

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK**

BRADY COHEN, individually and on behalf  
of all others similarly situated,

Plaintiff,

v.

NEW MOOSEJAW, LLC and NAVISTONE,  
INC.,

Defendants.

Civil Action No.:

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Brady Cohen (“Plaintiff”), individually and on behalf of himself and all others similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

**NATURE OF THE CASE**

1. This is a class action suit brought against Defendants New Moosejaw, LLC (“Moosejaw”) and NaviStone, Inc. (“NaviStone”) (collectively, “Defendants”) for wiretapping the computers of visitors to Defendant Moosejaw’s website, Moosejaw.com. NaviStone employs these wiretaps to observe visitors’ keystrokes, mouseclicks and other electronic communications in real time for the purpose of gathering visitors’ Personally Identifiable Information (“PII”) to de-anonymize those visitors – that is, to match previously unidentifiable website visitors to postal names and addresses. These wiretaps enable Defendants to immediately, automatically, and secretly observe the keystrokes, mouseclicks and other electronic communications of visitors regardless of whether the visitor ultimately makes a

purchase from Moosejaw. By doing so, Defendants have violated Title I of the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22, also known as the “Wiretap Act,” which prohibits the intentional interception of wire, oral, and electronic communications unless specifically authorized by a court order.

2. On several occasions within the past 6 months, Plaintiff Brady Cohen visited Moosejaw.com, but has never made any purchase from Moosejaw. During each of Plaintiff’s visits Moosejaw wiretapped his electronic communications with the website, disclosed the intercepted data to NaviStone in real time, and used the intercepted data to attempt to learn his identity, postal address, and other PII.

3. Plaintiff brings this action on behalf of himself and a class of all persons whose electronic communications were intercepted through the use of NaviStone’s wiretap on Moosejaw.com, pursuant to 18 U.S.C. § 2520, and seeks all civil remedies provided under the Wiretap Act including but not limited to statutory damages of \$10,000 per class member.

### **PARTIES**

4. Plaintiff Brady Cohen is a natural person and citizen of the State of New York who resides in New York, New York. Several times over the last six months, Mr. Cohen browsed Defendant Moosejaw’s website at Moosejaw.com while shopping for outerwear. Although Mr. Cohen never purchased anything from Defendants and never consented to any interception, disclosure or use of his electronic communications, Mr. Cohen’s keystrokes, mouseclicks and other electronic communications were intercepted in real time and were disclosed to NaviStone through Moosejaw’s use of NaviStone’s wiretap. Mr. Cohen was unaware at the time that his keystrokes, mouseclicks and other electronic communications were being intercepted and disclosed to a third party.

5. Defendant New Moosejaw, LLC is a Delaware limited liability company with its

principal place of business at 32200 North Avis Suite 100, Madison Heights, Michigan.

Moosejaw does business throughout New York and the entire United States. “Moosejaw is a leading online active outdoor retailer with a large web presence as well at 10 physical stores.”<sup>1</sup>

“Moosejaw carries more than 400 brands, including Patagonia, The North Face, Marmot, Arc’teryx and more. [Moosejaw] ha[s] an extensive assortment of apparel and gear for climbing, hiking, camping, snow sports, yoga, swimming and biking.”<sup>2</sup>

6. Defendant NaviStone, Inc. is a Delaware corporation with its principal place of business at 1308 Race Street, Cincinnati, Ohio 45202. NaviStone does business throughout New York and the entire United States. NaviStone is an online marketing company and data broker that deals in U.S. consumer data.

#### **JURISDICTION AND VENUE**

7. This action is brought pursuant to the federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*

8. The jurisdiction of this Court is predicated on 28 U.S.C. § 1331.

9. Both Defendants transact business in this District. Venue is proper in this District under 28 U.S.C. § 1391 because Plaintiff resides in this District, Defendants do substantial business in this District, and a substantial part of the events giving rise to Plaintiff’s claims took place within this District.

