even 20 years ago, a person would have to go down to the county clerk's office and show his face, make the request, pay a small fee, receive a folder, make copies, and be on his way. It was a hassle, but that hassle protected people's privacy while balancing free speech rights to access certain information.

Today, anyone can stay at home, pay several dollars, and access entire life histories online. The old public records laws were meant to deal with the pre-Internet world. They do not adequately protect our online generation. "Public record" has now become super-public with the advent of the Internet, and records are far more accessible and visible than they've ever been. In line with the Consumer Privacy Bill of Rights call for a Respect for Context,[8] the context of public record laws—from the legislative history behind their inception to the practicalities of accessing public information—has completely shifted. Providing one's personal information for the purpose of obtaining a marriage license, for example, does not align with the unexpected context of seeing that same information resurface for sale on a data broker website.

Although many consumers do not realize that their information is so easily accessible online,[9] those who do often wish to remove themselves.[10] These sites are not merely

---

[7] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," Feb. 23, 2012, at 13.
[8] *Id.* at 15.
[9] FTC Commissioner Julie Brill remarked, "To consumers, the practices of data brokers are unknown. Indeed, consumers are often unaware of the existence of data brokers." Julie Brill, Commissioner, Remarks at the Big Data, Big Issues Symposium, Fordham University School of Law, Mar. 2, 2012, *available at* http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.
[10] After a Consumers Union poll found that 82% of 2006 surveyed respondents were "concerned about companies selling or sharing their information without permission," HearUsNow.org launched a public

unsettling: they facilitate stalking, identity theft, and unsolicited marketing.[11] Consumers don't have a say in whether they're listed, and the sites make it difficult and time-consuming to remove listings. It is a frustrating maze of red tape, faxes, mailings, and Terms of Use.[12]

There are over 180 different data brokers, and that number continues to rise.[13] Many data brokers are co-owned or affiliated and share databases, but do not publicly share these relationships. As such, consumers find themselves sending multiple, separate opt-outs to what appear to be different companies located at the same address or fax number. For example, Intelius, Inc. owns the information and controls the opt-out requests for approximately 70% of the data broker industry, including Intelius.com, Zabasearch.com, PublicRecordsNow.com, USSearch.com, PeopleLookUp.com, LookUpAnyone.com, PhonesBook.com, and iSearch.com.[14] The same is true for Confi-Chek, which owns Veromi.com, CriminalSearches.com, PrivateEye.com, EnformionUSA-People-Search.com, PublicBackgroundChecks.com, and PeopleFinders.com, among others.[15] The lack of transparency surrounding these relationships adds to the time-consuming and difficult nature of opt-outs.

a. Current Opt-Out Processes

Given the variety of opt-out processes, the high number of websites, and the confusing web of interrelated partnerships among websites, removing one's information is a daunting, if not virtually impossible, task. Even with practice and knowledge, the 18 removals that DeleteMe performs for customers take several hours and are repeated 4 times per year (once each quarter), requiring a fax machine, postage, envelopes, a printer, paper, a

---

initiative in September of 2011 to encourage individuals to contact their congressional representatives about data brokers. http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html, https://secure.consumersunion.org/site/Advocacy?cmd=display&page=UserAction&id=2555

[11] The nonprofit consumer organization Privacy Rights Clearinghouse lists additional negative consequences of electronic public records, including "less participation in public life," "justice only for the rich," "destruction of reputations," "secondary uses of information," "loss of social forgiveness," and the creation of an Orwellian "dossier society." Beth Givens, *Public records on the internet: the privacy dilemma*, PRIVACY RIGHTS CLEARINGHOUSE, Mar. 2006, https://www.privacyrights.org/ar/onlinepubrecs.htm. For these reasons, domestic violence groups such as WomensLaw.org recommend that victims remove their personal information from the internet, including data broker websites. http://www.womenslaw.org/laws_state_type.php?id=13404&state_code=PG&open_id=all#content-13488. The Privacy Rights Clearinghouse advises victims of stalking on how to "guard [their] personal information and lessen the chance that it will get into the hands of a stalker or harasser," urging victims to opt out of data broker websites "when possible if you believe they have accurate contact information for you." https://www.privacyrights.org/fs/fs14-stk.htm#6

[12] For a list of 24 of the largest people search websites' opt-out procedures, visit http://abine.com/optouts.php.

[13] https://www.privacyrights.org/online-information-brokers-list

[14] The domain registration record for Zabasearch.com, for example, shows that Intelius owns the domain. http://whois.domaintools.com/zabasearch.com

[15] In its Privacy Policy, PeopleFinders.com discloses that Confi-Chek, Inc. is its parent company. http://www.peoplefinders.com/privacy.aspx. *See also* Melane Turner, *Looking for someone? Web site can help*, SACRAMENTO BUSINESS JOURNAL, Jul. 18, 2008, available at http://www.bizjournals.com/sacramento/stories/2008/07/21/story9.html.

computer with an internet connection, a telephone, and a number of computer programs and browser applications.

These opt-out procedures vary greatly.[16] Some are online, requiring consumers to locate their listing, enter information about themselves, complete a CAPTCHA, and click a verification link sent to their email address.[17] Others require faxing a lengthy opt-out letter and a copy of one's photo identification to the people search company. A typical letter must contain a consumer's first name, last name, middle initial, aliases and AKA's, complete current address, complete previous addresses going back 20 years, and date of birth. Others require a hard-copy mailing of the letter and identification above. Others require a phone call to the website's customer service department.[18] The data broker BeenVerified.com requires an email to their support team containing the personal information listed above, with the additional requirement of providing one's listed family members:[19]

> Your name as shown on our site
>
> Your Age
>
> Current address (City, State, Zip)
>
> Previous addresses
>
> Listed Relatives

b. Risks of Imminent Harms to Consumers

Many consumers have legitimate concerns about their names, addresses, and other personal information being available online, particularly persons in at-risk groups such as domestic violence victims, law enforcement officers, and judicial officers. We prefer to keep this information private, both for our mental and physical safety. We share it with those we trust and guard it from the public at large, often out of fear that dangerous individuals will threaten or impose upon us at our most sacred place: our home.

