



September 26, 2016

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12th St., SW, Room TW-A325  
Washington, D.C. 20554

**Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC  
Docket No. 16-106**

Dear Ms. Dortch:

On behalf of Atomite, Inc., a Data Privacy Management (DPM) enterprise specifically designed to address government mandates that businesses interested in redeploying their customers' personal information for marketing purposes should only do so after providing those customers with bona fide transparency, choice, control and compensation, I write regarding the above-referenced Notice of Proposed Rulemaking (Broadband Privacy NPRM) released by the Commission on April 1, 2016, and to supplement my previous comments (i) filed with the Commission on May 25, 2016 (<https://ecfsapi.fcc.gov/file/60002056622.pdf>), a copy of which is attached hereto as Exhibit A (Atomite's Previous Public Comments) and (ii) discussed with the Commission's staff in an *ex parte* meeting held on June 27, 2016 (<https://ecfsapi.fcc.gov/file/1062913916013/Atomite%201%20FCC%20NPRM%20Ex%20Parte%20Meeti%20Summary%20062816.pdf>) and which was thereafter summarized in an *ex parte* presentation filing, a copy of which is attached hereto as Exhibit B (Atomite's Previous Ex Parte Presentation; and, together with Atomite's Previous Public Comments, Atomite's Previous Broadband Privacy NPRM Comments).

In sum, Atomite's Previous Broadband Privacy NPRM Comments conveyed Atomite's view that (i) *a multi-stakeholder public-private approach* which incorporates significant and fluid input from industry and other third parties with subject matter expertise will result in the development of a set of *industry best practices* designed to evolve with the needs of ISP subscribers and innovations in technologies and business models of broadband providers, the kind of evolution which historically has not resulted from hard and fast rules promulgated by government regulators, no matter how well-intentioned, (ii) with such industry best practices in place, those broadband providers which can provide pre-agreed kinds of evidence of their adherence to such practices should be the beneficiaries of a *regulatory safe harbor*, one that offers these providers an incentive to *both* protect their subscribers' privacy rights *and* continue to develop innovative products and services which will ultimately result in a true 'win-win-win' for ISPs and their subscribers and marketing partners, and (iii) not only should the Commission require broadband providers "to create a *consumer-facing privacy dashboard* (emphasis added) that would allow customers to: (1) see the types and categories of customer PI collected by BIAS providers; (2) see the categories of entities with whom that customer PI is shared; (3) grant or deny approval for the use or disclosure of customer PI; (4) see what privacy selection the customer has made (i.e., whether the customer has chosen to opt in, opt out, or take no action at all with regards to the use or disclosure of her PI), and the consequences of this selection, including a description of what types and categories of customer PI may or may not be used or disclosed by a provider depending on the customer's privacy selection; (5) request correction of inaccurate customer PI; and (6) request deletion of any categories of customer PI that the customer no

longer wants the BIAS provider to maintain (e.g., online activity data), so long as such data is not necessary to provide the underlying broadband service or needed for purposes of law enforcement”<sup>1</sup>, but that the Commission should also enable broadband providers to utilize trusted third parties (TPPs) such as Atomite to provide such consumer-facing privacy dashboards.

Subsequent to making its Previous Broadband Privacy NPRM Comments, Atomite has conducted an extensive review of the Commission’s past practices for precedent in the realm of reliance upon industry best practices, utilization of TPPs and the creation of regulatory safe harbors and has found extensive evidence for each. In fact, strong support for each of these positions can be found in the FCC’s Second Report and Order and Memorandum and Opinion and Order In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services ([https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-06-56A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf)) (the FCC’s CALEA Opinion and Order), several particularly salient excerpts of which are set forth below for each of reference:

### “3. Compliance Solutions Based on a Trusted Third Party

26. The record indicates that TPPs are available to provide a variety of services for CALEA compliance to carriers, including processing requests for intercepts, conducting electronic surveillance, and delivering relevant information to LEAs. Given the effectively unanimous view of commenters that the use of TPPs should be permitted but not required, we conclude that TPPs may provide a reasonable means for carriers to comply with CALEA, especially broadband access and VoIP providers and smaller carriers. We emphasize, however, that if a carrier chooses to use a TPP, that carrier remains responsible for ensuring the timely delivery of CII and call content information to a LEA and for protecting subscriber privacy, as required by CALEA. Thus, a carrier must be satisfied that the TPP’s processes allow the carrier to meet its obligations without compromising the integrity of the intercept. Carriers will not be relieved of their CALEA obligations by asserting that a TPP’s processes prevented them from complying with CALEA. We note DOJ’s concern about carriers attempting to use TPPs to shift costs to LEAs, but we make no decision here that would allow carriers who choose to use a TPP to shift the financial responsibility for CALEA compliance to the Attorney General under Section 109 (see discussion on cost recovery, *infra*). We will evaluate whether the availability of a TPP makes call identifying information “reasonably” available to a carrier within the context of section 103 in acting on a section 109 petition that a carrier may file (see discussion on section 109 petitions, *infra*). As noted by several commenters, telecommunications carriers and manufacturers have legally-mandated privacy obligations, and we take no action herein to modify those obligations based on potential broadband access and VoIP provider use of TPPs. Finally, in accord with the consensus of comments, we will defer to standards organizations and industry associations and allow them to determine the degree to which the ability of a TPP external system to extract and isolate CII makes that information reasonably available for purposes of defining CALEA standards and safe harbors (emphasis added).”<sup>2</sup>

### “2. Compliance Solutions Based on CALEA “Safe Harbor” Standards

22. Consistent with a broad range of comments, we find that it would be premature for the Commission to pre-empt the ongoing industry process to develop additional standards for packet-mode technologies. We believe that industry organizations, whose meetings are generally open to all interested parties – including LEAs – can best develop those standards, just as they previously developed circuit switched

---

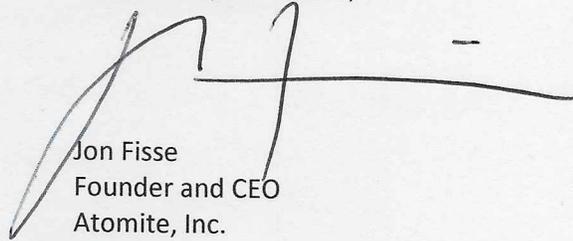
<sup>1</sup> Broadband Privacy NPRM at para. 95.

<sup>2</sup> CALEA Opinion and Order at para. 26.

standards. Further, given the diversity of technologies supporting communications services and the breadth of organizations involved both domestically and internationally in developing packet-mode standards, we find it both infeasible and inappropriate to specify the organizations qualified to develop standards that may be used as “safe harbors.” (emphasis added) Finally, we find no reason to become involved at this time in the technically complex issue of determining the appropriate format to be used for the transmission of broadband CII data to LEAs. Rather, for all of these technical issues, we find that the industry standards process remains the preferred forum. We note again, however, to the extent that any party perceives a problem with an industry developed packet-mode standard, it may file with the Commission a deficiency petition under section 107(b) of CALEA.”<sup>3</sup>

For the reasons set forth herein, Atomite respectfully submits for the Commission’s consideration its view that in enabling broadband providers to rely on industry best practices and utilize TPP’s such as Atomite to implement certain elements thereof (e.g., consumer-facing privacy dashboards), and provide a regulatory safe harbor for those that do so properly, the Commission will properly incent these providers to *both* protect their subscribers’ privacy rights *and* continue to develop innovative products and services which will ultimately result in a true 'win-win-win' for these providers and their subscribers and marketing partners.

Respectfully submitted,



Jon Fisse  
Founder and CEO  
Atomite, Inc.

[Jfisse@atomite.net](mailto:Jfisse@atomite.net)  
(917) 882-8944

---

<sup>3</sup> CALEA Opinion and Order at para. 22.

**Exhibit A**  
Atomite's Previous Public Comments



May 25, 2016

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12th St., SW, Room TW-A325  
Washington, D.C. 20554

**Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC  
Docket No. 16-106**

Dear Ms. Dortch:

On behalf of Atomite, Inc., a Data Privacy Management (DPM) start-up enterprise specifically designed to address government mandates that businesses interested in redeploying their customers' personal information for marketing purposes should only do so after providing those customers with bona fide transparency, choice and control, I write regarding the above-referenced Notice of Proposed Rulemaking (Broadband Privacy NPRM) released by the Commission on April 1, 2016.