10. This Court has personal jurisdiction over Defendants because Defendants conduct substantial business within New York, such that Defendants have significant, continuous, and pervasive contacts with the State of New York. Furthermore, a substantial part of the events

---

<sup>1</sup> <https://news.walmart.com/2017/02/15/walmart-announces-the-acquisition-of-moosejaw-a-leading-online-outdoor-retailer>

<sup>2</sup> *Id.*

giving rise to Plaintiff's claims took place within New York.

### **FACTS COMMON TO ALL CLAIMS**

#### **Overview Of NaviStone's Wiretaps**

11. Defendant NaviStone is a marketing company and data broker that deals in U.S. consumer data. NaviStone's business model involves entering into voluntary partnerships with various e-commerce websites. Upon partnering with NaviStone, these e-commerce websites will agree to insert a small parcel of computer code into their websites, which is provided by NaviStone (and is written by NaviStone). This small parcel of computer code serves as a so-called "back door" in computer terminology – its function is to retrieve and execute a much larger portion of JavaScript code that is remotely hosted on NaviStone's servers. As NaviStone explains on <http://navistone.com>, "[a]dding a simple line of code to each page of your website enables a wealth of new marketing data."

12. This "back door" code permits NaviStone to execute its own computer code on the websites of its e-commerce partners. Stated otherwise, the "simple line of code" that NaviStone requests its partners add "to each page of [their] website[s]" serves to call and execute remote computer code that is: (i) provided by NaviStone, (ii) written by NaviStone, and (iii) hosted on a remote server by NaviStone.

13. As currently deployed, NaviStone's remote code functions as a wiretap. That is, when connecting to a website that runs this remote code from NaviStone, a visitor's IP address and other PII is sent to NaviStone in real-time. NaviStone's code will then continue to spy on the visitor as he or she browses the website, instantaneously reporting the visitor's every keystroke and mouse click to NaviStone. This real-time interception and transmission of visitors' electronic communications begins as soon as the visitor loads [Moosejaw.com](http://Moosejaw.com) into their web

browser. Every keystroke and mouseclick is instantaneously intercepted and transmitted to NaviStone through the wiretap. This real-time transmission includes, among other things, information typed on forms located on Moosejaw.com, regardless of whether the user completes the form or clicks “Submit.” Upon transmission to NaviStone, this information is used to de-anonymize website visitors.

14. NaviStone maintains a back-end database containing data and profiles on consumers across the U.S., which includes consumers’ names and mailing addresses. As users browse the various e-commerce websites that deploy NaviStone code, NaviStone attempts to “match” website visitors with records of real-life people maintained in its back-end database. This matching may occur as simply as running a database query to correlate the IP address of a website visitor, though NaviStone may also attempt to match user profiles through the use of names, addresses, and other PII. Once a match is found, NaviStone de-anonymizes the user and updates its back-end database with the user’s current browsing activities and PII.

15. NaviStone has partnered with hundreds e-commerce websites since beginning its operations. By combining and correlating its data, NaviStone can watch consumers as they browse hundreds of participating e-commerce sites, in real-time.

16. Pursuant to an agreement with NaviStone, Moosejaw intentionally embedded NaviStone’s software coded wiretap on Moosejaw.com

17. NaviStone obfuscates the wiretap codes through dummy domains to attempt to conceal its activities. For example, part of NaviStone’s remote code running on the Moosejaw is located at <http://code.murdoog.com/onetag/C1DFC24D045BDD.js> (as of the writing of this Complaint).

18. On June 20, 2017, a leading tech news website, gizmodo.com, published an

exposé on NaviStone’s wiretaps entitled “Before You Hit ‘Submit,’ This Company Has Already Logged Your Personal Data.”<sup>3</sup> The Gizmodo article describes NaviStone as “a company that advertises its ability to unmask anonymous website visitors and figure out their home addresses.”<sup>4</sup> The article revealed that NaviStone is “in the business of identifying ‘ready to engage’ customers and matching ‘previously anonymous website visitors to postal names and addresses.’ [NaviStone] says it can send postcards to the homes of anonymous website shoppers within a day or two of their visit, and that it’s capable of matching ‘60-70% of your anonymous site traffic to Postal names and addresses.’”<sup>5</sup>