The Administration expresses its version of the harm principle on page 6: "Individuals who actively share information with their friends, family, colleagues, and the general public through websites and online social networking sites may not be aware of the ways those services, third parties, and their own associates may use information about them. Unauthorized disclosure of sensitive information can violate individual rights, cause injury or discrimination based on sensitive personal attributes, lead to actions and decisions

[16] For a list of 24 of the largest people search websites' opt-out procedures, visit http://abine.com/optouts.php.
[17] Spokeo.com uses this method. *See* http://www.spokeo.com/privacy.
[18] MyLife.com uses this method. *See* http://www.mylife.com/faq.pub.
[19] http://www.beenverified.com/faq

taken in response to misleading or inaccurate information, and contribute to costly and potentially life-disrupting identity theft."

Numerous address confidentiality laws reflect this sentiment by allowing certain groups of people to keep their contact information out of public view. See, e.g., Illinois's Address Confidentiality for Victims of Domestic Violence Act,[20] California's Confidential Records Address of Public Officers and Employees,[21] and Pennsylvania's Address Confidentiality Program.[22] At-risk groups include victims of stalking, prosecutors, child abuse investigators, members of Congress, police officers, city council members, judges, trial court employees, employees of the Department of Motor Vehicles, psychiatric social workers, and the spouses of all of the above.[23]

Domestic violence groups such as WomensLaw.org recommend that victims remove their personal information from the internet.[24] The nonprofit consumer organization Privacy Rights Clearinghouse[25] advises victims of stalking on how to "guard [their] personal information and lessen the chance that it will get into the hands of a stalker or harasser," urging victims to opt-out of people search websites "when possible if you believe they have accurate contact information for you."[26] It's not a far stretch to wonder how often data brokers leads rapists and stalkers to their victims' front doors, as one anonymous author recently wrote about Spokeo.com:

> The whole issue of Spokeo and online privacy reminds me of the victim-blaming rhetoric I hear so much of every day. According to this rhetoric, it's the victim's responsibility to stay safe by protecting her own data. But I did that, and my rapist found me anyway, possibly because Spokeo made it easy. That site and sites like it put me and victims everywhere in danger.[27]

In addition to the safety concerns above, having one's personal information available for viewing and sale on people search websites makes one more vulnerable to identity theft. In 2009, researchers at Carnegie Mellon University demonstrated that knowing an individual's state and date of birth, both of which are sold for a negligible amount on people search websites, allowed prediction of that individual's Social Security Number in a

---

[20] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2101&ChapterID=59. This statute was based upon legislative findings that "persons attempting to escape from actual or threatened domestic violence frequently establish new addresses in order to prevent their assailants or probable assailants from finding them. The purpose of this Act is to enable State and local agencies to respond to requests for public records without disclosing the location of a victim of domestic violence, to enable interagency cooperation with the Attorney General in providing address confidentiality for victims of domestic violence, and to enable State and local agencies to accept a program participant's use of an address designated by the Attorney General as a substitute mailing address." *Id.*

[21] http://www.dmv.ca.gov/pubs/vctop/d02/vc1808_4.htm

[22] http://www.pcadv.org/Domestic-Violence-Information-Center/Address-Confidentiality/

[23] *Id.*

[24] http://www.womenslaw.org/laws_state_type.php?id=13404&state_code=PG&open_id=all#content-13488

[25] https://www.privacyrights.org/

[26] https://www.privacyrights.org/fs/fs14-stk.htm#6

[27] "Did My Rapist Find Me On Spokeo?" http://jezebel.com/5890590/did-my-rapist-find-me-on-spokeo

significant number of trials.[28] The Social Security number is "one of the pieces of information most often sought by identity thieves: knowledge of a person's name, SSN, and data of birth, is often a sufficient condition to impersonate that individual and obtain access to a variety of services."[29]

The Carnegie Mellon researchers used a data broker, PeopleFinders.com, as an example of a source of personal information that leads to prediction of Social Security Numbers and thus identity theft:

> Mass amounts of birth data for US residents can be obtained or inferred - often for free, or at negligible per unit prices - from multiple sources, including commercial data brokers (such as www.peoplefinders.com, which sells access to birth data and personal addresses for ``almost every adult in the United States'')...[30]

The Identity Theft Assistance Center reports that 8.1 million adults in the U.S. suffered identity theft in 2011, each of whom lost an average of $4,607.[31]

Although most data brokers state that they fall outside the reach of the Fair Credit Reporting Act (FCRA) and forbid purchasers of their data from using it for hiring, housing and employment, it is naïve to assume that purchasers never use background checks for these sensitive purposes. FTC Commissioner Julie Brill has stated her concerns on this issue:

> I have long been concerned about data that are used in place of traditional credit reports to make predictions that become a part of the basis for making determinations regarding a consumer's credit, his or her ability to secure housing, gainful employment or various types of insurance.[32]

Look at what happened to Kathleen Casey, a woman who was denied employment after a background check had incorrectly reported that she had several felony convictions.[33] Her record was clean, but an error in the background check linked someone else's 14 convictions to her.[34] When people like Kathleen Casey lack the knowledge that their information is sold by data brokers or the right to ensure that data about them is accurate, yet lose out on employment opportunities because of errors, their conundrum evokes many of the same concerns present in substantive due process cases. Employers are

---

[28] http://www.heinz.cmu.edu/~acquisti/ssnstudy/
[29] *Id.*
[30] http://www.heinz.cmu.edu/~acquisti/ssnstudy/
[31] http://www.identitytheftassistance.org/pageview.php?cateid=47
[32] "Brill To Brokers: Give Consumers Access To Their Data," *IAPP*, https://www.privacyassociation.org/publications/2012_01_27_brill_to_brokers_give_consumers_access_to_their_data
[33] Robertson, Jordan. "When your criminal past isn't yours," ASSOCIATED PRESS, Dec. 20, 2011, http://finance.yahoo.com/news/ap-impact-criminal-past-isnt-182335059.html
[34] *Id.*

judging potential hires based on their background checks, yet the potential hires cannot respond to or even view the content of their own files.

c. Patterns of Consumer-Unfriendly Behavior

Many data brokers have exhibited deceptive behavior and intentionally obtuse opt-out practices in the past. In 2005, the data broker ChoicePoint settled with the FTC after a data breach of more than 163,000 consumer records, paying $10 million in civil damages and $5 million in consumer redress.[35] The breach led to 800 verified cases of identity theft.