General Comments to Broadband Privacy NPRM

The FCC's proposed framework for ensuring that ISP subscribers' personal information is redeployed for purposes other than the provision of broadband services only after the subscribers are provided with a clear understanding of the alternative uses, opt-in consent rights and protection against unauthorized access is comprehensive and well-intentioned, in particular given the reality that left to their own devices, most subscribers would be insufficiently aware of, informed about, equipped to decide on and compensated for the use of their property rights. That said, given the speed at which technology and corresponding business models evolve, history has shown that hard and fast rules promulgated by government regulators in this and similar contexts without significant and fluid input from industry and other third parties with subject matter expertise often leads to unintended collateral effects which can materially undermine the very objectives which underpin the government-mandated rules and regulations<sup>4</sup>.

---

<sup>4</sup> The FTC was sensitive to this issue when it concluded in its seminal 2012 Privacy Report (FTC Report, *Protecting Consumers in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.) that "[t]he Commission agrees that a flexible, technology-neutral approach...is appropriate to accommodate the rapid changes in the marketplace and will also allow companies to innovate." More recently, Dorian Benkoil in his February 2, 2015 article entitled *Privacy vs. Policy: What Does the End of the Cookie Mean?* (<http://mediashift.org/2015/02/privacy-vs-policy-what-does-the->

Given the above, it is Atomite's view that what is called for in this context is more than the establishment of a standalone set of *principles* (e.g., transparency, choice, control, privacy-by-design, security) but less than a 'set it and forget it' set of ironclad *requirements* (e.g., the use of persistent identifiers and deep packet inspection (DPI) for purposes other than network management are to be unconditionally prohibited in all circumstances); instead a hybrid approach should be taken pursuant to which a set of clear *parameters* is established by the FCC to be flushed out via a public-private initiative which is more generally referred to by the FCC in its NPRM as a "multi-stakeholder process."<sup>5</sup> This public-private multi-stakeholder initiative would be led by the FCC and enable governmental authorities, ISP providers, ISP subscribers, consumer privacy advocates, marketers, relevant trade associations, academics and innovative start-up enterprises to engage in a continuing dialogue, resulting in *industry best practices* which will evolve with the needs of ISP subscribers and innovations in the technologies and business models of ISPs<sup>6</sup>. With these industry best practices in place, those broadband providers which can provide pre-agreed kinds of evidence of their adherence to such practices should be the beneficiaries of a regulatory safe harbor<sup>7</sup>, one that offers these providers an incentive to continue to develop innovative products and services which will ultimately result in a true 'win-win-win' for ISPs and their subscribers and marketing partners<sup>8</sup>.

---

end-of-the-cookie-mean/) reported that "[b]ecause the technology moves more quickly than regulators' or lawmakers' ability to draft rules to match it, [FTC Bureau of Consumer Affairs Director Jessica L.] Rich[, at a January 21, 2015 Industry Preview conference run by AdExchanger,] called for 'tech neutral' regulations that focus on higher principles, such as [Privacy by Design, Increased Transparency and 'Usable Choice']."

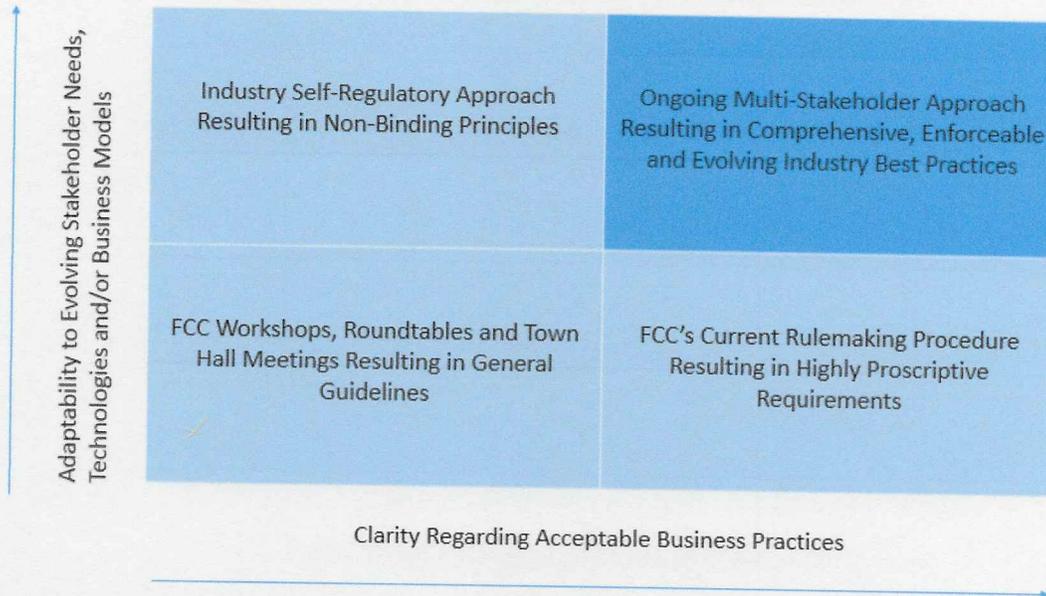
<sup>5</sup> Broadband Privacy NPRM at para. 293.