19. Indeed, on its own website, NaviStone boasts that it “invented progressive website visitor tracking technology,” which allows it to “reach [] previously unidentifiable website visitors.”<sup>6</sup> According to NaviStone, “[b]y simply adding one line of code to each website page, you can unlock a new universe of ‘ready to engage’ customers.”<sup>7</sup>

20. NaviStone also explains how to implement this software wiretap on its clients’ webpages:

- 1: Insert One Line Of Code On Each Webpage.  
We’ll provide you and your IT team with a short tracking code (and instructions) to insert on *each page* of your website. Data collection begins immediately and is reviewed for quality by our staff.
- 2: Identify Engaged Website Visitors.  
Data is stored in a secure environment specifically dedicated to your company’s information. Website visitors are identified as direct marketing prospects or reactivation targets based on their level of engagement on your site, as identified by unique algorithms developed by our data

---

<sup>3</sup> <https://gizmodo.com/before-you-hit-submit-this-company-has-already-logge-1795906081>

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> <https://www.navistone.com/>

<sup>7</sup> *Id.*

scientists.

- 3: Identify Verified Names and Addresses.  
When unidentified website visitors show an intent to purchased based on the modeling process described above, NaviStone® will secure postal names and addresses to include in your direct marketing prospecting and reactivation programs. ...
- 4: Use, Expand, Repeat.  
NaviStone® will continue to track website behavior to identify new, unique prospects and reactivation targets so you can expand and optimize this unique process for success time and time again.<sup>8</sup>

21. NaviStone’s wiretap intercepts communications in real time. As *Gizmodo* put it, “before you hit ‘submit,’ this company has already logged your personal data.”<sup>9</sup> *Consumerist* also shared the same concern: “these forms collect your data even if you don’t hit ‘submit.’”<sup>10</sup>

22. NaviStone’s wiretap is engaged as soon as the visitor arrives at *Moosejaw.com*. By merely loading the main page on *Moosejaw.com*, with no other action, the visitor is connected to NaviStone’s wiretap, which begins to intercept and monitor their communications.

23. As the visitor interacts with *Moosejaw.com*, for example, by adding an item to a shopping cart, typing information onto a form, viewing an item, etc., all of these communications are intercepted and disclosed to NaviStone in real time, through the wiretap. Indeed, as will be demonstrated below, when NaviStone’s code is deployed on a webpage that contains an online form – such as a “sign up” page or an “account registration” page – the data is sent to NaviStone as it is typed. Visitors do not need to click “Submit” on the form, or take any

---

<sup>8</sup> <https://www.navistone.com/how-it-works> (last visited Nov. 3, 2017).

<sup>9</sup> <https://gizmodo.com/before-you-hit-submit-this-company-has-already-logge-1795906081> (last visited Nov. 3, 2017).

<sup>10</sup> <https://consumerist.com/2017/06/29/these-forms-collect-your-data-even-if-you-dont-hit-submit/>

other action, for their communications to be intercepted and disclosed to NaviStone.

24. NaviStone's wiretaps are deployed on hundreds of e-commerce websites. Upon information and belief, NaviStone maintains and correlates its back-end database of User Data and PII across these hundreds of websites. For example, assume that Site X and Site Y are both running NaviStone's wiretap. Now, assume that a user provides her name and phone number to Site X, but not to Site Y. Through the use of NaviStone's wiretap and back-end database, NaviStone can de-anonymize the user on Site Y and know her name and phone number, even though she never provided that information to Site Y.

**NaviStone's Wiretap In Action On Moosejaw.com**

25. The operation of NaviStone's wiretap on the Moosejaw.com website can be observed using the Developer Tools Window in the Google Chrome browser. In the images below, the Moosejaw.com website, as it appears normally through the browser is shown in the left-hand side of the window, while the Developer Tools Network View, showing incoming and outgoing transmissions, is shown in the right-hand window.