Intelius's network of sites has come under fire in the past for deceptive marketing,[36] unauthorized charges to customers' credit cards,[37] having inaccurate data,[38] not honoring opt-out requests,[39] and having a complicated opt-out process.[40] TechCrunch's Michael Arrington reported that Intelius CEO Naveen Jain left another company he founded "in disgrace in late 2002 after violating insider trading laws." Intelius has received hundreds of complaints to the Washington State Attorney General's Office, the Better Business Bureau, and the Federal Trade Commission, and has been sued numerous times. In fact, Intelius or Intelius-owned sites made up 11.9% of *all* FTC complaints in 2005-2006.[41]

In 2010, another Intelius partner site, USSearch, settled with the FTC over charges that its PrivacyLock service, for which consumers paid $10 to remove their personal information from sale and public view, was deceptive.

In 2011, Abine filed an FTC complaint against BeenVerified for allegedly deceptive business practices when the data broker appeared to re-post supposedly removed personal information every three months.[42]

d. Open Questions and Issues Needing Clarification

Due to a lack of consumer awareness of the existence of data brokers, complex opt-outs, severe risks of harm, and an industry history of deceptive behavior, the current state of the

---

[35] "ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress," Federal Trade Commission, Jan. 26, 2006, http://www.ftc.gov/opa/2006/01/choicepoint.shtm

[36] Johnson, Gene. "Intelius to pay $1.3M for deceptive marketing," THE STATESMAN, Aug. 10, 2010, http://www.statesman.com/business/technology/intelius-to-pay-1-3m-for-deceptive-marketing-852344.html

[37] Shapiro, Nina. "Intelius and the Dubious Art of 'Post-Transaction Marketing,'" SEATTLE WEEKLY, Mar. 18, 2009, http://www.seattleweekly.com/2009-03-18/news/intelius-and-the-dubious-art-of-post-transaction-marketing/

[38] *Id.*

[39] Blue, Violet. "How to Remove Yourself from People Search Websites," ZDNET, Aug. 16, 2011, http://www.zdnet.com/blog/violetblue/how-to-remove-yourself-from-people-search-websites/612

[40] http://en.wikipedia.org/wiki/Intelius

[41] KnowPrivacy.org, http://knowprivacy.org/complaints.html

[42] Angwin, Julia. "Sites are accused of privacy failings," WALL STREET JOURNAL, Feb. 13, 2012.

data broker industry is unacceptable to consumers. Five key categories require clarification and investigation.

i. Data Accuracy

Data brokers have a lot of our personal information and we can neither see nor correct it. As we described in Section (3)(b) above, there are cases of this information being used for employment and other sensitive purposes. We have seen extensive examples of inaccurate consumer data through our DeleteMe service. Multiple listings for the same person, misspellings, incorrect addresses, grossly inaccurate estimations of net worth, and other errors are common. Whether the inaccuracies are due to scraping from unverified sources, a lack of quality control oversight, internal problems with data organization, or something else, they benefit neither consumers nor data brokers.[43]

ii. Opt-Out Definition and Process

The term "opt out" has come to describes the process that data brokers offer to suppress one's personal information. However, the definition of "opt out" is unclear. Is an opt-out a complete, permanent deletion of that person's records from a database, or does it merely suppress the records from public view but keep them in the database? Are opted-out records still sold? If a record is deleted or suppressed, how long does that effect last? Does an opt-out on one site carry over to partnered or affiliated sites? What information is included in an opt-out?

The data broker industry needs to assess whether its concept of an opt-out aligns with consumer understanding and expectations. For example, most consumers seek to delete their information permanently from information databases, so a suppression-only solution may not meet their privacy expectations.[44] Furthermore, a data broker's concept of what information should be opted out may be too technical and confusing to satisfy consumers. We expect that data brokers will argue that they are not repopulating opted-out information, but that they are collecting new, independent information from their data sources. These companies may argue that their data collection process is automatic and outside their control. The data source distinction, however, is immaterial to reasonable consumers. If consumer A seeks to remove his name, he does not care whether his name came from data source 1 or 2; Facebook or a supermarket rewards card, for example. All that matters is that his name is publicly available on the site, despite his opt-out and in contravention of the company's opt-out statements. Reasonable consumers who undertake opt-outs do so to remove their information from data brokers. That purpose is thwarted when the information returns, regardless of its source.

---

[43] We note that some consumers who wish to throw others off their trail may be happy with inaccurate data.

[44] Ninety-two percent of adult Americans surveyed agreed that there should be a law that requires "websites and advertising companies to delete all stored information about an individual if requested to do so," and 66% believe that advertisers should be legally required to delete information about their Internet activity immediately, whether consumers request it or not. Turow et al., "Americans Reject Tailored Advertising and Three Activities that Enable It," Sept. 29, 2009, available at SSRN: http://ssrn.com/abstract=1478214 or http://dx.doi.org/10.2139/ssrn.1478214.

Another area of concern regarding opt-outs is whether data brokers recycle information that consumers provide in their removal requests to update those consumers' listings. Intelius states in its Privacy Policy that it uses this information for opt-out purposes only, but other data brokers are less clear.[45] This question requires further investigation and explanation.

iii. Transparency of Data Sources

Data brokers rely on the public records classification to justify their access to, and treatment of, consumer data. However, comprehensive investigation is warranted to determine if these sources are, in fact, open to the public, or whether some come from private, closed sources. Data sources lie on a spectrum from legitimately public, and thus covered by public records law, to legitimately private:[46]

- actual public records, such as a trademark filing or public FTC comment
- information provided in exchange for a benefit, such as a rebate or warranty card
- information voluntarily disclosed to social networks on a *public* sharing setting
- information provided for one purpose and taken far out of context (for example, signing up for an account on a pizza delivery website and learning that Acxiom purchased it)
- information inaccessible to the general public, e.g., a private marketing database
- information voluntarily disclosed to social networks on a *private* sharing setting
- information obtained illegally, e.g., through a data breach

In order to make more informed decisions about how and with whom they share their information, consumers need to know how their personal data ends up with data brokers. If they knew that sending in a rebate card would result in their email address being sold on Spokeo.com, some consumers would think twice about the value of that action. The Respect for Context principle highlights this relationship between providing data for one source and later seeing that data in another source. Just as data brokers are responsible for how they acquired data, the original sources should be equally forthcoming.