<sup>6</sup> See *Responses to Specific Questions Raised in Broadband Privacy NPRM- FCC Question No. 3 and Atomite Response No. 3* on pages 4-5 of this public comment submission for a more detailed discussion of the way in which this public-private initiative can be led and managed by the FCC, including a reference to the FTC's robust approach in this context.

<sup>7</sup> For the FCC's references to the prospect of implementing a regulatory safe harbor, see Broadband Privacy NPRM at paras. 92, 178, and 182, Appendix B at para. 58 and footnote 166.

<sup>8</sup> Should there be any doubt that ISP providers would have sufficient incentive to play a productive roll in this public-private initiative, it is important to note that FTC Bureau of Consumer Affairs Director Rich commented in her 2015 AdExchanger Industry Preview conference presentation that "we see that providing transparency and choices about privacy is increasingly a selling point for businesses. We see more and more ads touting the privacy features for products, and more and more tools being marketed that are designed to help consumers protect their privacy", leading her to conclude that "[o]ne of the greatest assets a business has is the trust of its customers. As consumers increasingly demand privacy, companies can leverage this demand as part of a broader business strategy. There are real benefits that companies can realize in competing on privacy and gaining consumers' trust."

## Alternative Regulatory Frameworks



Leveraging existing proposals for industry best practices from governmental bodies and organizations such as the FTC, GSMA, MEF, IAB, NAI, DAA, NTIA and NIST, and with the FCC having the ‘final say’ on key issues which can be communicated in the form of no-action letters similar to those issued by the U.S. Securities and Exchange Commission in the investment markets context, a “‘privacy protection seal’ that BIAS providers could display on their websites to indicate compliance with [industry best practice] guidelines”<sup>9</sup> or their equivalent indicating whether or not particular proposed ISP practices would enjoy the benefits of a regulatory safe harbor, the public-private initiative would initially determine which of the FCC’s *proposed rules* in the current Broadband Privacy NPRM, which would serve as *guidelines or parameters* in this context, would be modified, supplemented or deleted prior to initial implementation. In making such a determination, those participating in the public-private initiative would be required to make informed determinations as to which guidelines would “best balance...consumer benefits with minimizing regulatory burdens on broadband providers”.<sup>10</sup>

Prior to responding to a number of specific questions raised by the FCC’s NPRM, Atomite takes note of the public requests for an extension of time to file comments and reply comments in response to the Broadband Privacy NPRM received by the FCC to date on this matter<sup>11</sup>. Similar to the other extension

<sup>9</sup> Broadband Privacy NPRM at para. 257.

<sup>10</sup> Broadband Privacy NPRM at para.135.

<sup>11</sup> See, for example, the public requests for an extension of time to file comments and reply comments in response to the Broadband Privacy NPRM submitted by the Association of National Advertisers (ANA), the State Privacy & Security Coalition, Inc. (State Privacy & Security Coalition), the American Advertising Federation (AAF) and the American Cable Associations (ACA) available at [http://apps.fcc.gov/ecfs/comment\\_search\\_solr/doSearch?proceeding=16-106&applicant=&lawfirm=&author=&disseminated.minDate=&disseminated.maxDate=&received.minDate=&received.maxDate=&dateCommentPeriod.minDate=&dateCommentPeriod.maxDate=&dateReplyComment.minDate=&](http://apps.fcc.gov/ecfs/comment_search_solr/doSearch?proceeding=16-106&applicant=&lawfirm=&author=&disseminated.minDate=&disseminated.maxDate=&received.minDate=&received.maxDate=&dateCommentPeriod.minDate=&dateCommentPeriod.maxDate=&dateReplyComment.minDate=&)