26. When Moosejaw.com is loaded into a browser, the website automatically retrieves a computer file located on a remote server. At the time this Complaint was written, the computer file was named "C1DFC24D045BDD.js," and it was hosted at <http://code.murdoog.com/onetag/>



The screenshot displays the Moosejaw website with several promotional banners. The top banner offers '50% BACK IN MOOSEJAW REWARD DOLLARS' with the code '5XREWARD17'. Below it is a 'SOREL 25% OFF' banner, and at the bottom is a 'THE NORTH FACE UP TO 40% OFF' banner. The browser's network tab is open, showing a list of requests. The first request is a JavaScript file named 'C1DFC24D045BDD.js' with a status of 200, a type of script, and a size of 24.9 KB. The second request is a script from 'https://code.murdoog.com/onetag/C1DFC24D045BDD.js' with a status of 200 and a size of 1.0 KB. The third request is another script with a status of 200 and a size of 1.2 ms. The network tab also shows a waterfall chart and a summary of 330 requests, 26.9 KB transferred, and a finish time of 3.1 min.

27. The file “C1DFC24D045BDD.js” is 24.9 KB in size and contains computer code written in a language called JavaScript. It appears as such:

```

/*! MGX v2 |(c) 2015 Melasa Group, llc. | melasagroup.com | moosejaw.com | origin onetag 10/19/2017 1:40:08 AM */
/*! 1.05 */
(function(n,t,i){n._MGX_LU=function(n){this.url=n;this.addParam=function(n,t){return typeof t=="undefined"||t==null||t==""?this:(this.url+=this.url.indexOf("?")
<0?"?":"&"+this.url+"&"+encodeURIComponent(t),this)};n._MGX_LG=function(n,i,r,u,f,e){try{var o=t.createElement("img"),s=t.getElementsByTagName("body")[0],h=new
_MGX_LU("https://apis.murdoog.com/mgx_2/visitation/pklog/message");h.addParam("k",n).addParam("v",i).addParam("p",r).addParam("r",u).addParam("ms",f.replace(/(\r\n|\n\r
&#x=);/g,"").replace(/[\s\uFEFF\uA0]/g,"")).addParam("st",e.replace(/(\r\n|\n\r&#x=);/g,"").replace(/[\s\uFEFF\uA0]/g,""));o.style="display:none";o.src=h.url;h.appendChild(o)}catch(c){};try{if(/(googlebot|bingbot)/i.test(n.navigator.userAgent))return;i(n,t)}catch(r)
{n._MGX_LG("DFC24D045BDD",null,null,"100",r.message,r.stack)}(window,document,function(n,t){if(t.cookie.indexOf("MGX_Dev")>-1&&typeof n._MGX_Dev=="undefined")
{n._MGX_Dev=unescape(t.cookie.split("MGX_Dev=")[1].split(";")[0]);var i=n._MGX_Dev.split("/")},u=new
n._MGX_LU("/api2.murdoog.com/dev/C1DFC24D045BDD.js").addParam("seq",typeof i[0]!="undefined"?i[0]:"").addParam("ver",typeof i[1]!="undefined"?
i[1]:"").addParam("wrp",typeof i[2]!="undefined"?i[2]:""),r=t.createElement("script");r.type="text/javascript";r.src=u.url;t.body.appendChild(r);console.log("Loading MGX
Dev Library "+MGX_Dev)}else(function(n,t,i){typeof t[n]!="undefined"&&(t[n]new i(n,t,t.document)))(typeof
MGXnamespace=="undefined"?MGX:MGXnamespace,n,function(n,t,i,r){var u;return{Info:"MGX Version 2.04.xxx(see MGX.Version for
subversion)",TimeOut:1e4,Delay:1e3,ProspectingInterval:3e3,LoopInterval:1e3,CommitType:"jsonp",BaseApi:"https://apis.murdoog.com/mgx_2/C/RawData/",PixelApi:"https://apis.m
urdoog.com/mgx_2/C/Pixel/",ProspectingString:"",Debug:1,FrameRef:1,OverrideHost:1,SyncVisitor:1,SyncUrl:[],Def:{pageLoad:{Label:"PageLoad"}},EmailParams:
{RestrictedFields:"",RestrictedValues:""},Version:"2.04.023",AccessKey:"DFC24D045BDD",Prospecting:"B2926D",BulkParam:"cohcid",BaseUrl:["moosejaw.com"],SuppressUrl:
[],PageLoadId:"",MgxVisitorId:"",SessionId:"",NewSession:"",Sequence:1,VisitSequence:1,RunOnce:0,KeyCode:"",Cid:"",Uid:"",Eid:"",Sid:"",Xid:"",Csi:"",JSON:t.J
SON,title:i.title,Domain:t.location.hostname.split(".").length==2?"."+t.location.hostname:t.location.hostname.slice(t.location.hostname.indexOf(".")),Url:t.location.href,
Protocol:t.location.protocol,Host:t.location.hostname,Path:t.location.pathname,Search:t.location.search,Hash:t.location.hash,Referrer:1,referrer:EmSent:
[],Em:"",utmSource:"",utmMedium:"",utmCampaign:"",regex:{Guid:/[0-9a-f]{8}-[0-9a-f]{4}-[1-5][0-9a-f]{3}-[89ab][0-9a-f]{3}-[0-9a-f]{12}$/i,Email:/[\\w-\\.]+@[\\w-\\.]+\\.([a-z
]{1,3})/i,Money:/\\$(\\d{1,3},?\\s)?\\d{2}/i},evs:{cl:0,chs:0,sc:0},pg:"pageLoad",restrict:
{"identifier","priority","altFunction","preProcess","postProcess","waitFor"},procs:
["setPageType","setUId","setEid","setCsi","handleEm","handlePageLoad","handleProspecting","handleEvents","handleLoops"],cd:[],rs:[],main:function(n){var t=this;t.RunOnce[
t.RunOnce=1,t.FrameRef&&t.setFrame()}.t.pg="pageLoad",t.chkHost()||t.OverrideHost}&&(t.Delay?setTimeout(function()
{t._main(n),t.Delay:t._main(n)}),t._main=function(n){var r=this;r.each(n,function(n,i){try{r.log.add("BEGIN["+i+"]",r.Debug);r[i]
();r.log.add("END["+i+"]",r.Debug)}catch(u){t._MGX_LG(r.AccessKey,r.VisitorId,r.PageLoadId,"200",u.message,u.stack);r.log.add("ERROR["+i+"]":
"+u.message,r.getCallStack(u),r.Debug)});typeof r.completed=="function"&&r.completed();typeof
t.MGX_Ready=="function"&&t.MGX_Ready();r.getCookie("MGX_Analyze")!=""&&setTimeout(function(){if(typeof t.MGXA=="undefined"){var
n=t.createElement("script");n.src="https://code.murdoog.com/js/mgxa.js";n.type="text/javascript";i.body.appendChild(n)}else t.MGXA(),2e3}),init:function()
{this.log.add("INFO[init]: Start MGX Init function",this.Debug);var
t=this.getCookie("MGX_P"),i=this.getCookie("MGX_U"),n=this.getCookie("MGX_PX"),r=this.getCookie("MGX_CID");this.NewSession=""?"1":"0";this.regex.Guid.test(t)||
(t=this.uid());this.setCookie("MGX_P",t,365);this.VisitorId=t;this.regex.Guid.test(i)||
(i=this.uid());this.setCookie("MGX_U",i,365);this.MgxVisitorId=i;this.regex.Guid.test(n)||
(n=this.uid());this.setCookie("MGX_PX",n);this.SessionId=n;this.regex.Guid.test(r)||
(r=this.uid());this.setCookie("MGX_CID",r,365);this.Cid=r;this.PageLoadId=this.uid();this.setUtm();this.log.add("INFO[init]: End MGX Init
function",this.Debug)},run:function(){var n=this;n.RunOnce?
(n.RunOnce=0,n.Referrer=n.Url,n.Url:t.location.href,n.Protocol:t.location.protocol,n.Host:t.location.hostname,n.Path:t.location.pathname,n.Search=t.location.search,n.Hash=t
.location.hash,n.Sequence=1,n.VisitSequence=1,n.setCookie("MGX_E",n.stringify({p:n.PageLoadId,d:n.ev}),null,10),n.ev=
{cl:0,chs:0,sc:0},n.init(n),n.main(["setPageType","handleEm","handlePageLoad","handleEvents"]);n.main(n.procs),error:function(){},trim:function(n){return typeof
n=="string"?n.replace(/(\r\n|\n\r&#x=);/g,"").replace(/[\s\uFEFF\uA0]/g,""):n},getText:function(n){if(typeof n=="undefined")return"";var
i=this,i="";try{t=n.textContent|n.textContent}catch(n){this.log.add("ERROR[getText]: "+n.message,this.getCallStack(n),this.Debug)}return
this.trim(this.cleanText(t)),getValue:function(n){var t="";if(typeof n=="undefined")return t;switch(n.nodeName){case"INPUT":switch(n.type)
{case"text":case"hidden":case"password":case"button":case"reset":case"submit":case"color":case"date":case"datetime":case"datetime-
local":case"month":case"week":case"time":case"email":case"number":case"range":case"search":case"tel":case"url":t=n.value;break;case"checkbox":case"radio":n.checked&&
(t=n.value);break;case"TEXTAREA":t=n.value;break;case"SELECT":switch(n.type){case"select-one":t=n.value;break;case"select-multiple":for(j=n.options.length-1;j>=0;j=j-
1).options[j].selected&&(t+=t+" "+n.options[j].value);break;case"BUTTON":switch(n.type){case"reset":case"submit":case"button":t=n.value}return
this.trim(t)},getRegEx:function(n,t){if(typeof t=="string")return"";var i=n.exec(t);return i==null?this.isDefined(i[0]):"",elems:function(n,t){var i=this;return typeo
f n=="string"?i.sz1(n,t):i.type(n)=="array"?i.type(n)=="htmlcollection"?n[i].sText:function(n,t){var i=this,r="",u=i elems(n,t);return u.length&&i.each(u,function(n,t)
{var u=i.getText(t);i=="&&(r+=i+"",t+u);}),r},sRegex:function(n,t,i){var r=this,u="",f=r elems(t,i);return f.length&&r.each(f,function(t,i){var