In addition to being forthcoming about the sources of their information, data brokers should be transparent about the relationships between different sites and companies. Although all data brokers have minimal contact with the consumers whose information they sell, some brokers are more visible than others. Parent companies tend to be difficult to identify, as is the case with Confi-Check.[47] Some of the largest data brokers, which actually sell to other brokers further down the information stream, are also the least known: for example, Acxiom.com is "one of the biggest companies you've never heard of."[48]

---

[45] http://www.intelius.com/privacy.php.

[46] By listing these examples in this order, we mean to convey a general sense of the spectrum from public to private. We do not intend for our examples to be interpreted as a literal, linear progression of magnitude.

[47] *See* Section 3, *supra.*

[48] "The Persuaders," FRONTLINE, 2004, http://www.pbs.org/wgbh/pages/frontline/shows/persuaders/etc/script.html

More consumer-facing data brokers should not be disproportionately penalized because they are more visible than others.

Another key element of transparency is these companies' accessibility for consumer support. Knowing which companies share databases and resources, as well as how to reach these companies, could save consumers the considerable effort of doing their own reconnaissance work. To provide one example, it is unacceptable for a consumer wishing to contact the data broker DOBSearch.com to have to read the site's entire Terms of Use,[49] locate a mention of a parent company Concert Technologies, Inc., and run several searches for Concert Technologies Inc.'s corporate filings just to find that the company is based out of Charles Town, West Virginia, and can be reached at (304) 724-2113.[50] This sort of deliberate obtuseness stands in stark contrast to the Administration's call for data brokers "to compensate for the lack of a direct relationship [with consumers]" by being more forthright and accessible.[51]

iv. Compliance

As we have heard from our DeleteMe customers, consumers have concerns over compliance mechanisms for opt-outs. Data brokers have all the power in their relationship with consumers: the brokers control the information and the opt-out process. Consumers cannot even see their own information. Many questions arise: who, if anyone, ensures that data is accurate? Who ensures that opt-outs are honored, or even offered?

Abine has sought to offer some compliance assurance through our DeleteMe service: we search for our customers' personal information on a list of the major data brokers, record the information we found through screen shots and other methods, submit opt-outs, and repeat the process every 3 months. Although most sites do comply, it's important to note that we only include data brokers on our removal list if they offer a removal option, which many do not. Furthermore, seeking compliance often takes repeated opt-outs and consistent monitoring. A consumer's only realistic option is to file an FTC complaint when observing non-compliance.

v. Special Care for High-Risk Groups

As we described in Section (3)(b) above, it is critically important that certain at-risk groups be able to quickly and effectively suppress their personal information from public view. Several of these groups include battered women, victims of stalking or domestic violence, past and present members of law enforcement, individuals who have suffered identity theft, and judicial employees. Even if data brokers are resistant to do the same for consumers at large, data brokers should offer these special groups an immediate, simple, easily-accessible, and universal opt-out.

---

[49] http://www.dobsearch.com/terms.php

[50] http://www.westvirginia-companies.com/companies/concert-technologies-inc.html

[51] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," Feb. 23, 2012, at 15.

Many members of these groups may be hesitant to provide their information to data brokers or include themselves in databases of similarly at-risk individuals, even if the purpose of such data sharing is for their protection. Whichever solution is implemented should carry enforceable guarantees of security and privacy.

4. Our Recommendations for Data Brokers

The FTC's public statements in recent months suggest that they envision a 2-tiered approach to data broker opt outs. Commissioner Brill said,

> Just six weeks ago, I called on the data broker industry to develop a user-friendly, one- stop shop that will give consumers information about who the data brokers are, and provide access to information that data brokers have amassed about them. If a consumer learns that the data broker sells her information for marketing purposes, she should be able to opt-out.[52]

Statements like these seem to say that the first tier, which would always be available, is a single location where consumers can view all the information that data brokers have about them and correct the accuracy of their data if necessary. The second tier, an actual opt-out, seems to be available to consumers only if particular data brokers are selling their information for marketing purposes.

Assuming that we are interpreting the Commission's intent correctly, this two-tiered approach seems both difficult to implement and short of consumers' desires to remove their information from these databases, not merely view it. We applaud the FTC's efforts to provide data broker transparency, and we want to work together to develop a workable solution.

There are several key questions that need to be addressed. Who would verify that data brokers were selling information for marketing purposes, and what activities will be defined as "marketing purposes?" We argue instead that a true one-stop shop will allow consumers two simultaneous options: (1) opt out of having their information publicly displayed and/or sold by data brokers, and (2) editing their information to ensure that it is correct. Consumers could choose to do one, both, or none of these options.

In describing how such a system does not exist, the data broker BeenVerified.com ironically describes both the system that we believe consumers deserve and some of the problems with the status quo:

> Please note that we cannot guarantee like or similar records from reappearing in the future. Public records come from multiple sources and are constantly being updated

[52] Julie Brill, Commissioner, Remarks at the Big Data, Big Issues Symposium, Fordham University School of Law, Mar. 2, 2012, *available at* http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

> and there is no one universal system for identifying individuals that can provide a total opt out.

Opponents to such a system may argue that this information is already in the public record and that forcing its removal harms data brokers and impedes on their rights to free speech. In fact, the Administration noted the importance of balancing both sides:

> The rights of freedom of speech and freedom of the press involved in the collection and use of these documents must be balanced with the need for transparency to individuals about how data about them is collected, used, and disseminated and the opportunity for individuals to access and correct data that has been collected about them.[53]

We have several responses. First, the First Amendment certainly is important, but it is not boundless. The speech at issue—data brokers' aggregation and sale of personal information—is commercial, making infringements upon it subject to the less stringent intermediate scrutiny test. Implementing a universal opt-out must further an important government interest in a way that is substantially related to that interest. The government interests at stake include privacy, personal safety, and due process,[54] all critical matters. Offering an opt-in and non-mandatory choice to consumers to remove their information is substantially related to protecting these critical interests.