requests, the rationale offered by the ANA for its request for extension is that “[t]his NPRM, which consists of 147 pages in the Federal Register, contains numerous proposed requirements with potentially complex impacts regarding the privacy of collected and user data. Commissioner Rosenworcel mentioned in her oral remarks during the Commission’s consideration of this matter that there are more than 500 questions raised in the NPRM. Yet the timetable for the filing of initial comments is limited to a mere 57 days from the release of the Notice”<sup>12</sup> and “[b]ecause the potential implications of the NPRM for advertising and marketing interests are significant and far-reaching, they require sufficient and thoughtful analysis.”<sup>13</sup> While the FCC ultimately concluded in response to these requests that “a timely resolution of this proceeding will be beneficial for both consumers and industry alike, providing clarity and certainty going forward, and as such, an extension of the comment deadline is not in the public interest”<sup>14</sup>, for the reasons noted above, Atomite believes it would be in the public interest for the FCC to conclude that rather than promulgate highly prescriptive requirements without availing itself of the benefits of the kind of public-private initiative described in this comment letter, it will pursue a multi-stakeholder public-private initiative calling for significant and fluid input from industry and other third parties with subject matter expertise, ultimately resulting in the development of a robust set of industry best practices and an enforcement regime designed to evolve with the needs of ISP subscribers and innovations in technologies and business models of broadband providers.

#### Responses to Specific Questions Raised in Broadband Privacy NPRM

##### **FCC Question No. 1**

“[W]e seek comment on whether we should take further steps to ensure (1) that customers have access to sufficient information regarding their BIAS provider’s privacy policies, and (2) that such information is presented in a form that is both palatable and easily comprehensible for customers. In particular, we seek comment on whether the Commission should require BIAS providers to create a *consumer-facing privacy dashboard* (emphasis added) that would allow customers to: (1) see the types and categories of customer PI collected by BIAS providers; (2) see the categories of entities with whom that customer PI is shared; (3) grant or deny approval for the use or disclosure of customer PI; (4) see what privacy selection the customer has made (i.e., whether the customer has chosen to opt in, opt out, or take no action at all with regards to the use or disclosure of her PI), and the consequences of this selection, including a description of what types and categories of customer PI may or may not be used or disclosed by a provider depending on the customer’s privacy selection; (5) request correction of inaccurate customer PI; and (6) request deletion of any categories of customer PI that the customer no longer wants the BIAS provider to maintain (e.g., online activity data), so long as such data is not necessary to provide the underlying broadband service or needed for purposes of law enforcement. We seek comment on the costs and benefits of requiring the creation of such a dashboard, and any alternatives the Commission should consider to minimize the burdens of such a program on small providers.”<sup>15</sup>

---

dateReplyComment.maxDate=&address.city=&address.state.stateCd=&address.zip=&daNumber=&fileNumber=&b  
ureauidentificationNumber=&reportNumber=&submissionType=&\_\_checkbox\_exParte=true.

<sup>12</sup> ANA Letter available at <http://apps.fcc.gov/ecfs/document/view?id=60001569332>.

<sup>13</sup> *Id.*

<sup>14</sup> FCC Order re Denial of Extension of Time to File BB Privacy Comments and Replies available at [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2016/db0429/DA-16-473A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0429/DA-16-473A1.pdf).

<sup>15</sup> Broadband Privacy NPRM at para. 95.

### **Atomite Response No. 1**

Atomite's TransPrivacy™ software service, an end-to-end data privacy management (DPM) solution for heavily-regulated B2C enterprises, in general, and mobile carriers and ISPs in particular, is a consumer-facing privacy dashboard which contains all of the features and functionality referenced by the FCC.

Atomite's offerings reward consumers who opt-in and permission Atomite wireless carrier and ISP licensees to use their "Customer Proprietary Information"<sup>16</sup> (CPI) for marketing purposes.

These customers earn affinity points (Privacy Points™) redeemable for valuable goods and services (e.g., free GBs of data; early mobile device upgrades; a discount on monthly service fees; iTunes; Netflix trial periods; and fully-paid or discounted dining, shopping, entertainment, travel, merchandise and gift card offers).

Through the use of an intuitive user interface, the customers have full control over what CPI is shared, with whom, for what purposes and for how long.

Atomite conducts digital audits of its licensees' deployment of its TransPrivacy™ offerings to ensure that its wireless carrier and ISP licensees are respecting consumer-reflected choices regarding the use of their CPI for marketing purposes, thereby enhancing the licensees' trust and goodwill with both customers and relevant governmental authorities.