Second, public record information will still be available and obtainable through the original public record sources, data brokers when consumers choose not to opt-out of them,[55] and through any other means that consumers disclose voluntarily and intentionally. Public record legislation encourages more accurate recordkeeping with greater assurances of accuracy, including designated custodians of information, procedures for viewing and copying information, definitions of which materials constitute public records, and limits on fees.[56] Primary sources are simply more accurate: each source removed is analogous to a game of telephone, with each source further down the data supply chain being less accurate and with less oversight than the one before it. Although one of the greatest benefits of the Internet's advent is greater accessibility and visibility of information, this benefit does not exist in every case. With data brokers, the harm to and concern of vast numbers of consumers outweighs the benefit to a small number of commercial stakeholders in the data broker industry.

---

[53] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," Feb. 23, 2012, at 13.

[54] *See* Section 3, *supra,* for a discussion of how the availability of personal information through data brokers leads to various types of harms.

[55] Although the data brokers are the only ones with accurate records of how many opt-out requests they receive each year, we suspect that a negligible percentage of the United States population currently asks to be removed. We invite data brokers to respond with their own figures. Data brokers are also free to offer consumers incentives to keep their information in their databases. One incentive could be to offer consumers a portion of the profit that the data broker receives from selling their information.

[56] A state-by-state list of public record legislation is available at http://www.lc.org/hotissues/2001/aba_1-18/public_records_laws_by_state.htm.

a. *Preferred Solution: Establish a One-Stop Shop for Opting Out*[57]

Whether it is established by the Administration, the FTC, the data broker industry, consumer rights organizations, or another group or entity, consumers need a simple, one-step opt-out through which they can block their information from being sold by data brokers. We envision a solution similar to the National Do Not Call Registry for telemarketing.

A solution that is both effective and satisfying to consumers will contain several key elements. It must be (i) an opt-out, (ii) universal, and (iii) simple.

i. What Constitutes an Opt-Out?

Keeping in mind that data brokers run the gamut of visibility and search functionality—some are almost completely hidden from consumer view and do not publicly display listings (e.g. Acxiom), while others offer a public search function that therefore may appear more alarming to consumers (e.g. PeopleFinders.com)—an effective opt-out must address all varieties of these companies. The complex nature of the industry should not penalize consumers.

An opt-out should:

- [For those companies with public search and display features] Remove the requested information from public view, such as through a search feature on the data broker's website or through advertisements containing that consumer's personal information
- Remove all information reasonably connected to the requested opt-out (i.e., if a consumer with 20 previous addresses makes an opt-out request that only includes the 10 most recent addresses, and the data broker is reasonably able to discern that other records belong to the same person, the data broker must remove those records. In other words, assuming the consumer provides sufficient information to identify his or her records with reasonable certainty, the burden should be on the data broker to remove them.)
- Eliminate the option to purchase the opted-out information
- Apply to all data brokers (see Section (4)(a)(i) on universality below)

[57] Note that Abine supports a universal opt-out solution despite the fact that simplified, well-publicized, and consistently upheld opt-out procedures could theoretically decrease the need for services like DeleteMe that work on behalf of consumers to remove their information from data brokers. We believe that individual privacy and safety is far more important than our potential revenue. We recognize that our extensive experience with people search sites and opt-out procedures is accompanied by a duty to share that knowledge to protect consumer privacy and support transparent business practices. To that end, we have publicly posted instructions for consumers who wish to remove themselves from 24 of the largest people search websites at http://abine.com/optouts.php.

- Persist for a significant time period (given that the National Do Not Call Registry lasts as long as a consumer keeps his or her phone number, which could be indefinitely, we think that five years or longer is a reasonable length for an opt-out)
- Not use the information submitted for the opt-out for any purpose besides the above, be destroyed after these purposes are fulfilled, and expressly state this fact to consumers

Notice that we do not request that an opt-out compel data brokers to delete the information from their internal databases. Consumers' worries surround the sale and publicity of their data, so if the brokers wish to use it in some internal way, perhaps for organization or more effective opt-outs, than we see no reason to prohibit it.

ii. Universality and Compliance

Because the majority of consumers know little to nothing about data brokers, let alone that their information is listed and sold, an effective opt-out system must cover all companies. As we have seen through our DeleteMe service, opt-outs are a full time job: they are complex and time-consuming, and the list of data brokers continues to grow. If a concerned consumer wishes to protect her information, it is unrealistic to expect her to have the time or knowledge to do so on over 180 sites. The opt-out process should extend across all reasonably identifiable sites in the industry—online and offline, mobile and desktop—and include a measure of determining and reporting on compliance. FTC Commissioner Brill has asked for precisely this system:

> I call on the data broker industry to develop a system where a consumer's corrections to one data broker's files will automatically correct the same information held by other data brokers. It is critical that all data brokers come to the table to develop this mechanism—including those in the mobile space.[58]

If the industry itself is best equipped to understand the opt-out process and the companies in the industry, perhaps self-regulation solution is the best-suited solution. Companies with a record of compliance could be rewarded with a seal or other indicator of approval, and compliance histories should be publicly available.

iii. Simplicity

The ideal opt-out system is simple. The complexity of current opt-outs dissuades consumers from undertaking them. Whether they're difficult to ascertain, require the use of faxes and other outdated equipment, or compel the disclosure of an uncomfortable amount of personal information, the process is too unmanageable. In contrast, a consumer-friendly opt-out has several features:

- It is publicly available

[58] Julie Brill, Commissioner, Remarks at the Big Data, Big Issues Symposium, Fordham University School of Law, Mar. 2, 2012, *available at* http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

- It is free
- It can be completed online (thus it must not require the use of paper mailings, faxes, or other antiquated methods)[59]
- It requires the minimal amount of personal information needed to locate and suppress the correct record[60]
- Consumers can find it easily (e.g., the opt-out is no deeper than two pages into a website and/or it contains metadata to ensure that it appears in search engines)

Note that we do not specify the exact terms of the opt-out itself—we leave those details up to the data brokers.

b. Secondary Solution: Establish a 1-Stop Shop for Viewing Data and Checking Accuracy

We strongly support both an opt-out and data correction option. However, given the FTC's apparent proclivity to implement the latter, we acknowledge that one step forward to give consumers greater control over their information is better than none. The Administration seems to agree in its Access and Accuracy principle:

> Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation.[61]

The Control and Transparency principles further highlight the need to view and correct information.[62] The same characteristics from points (4)(a)(ii) and (4)(a)(iii) above should apply to the system for correcting one's information, with the additional caveat that consumers should not receive any penalty for checking their information.

5. Do Not Track and Online Advertising

Every time consumers go online, hundreds of companies monitor, collect, and sell their activities.[63] These companies build detailed profiles of users based on information like

---

[59] There should also be a telephone version for the less technologically savvy or those without Internet access.

[60] Some data brokers argue that they need highly personal identifiers, such as drivers' licenses, as authentication for opt-outs. Because we have yet to encounter a consumer who wants to be listed on a data broker website, we doubt that such stringent authentication is necessary. If a consumer had his information opted-out by mistake, we think he would view it as a fortunate act. We may ultimately have to defer to the brokers to determine how much information is necessary.

[61] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," Feb. 23, 2012, at 19.

[62] "Data brokers and other companies that collect personal data without direct consumer interactions or a reasonably detectable presence in consumer-facing activities should seek innovative ways to provide consumers with effective Individual Control…[they should be] providing appropriate use controls once information is collected under the Access and Accuracy and Accountability principles to compensate for the lack of a direct consumer relationship." *Id.* at 13.

[63] We maintain a list of these companies at http://www.donottrackplus.com/trackers/index.php.

their geographical location, purchases, clicks, site visits, articles read, things shared, ethnicity, search queries, gender, and email content. These companies use consumers' online activities to guess at who consumers are, and thus what they're likely to be interested in and purchase. Consumer data has become the currency of today's Web, but most consumers aren't aware of the tradeoff.

a. Abine's Background in Privacy Software

Abine's three consumer privacy software options are Do Not Track Plus, TACO, and PrivacySuite. They present a range of tracker-blocking methods. We started in 2010 by acquiring TACO, which stands for Targeted Advertising Cookie Opt-Out, from its developer, Christopher Soghoian.[64] The original TACO worked by setting 27 opt-out cookies on a user's computer.[65] Each of the participating 27 ad networks, members of the Network Advertising Initiative (NAI),[66] offered an opt-out cookie for itself; when the ad network came across its own opt-out cookie, it refrained from at least targeting consumers with personalized ads, and at most restricting or stopping data collection. The terms depended on that particular ad network's opt-out policy. TACO set these opt-out cookies permanently so that ad networks would refrain from tracking users with these cookies enabled.[67] The permanent opt-out was important because it prevented users from accidentally deleting them when they cleared their browser caches.

With Do Not Track Plus we have implemented more varied and aggressive techniques to block tracking, including completely blocking tracking requests and broadcasting the Do Not Track HTTP header, in addition to setting NAI opt-out cookies. Do Not Track Plus examines each outbound request a browser receives. We evaluate that request, and if we think it's a tracking request (like a web beacon or tracking Javascript), we block it from being made. If we block the request, then no connection is established between the user's computer and the remote server for that request. We block tracking requests from third-party domains, as well as first-party requests for known tracking code.[68]

b. Overview of the Current State of Online Tracking

i. Hundreds of Ad Companies and Tracking Technologies Collect Detailed Personal Information

Abine has identified more than 200 different companies and 600 different tracking technologies through our work with three software options that block and opt out of online

[64] "Abine Acquires TACO, A Leading Privacy Add-On," Abine, Jun. 2010, http://www.abine.com/news/20100615_1.php.
[65] Kirk, Jeremy. "Browser Add-On Locks Out Targeted Advertising," IDG NEWS, Mar. 17, 2009, http://www.pcworld.com/businesscenter/article/161380/browser_addon_locks_out_targeted_advertising.html.
[66] "Opt Out of Behavioral Advertising," NAI, http://www.networkadvertising.org/managing/opt_out.asp.
[67] *Id.*
[68] "How Do Not Track Plus Compares," http://donottrackplus.com/learn/featuredetails.php.

tracking.[69] The connections between ad networks are labyrinthine: some networks are hydra-like; their presence calls several others to a page. Some actually serve ads, while others verify that the ad was sold or correctly placed. Others compile demographics and provide data for ad targeting. "And then there are scores of middlemen that gather data and sell ads all over the web, knitting together the various other players."[70]

The methods used for tracking are more diverse than the ad companies.[71] The term "tracking" is not well defined, even among privacy advocates, technologists, and advertisers. At its core, tracking involves the conveyance of personal information on the Internet. There are many different ways of tracking consumers, including:

- various types of cookies (standard HTTP, Flash, DOM, and HTML5)
- web beacons (usually one-pixel transparent images)
- web bugs (usually involving the setting of third-party cookies through Javascript as first-party cookies, then reading and interacting with cookies based on the tracking that has already taken place)
- ETags, also known as cache cookies
- Browser fingerprinting

Only 41% of consumers are aware of *any* of the different types of cookies listed above.[72]

Some tracking methods are controversial for allegedly circumventing user privacy controls. A few notable examples are the initial use (and some say abuse[73]) of Flash cookies for tracking purposes, the undeletable KISSMetrics cookie,[74] and Google's circumvention of Safari's ban of third-party cookies through the creation of invisible online forms.[75] Domain name server (DNS) aliasing is another contentious tracking method that exploits the third party/first party distinction upon which many tracking and privacy rules are built. For example, a consumer visiting CNN.com who has elected to block third-party cookies will receive her first-party CNN cookies and presumably block others. Let's say that the third-party advertising network Doubleclick, in conjunction with CNN, makes a machine called

---

[69] These software options are Do Not Track Plus, TACO, and PrivacySuite.