### **FCC Question No. 2**

"[S]ome have argued that consumers stand to benefit from the sale of personal information collected by entities such as ISPs and other telecommunications companies. In light of these potential consumer benefits, should we accept that, upon being fully informed about the privacy rights they are exchanging for a discounted broadband price, consumers can and should be allowed to enter into such bargains?"<sup>17</sup>

### **Atomite Response No. 2**

The ultimate objective of the Broadband Privacy NPRM is to ensure a 'level playing field' as between an ISP and its subscribers as it relates to the former's collection, use and sharing of the latter's CPI. Provided that the public-private multi-stakeholder initiative referenced above develops, implements and ensures compliance with industry best practices, the result will be the kind of level playing field which will enable an ISP subscriber to make an informed decision as to whether or not to 'make a market' in his or her CPI.

More specifically, Atomite's TransPrivacy™ offering enables an ISP's subscribers to earn Privacy Points™ by permissioning the ISP to redeploy their CPI for marketing purposes. In addition, the subscribers are not forced to make a Hobson's choice by having to make a binary 'all yes' or 'all no' decision with the "all yes" decision in many cases effectively leading to the disclosure of certain subscriber CPI he or she would not otherwise share if given the opportunity to share some, but not all of his or her CPI and the "all no" decision in many cases effectively leading to no access to broadband service. Rather the subscribers are empowered to modulate the type of CPI shared, for what marketing purposes, with which third party recipients and for how long. Along the same lines, ISPs which deploy Atomite's TransPrivacy™ data privacy

---

<sup>16</sup> See *supra* Appendix A (Proposed Rules), § 64.2003 Definitions, (h) *Customer Proprietary Information*.

<sup>17</sup> See *supra* para. 263.

management solution are offering their subscribers a carrot (i.e., consideration in exchange for property rights) and not a stick (e.g., no ISP service unless subscribers relinquish their property rights).

### **FCC Question No. 3**

“We seek comment on whether there are specific ways we should incorporate multi stakeholder processes into our proposed approach to protecting the privacy of customer PI...Would such processes be useful in developing guidelines and best practices relating to these proposed rules... Would a similar process be useful to address the privacy practices of broadband providers more generally, or in other specific areas? If so, how should the process be managed and governed? Should such processes serve as a supplement or an alternative to further rulemaking?”<sup>18</sup>

### **Atomite Response No. 3**

To address these questions, the FCC need look no further than the experience of the FTC and its reliance upon a broad set of methods over many years in order to adequately address consumer privacy concerns. These methods include, but are not limited to, (i) hosting privacy-related workshops, roundtables and town hall meetings, (ii) issuance of public reports based on such workshops and meetings, (iii) consultations with other government agencies such as the FCC and the Department of Commerce, (iv) testifying before Congress on privacy and data security issues and proposing legislation with respect to the same, (v) conducting outreach efforts through its consumer online safety portal, OnGuardOnline.gov, which provides information in a variety of formats to help consumers secure their computers and protect their personal information, (vi) development and public release of principles designed to serve as the basis for industry self-regulatory efforts to address privacy concerns, and (viii) issuance of warning letters and commencement of enforcement actions against companies which engage in deceptive trade practices in violation of consumer privacy rights.

For all of the reasons set forth herein, Atomite is of the view that a multi-stakeholder public-private approach which incorporates significant and fluid input from industry and other third parties with subject matter expertise will result in the development of a set of industry best practices designed to evolve with the needs of ISP subscribers and innovations in technologies and business models of broadband providers, the kind of evolution which historically has not resulted from hard and fast rules promulgated by government regulators, no matter how well-intentioned.

Respectfully submitted,

/s/ Jon Fisse  
Founder and CEO  
Atomite, Inc.  
[Jfisse@atomite.net](mailto:Jfisse@atomite.net)  
(917) 882-8944

---

<sup>18</sup> See *supra* para. 293.

**Exhibit B**  
Atomite's Ex Parte Comments



June 28, 2016

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12th St., SW, Room TW-A325  
Washington, D.C. 20554

**Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC  
Docket No. 16-106 ("Broadband NPRM")**

Dear Ms. Dortch:

On June 27, 2016, and in my capacity as Founder and CEO of Atomite, Inc. ("Atomite"), I met with Sherwin Siy, David Brody, Melissa Kirkel, Alex Espinoza, Brian Hurley, Gail Krutor and Brad Bourne from the Wireline Competition Bureau to discuss the Commission's Broadband NPRM. During the meeting we discussed comments filed in the Broadband NPRM proceeding by Atomite on May 25, 2016, in general, and, as reflected in the attached summary presentation, the various ways in which Atomite's TransPrivacy™ data privacy management (DPM) software solution offer the features and functionalities of the "consumer-facing privacy dashboard"<sup>19</sup> and "privacy protection seal"<sup>20</sup> the Commission inquiries about in the Broadband NPRM, in particular.

Sincerely,

/s/ Jon Fisse

Founder and CEO  
Atomite, Inc.  
(917) 882-8944  
jfisse@atomite.net

---

<sup>19</sup> Broadband Privacy NPRM at para. 95.

<sup>20</sup> Broadband Privacy NPRM at para. 257.

# Select Atomite Demo Site Screenshots

## Homepage

Customer receives a link to a personalized affirmative 'opt-in' start page via several mediums:

- i) A push notice from her wireless carrier asking whether she'd be interested in learning how to put her data to work in exchange for rewards;
- ii) She'd see a similar message when paying her wireless bill or when she's navigated to the 'do not track' option through her mobile device settings and is about to opt-out; and
- iii) She'd see a similar message as part of a general marketing campaign run by her carrier.

index.html

file:///Users/aleksey.vaynshteyn/Desktop/LX/Savedesign/Atomite/fisse\_project/index.html

Welcome, Jon!

# It's your data! Put it to work.

We reward you for managing how your data is put to work for you

[Get Started >](#)

**atomite**  
Digital loyalty has its benefits™

### Learn

Learn about how to protect, update, and share your data.

[Learn more](#)

### Decide

Decide how much data you want to share, with whom, and for what purposes.

[Learn more](#)

### Earn

Earn Privacy Points™ you can redeem for valuable products and services.

[See rewards](#)

Clear Data and Start New Session

Copyright 2015 Atomite. All rights reserved.

## Your data

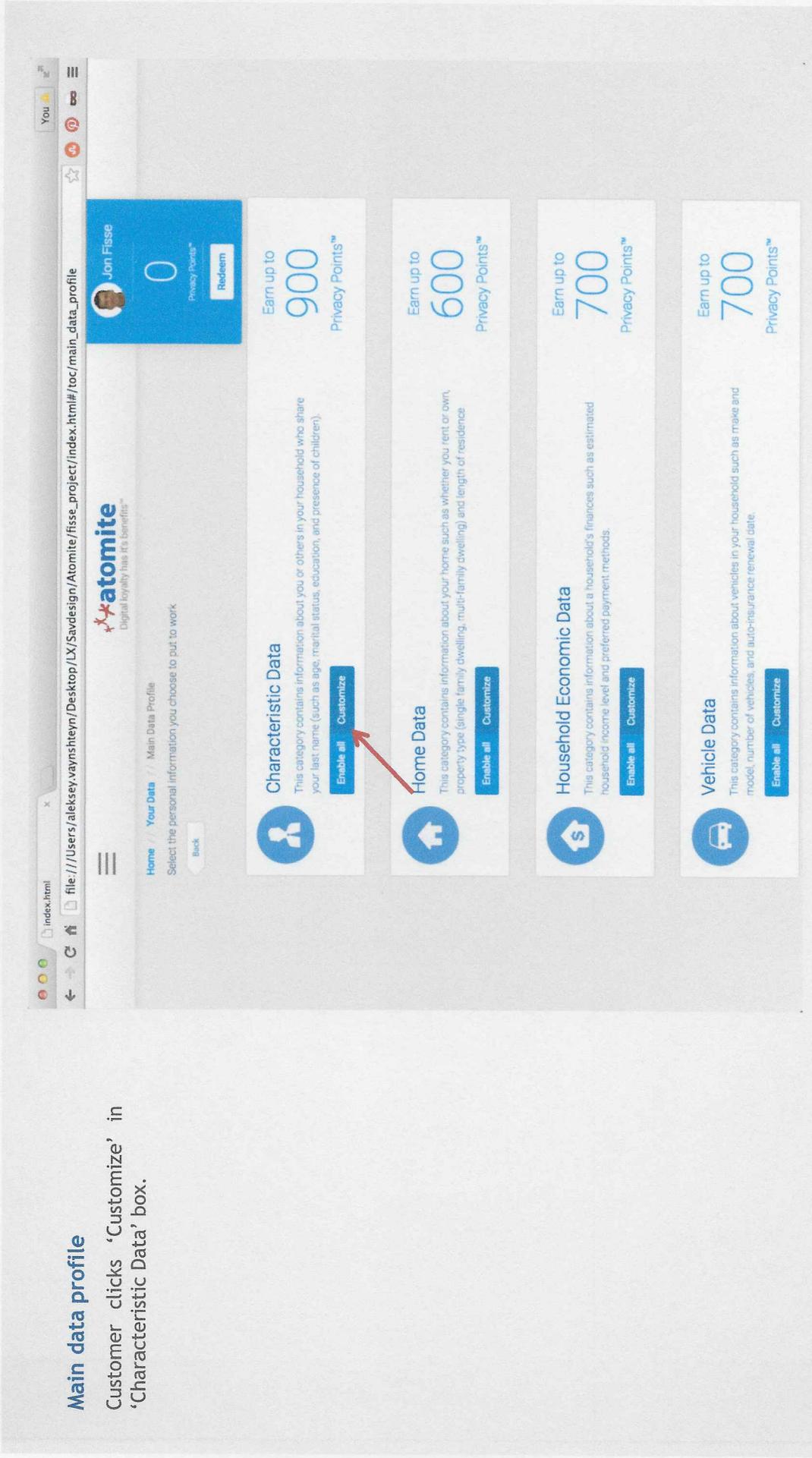
This is the control center. Customer can click 'Enable all' to share all data or click 'Customize' to pick and choose what to share. Customer clicks "Customize."