[70] Madrigal, Alexis. "Drudge Report Looks Old School, but Its Ad Targeting Is State-of-the-Art," THE ATLANTIC, Mar. 5, 2012, http://www.theatlantic.com/technology/archive/2012/03/drudge-report-looks-old-school-but-its-ad-targeting-is-state-of-the-art/253902/. The initial products had the hope that the advertising industry would self-regulate in such a way that opting-out would give consumers meaningful privacy, rather than merely not spooking them with targeted ads. But they didn't evolve their opt-outs, so industry had to drive more effective software solutions that gave consumers what they expected.

[71] For a thorough overview of tracking technologies, we recommend Ayenson et al., "Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning," July 29, 2011, *available at* SSRN: http://ssrn.com/abstract=1898390 or http://dx.doi.org/10.2139/ssrn.1898390.

[72] Insight Express, http://blog.insightexpress.com/2011/03/research-consumer-views-online-privacy-personalized-ads/.

[73] Singel, Ryan. "Researchers Expose Cunning Online Tracking Service That Can't Be Dodged," WIRED, July 29, 2011, http://www.wired.com/epicenter/2011/07/undeletable-cookie/.

[74] *Id.*

[75] Angwin, Julia and Valentino-Devries, Jennifer. "Google's iPhone Tracking," WALL STREET JOURNAL, Feb. 17, 2012, http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

Tracker.CNN.com that actually points to a machine on Doubleclick's network for tracking purposes. Because the domain still appears to be the first party (CNN.com), the block on third-party trackers will not be effective.

Noted privacy research Ashkan Soltani has compared the ongoing battle against new tracking methods and privacy circumventions to a game of whack-a-mole, saying that it is "a continued arms-race that consumers are engaged in when trying to protect their privacy online since advertisers are incentivized to come up with more pervasive tracking mechanisms unless there's policy restrictions to prevent it."[76]

We believe that consumers are especially concerned with the combination of online data about their browsing habits with offline data sold by data brokers. One example of this data combination occurs in political campaigns. Several companies, including CampaignGrid,[77] combine the information in consumers' voter and public record files with their Internet activity, including the articles they're reading and sharing, to get a deeply personal profile of an individual. They attempt to ascertain a voter's stance on key issues, such as abortion rights and gun control, religion, education, and more. The online tracking company RapLeaf Inc. faced criticism in 2010 when it sold information garnered about individuals' web habits to the Maine GOP.[78] The data was incredibly detailed:

> An online tracking company called RapLeaf Inc. had correctly identified [Linda Twombly] as a conservative who is interested in Republican politics, has an interest in the Bible and contributes to political and environmental causes. Mrs. Twombly's profile is part of RapLeaf's rich trove of data, garnered from a variety of sources and which both political parties have tapped.

This type of tracking poses threats to free speech and association. We are not the same when we know our activities are being watched. We should be free to be curious, to read things that interest us, meet new people, learn, travel, and grow without repercussions. The Internet is a tremendous resource for self-actualization, but not when it is used as an instrument of surveillance.

i. Consumer Sentiment Reflects A Lack of Understanding and a Dislike of Data Collection and Tracking

Few Americans believe that online tracking and targeted advertising are legal or happening today. When asked about behavioral advertising, only half of the participants in a 2010 study believed that it as a common practice.[79] "Sixty-one percent of Americans are

---

[76] *Id.*

[77] http://www.campaigngrid.com/.

[78] Steel, Emily. "A Web Pioneer Profiles Users By Name," WALL STREET JOURNAL, Oct. 24, 2010, http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html?KEYWORDS=rapleaf.

[79] McDonald, Allecia M., & Cranor, Lorrie F. "Americans' Attitudes About Internet Behavioral Advertising Practices," Proceedings of the 9th Workshop on Privacy in the Electronic Society WPES, Oct. 4, 2010, at 6. "Moreover, when Americans are informed of three common ways that marketers gather data about people in

confident that what they do online is private and not shared without their permission," and "57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations."[80]

Those consumers who are aware that tracking and targeting exist do not support it. Most adult Americans, 66%, do not want marketers to personalize advertisements to their interests. [81] Overall, consumers tend to prefer generic ads (64%) to those that are personalized (37%).[82] Ninety-four percent of consumers believe they should be able to opt out if tracking if they wish.[83]

ii. Contextual Versus Behavioral Ads and Their Effect on the Web's Financial Ecosystem

The current way that many ads are built and served makes it difficult to untangle non-targeted ads from targeted ones. Before a consumer sees an ad, a long chain of events takes place among ad servers, brokers, compliance agents, and others. This delivery chain is saturated with tracking steps. Because of these complications, privacy tools can become ad blockers by default.

We wish to clarify the distinction between content-based online advertising and targeted advertising. A consumer seeing personalized ads on Pandora based on the music he's listening to is contextual advertising: it is based on the real-time content the consumer sees, and it seems intuitive. Seeing an ad for a corkscrew while looking at a blog about wine is an example of contextual advertising.

In contrast, behavioral advertising is not based on the present content of the page a consumer is viewing, but rather the content of other sites and pages he visited before it. For example, a consumer who searched for exercise equipment on Amazon.com before coming to the same wine blog then sees workout-based banner ads on that blog (which has nothing at all to do with exercise). Behavioral advertising refers to the advertising networks that follow consumers across the web and target them with ads based on their previous behavior behavior, not their current site visit.

The significant differences between contextual and behavioral advertising involve different scopes. The behind-the-scenes advertiser audience for behavioral advertising is much wider than that of contextual advertising: a consumer's data leaves the realm of a single company and trades hands as it is sold and shared, usually without that consumer's

---

order to tailor ads, even higher percentages - between 73% and 86% - say they would not want such advertising." *Id.*

[80] "Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy," Sep. 25, 2008, www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

[81] Turow et al., "Americans Reject Tailored Advertising and Three Activities that Enable It," Sept. 29, 2009, available at SSRN: http://ssrn.com/abstract=1478214 or http://dx.doi.org/10.2139/ssrn.1478214.

[82] Insight Express, http://blog.insightexpress.com/2011/03/research-consumer-views-online-privacy-personalized-ads/.

[83] *Id.*

knowledge, which grows the potential for privacy abuses. Furthermore, behavioral advertising involves a wider temporal frame than does contextual advertising: across a user's browsing history compared to viewing a single page at a set point in time.

Those who oppose the use of tracker-blocking technology sometimes argue that preventing behavioral advertising will destroy the free Internet. We counter that the majority of publishers rely mostly on contextual ads:

> Pam Horan, president of the Online Publishers Association, estimated that the amount of revenues her group's members take in from behavioral targeting is in "the low double digits." Several major publishers I spoke with insisted that in their personal experience, it's often even less than that. "Although behavioral ads are something that publishers will offer more over time, advertisers on premium sites find more value in contextual advertising," Horan said.[84]

We see no problem with advertisers placing ads based on the content of a site or a consumer's publicly stated interests; in fact, we strive to leave contextual advertising undisturbed by our privacy software. Contextual ads strike an appropriate balance between advertisers' desire to profit and consumers' desire to be left alone online.

c. Our Recommendations for Do Not Track

An effective Do Not Track option has several features:

- Easily accessible in all major browsers' preferences (e.g., no more than two menus deep into browser preferences and clearly worded with the minimum number of selections required)
- Free
- Persistent (once a user enables it, it becomes the norm for all browser sessions)
- Limits and/or stops both data collection and behavioral advertising

a. A Do Not Track Option Should Cover Data Collection

We commend the WC3 standards committee for pioneering a universal standard for Do Not Track. The header itself shows promise. However, we do not believe that the Digital Advertising Alliance's (DAA) present implementation of the header is sufficient to protect consumer privacy in the ways stated by the Administration, most notably the Individual Control principle.[85] A Do Not Track option that will be satisfying to consumers will limit both data collection and behavioral advertising.

---

[84] Kaplan, David. "Who Would Suffer The Most (And Least) Under Do Not Track," PaidContent, Dec. 3, 2010, http://paidcontent.org/article/419-who-would-suffer-the-most-and-least-under-do-not-track/.

[85] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," Feb. 23, 2012, at 11. Interestingly, the DAA itself believes that Do Not Track is a poor term to describe the current self-regulation effort:

The DAA's present implementation of Do Not Track allows consumers to choose to stop seeing targeted advertisements. Personalized ads, however, are the tip of the online tracking iceberg: they are merely the tangible expression of the underlying, and highly prevalent, data collection. FTC Commissioner Julie Brill has repeatedly stated that the DAA agreement is insufficient to address consumer expectations, stating that "one of the most critical points is that Do Not Track is not just Do Not Target ... but also, when the consumer so chooses, Do Not Collect."[86]

Our own data support Commissioner Brill's statement that Do Not Track, as implemented by the DAA, is inconsistent with consumer expectations. We surveyed 500 adult web users, asking "Most browsers offer a 'do not track' option. If you chose this option, what would you expect to happen?" We offered four answer choices.

More than 86 percent of those surveyed believed, incorrectly, that Do Not Track stopped websites from tracking them, cleaned their browser from all tracking technologies when the browser was shut down, or prevented advertisers from selling information obtained online about consumers. Fewer than 14 percent of respondents chose the correct response: "Advertisers and websites could still collect and sell information about me, but would not be able to send me personalized ads."[87]

To reflect consumers' wants and concerns, a workable and sufficient Do Not Track option must limit data collection. We say "limit," not "stop," because we realize that some data collection is necessary for Web's operation. The amount and type of data collected is a gray area to be defined by technology companies like Abine, regulators, and the advertising industry. In any case, these mechanisms "require further development to ensure they are easy to use, strike a balance with innovative uses of personal data, take public safety interests into account, and present consumers with a clear picture of the potential costs and benefits of limiting personal data collection."[88] The status quo—allowing data collection to continue unimpeded—is insufficient.

We believe that both first-party websites and third-parties, such as ad networks, must take responsibility for implementing Do Not Track. The first-party site controls which ad networks and tracking technologies to which to grant access, as well as their own data collection techniques and transparency practices. The third-parties are better equipped to

---

> "'Do Not Track' is a misnomer. It's not an accurate depiction of what's going on,'' said Stuart P. Ingis, head of the Digital Advertising Alliance, a trade group representing the advertising industry. "This is stopping some data collection, but it's not stopping all data collection.''

Vega, Tanzina. "Do Not Track Won't Halt Data Flow," NEW YORK TIMES, Feb. 27, 2012, http://articles.boston.com/2012-02-27/business/31100691_1_privacy-bill-data-collection-interactive-advertising-bureau.

[86] Julie Brill, Commissioner, Remarks at the Big Data, Big Issues Symposium, Fordham University School of Law, Mar. 2, 2012, *available at* http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

[87] Mello, John P. "Most Consumers Clueless About 'Do Not Track' Technology," PCWorld, Feb. 25, 2012, http://www.pcworld.com/article/250689/most_consumers_clueless_about_do_not_track_technology.html.

[88] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," Feb. 23, 2012, at 13.

regulate the flow of data among others when it leaves the first-party website. If a consumer decides that he does not want to be tracked, any party that touches his data must act in accordance with his wishes.

b. Advertisers Should Make a Clear Distinction between Contextual and Behavioral Advertisements

As we described in Section (5)(b)(2) above, most online ads—even those not intended to behaviorally target users—are wrapped up in targeting technology. We call on the advertising industry to make a clear distinction between contextual ads, which will be served to users who enable Do Not Track, and behaviorally-targeted ads, which will be served to all other users. Clarifying this dichotomy will benefit all parties involved. Privacy tools will not block contextual ads that do not pose privacy concerns; advertisers will ensure that an ad displays, rather than being blocked completely; and consumers will see an ad reflecting his or her privacy choices.

6. Conclusion

We appreciate the opportunity to comment on privacy developments. These matters touch people's lives in significant and personal ways, and we want to ensure that any major changes keep consumers' interests at heart. We've heard various stakeholders say that these solutions won't be easy, or even that they're impossible. We disagree. Things become quite simple when you consider the greater good of the American people.