The screenshot shows a web browser window displaying the Atomite website. The browser's address bar shows the URL: `file:///Users/aleksey.vaynshteyn/Desktop/LX/Savedesign/Atomite/fisse_project/index.html#/toc`. The website header includes the Atomite logo and the tagline "Digital Loyalty has it's benefits™". Below the header, there is a navigation bar with a "Home" link and a "Your Data" link. The main content area is divided into four sections, each with a "Customize" button. A red arrow points to the "Customize" button in the "Your Data" section.

Section	Earn up to	Privacy Points™
Your Data	4,600	4,600
How Your Data Can Be Put to Work	900	900
Who Can Put Your Data to Work	5,300	5,300
More Ways to Earn Privacy Points™	5,200	5,200

## Main data profile

Customer clicks 'Customize' in 'Characteristic Data' box.



## Characteristic data

Customer earns Privacy Points™ for each item of information she enables an Atomite licensee to put to work for marketing purposes. Additional Privacy Points™ are given for updating the information.

The screenshot shows a web browser window with the URL `file:///Users/aleksey.vaynshteyn/Desktop/LX/SavedSign/Atomite/fisse_project/index.html#/toc/main_data_profile/characteristic_data`. The page header includes the Atomite logo and the text "Digital loyalty has it's benefits". A blue banner at the top right displays "300 pts". The main content area is titled "Characteristic Data" and features a user profile icon and a yellow callout box that says "Update your data to earn even more Privacy Points™". Below this, a table lists various data points with their current values and the number of points earned for each.

Characteristic	Current Value	Points Earned
Date of Birth	01/01/1955	+100 pts.
Gender	Male	+100 pts.
Ethnicity	White	+100 pts.
Education	Completed High School	0 pts.
Current Occupation	Other	0 pts.
Marital Status	Single	0 pts.
Number of Adults in Household	1	0 pts.
Presence of Children	No	0 pts.
Number of Children	0	0 pts.

## Redeem Privacy Points™

Now the customer can redeem Privacy Points™ for rewards.

The screenshot shows a web browser window displaying the Atomite website. The user's name is Jon Fisse, and their Privacy Points balance is 8,570. The website features a navigation menu with 'Home' and 'Redeem' options. A search bar is present, and the 'Show' filter is set to 'All Available'. The main content area is titled 'Redeem Your Privacy Points™' and lists several redemption options, each with a corresponding image and a 'Redeem' button.

Reward	Points Required	Redeem Button
amazon.com Gift Card	\$10 - 1000pts	Redeem
iTunes Gift Card \$15	\$10 - 1000pts	Redeem
STARBUCKS CARD \$10	\$10 - 1000pts	Redeem
\$20 off your next wireless bill	2,000 pts	Redeem
Free 1 month of HBO GO	1,500 pts	Redeem
Unlimited data for 1 month	1,500 pts	Redeem