```

The top line of the code contains a comment indicating that it is to be used on “Moosejaw.com.”

However, the remainder of the code lacks comments, explanations, proper indenting, or intelligible names for variables. Essentially, this code is obfuscated.

28. The domain “code.murdoog.com,” which deploys this code, is owned and operated by NaviStone.

29. Next, the code in C1DFC24D045BDD.js is executed, with no further actions by the user, or prompting by Moosejaw or NaviStone. This immediately begins intercepting the visitors’ electronic communications and transmitting them to https://apis.murdoog.com/

The screenshot displays a web browser window with the Moosejaw website. The main banner features a "CYBER MONDAY DEAL" with a "25% OFF" discount on SOREL products. Below this, there is a promotion for "THE NORTH FACE" with "UP TO 40% OFF".

The network inspector on the right shows a request to `https://apis.murdoog.com/mgx_2/C/RawData/DFC24D0458DD?v=4d27f1a2-866c-4a6e-8dff-0e25babe177b&tm=08ec4766-4a7a-464d-a6c8-0b021c10124e&se=86d1748b-f3ea-48e2-9cf0-5a45c85d699b&sd=eyl2joiNGQyN2YyYThODY2Yy00YTZlLThkZmYtMGUyNWJhYmUxNzdliiwibS16iA4ZW`. The request body is a large Base64-encoded string containing various parameters and session identifiers.

Name	Status	Type	Initiator	Size	Time	Waterfall
C1DFC24D0458DD.js	200	script	home	24.9 KB	35 ms	
DFC24D0458DD?v=...	200	script	home	1.0 KB	92 ms	
DFC24D0458DD?v=...	200	script	home	1.0 KB	12 ms	

Summary: 3 / 390 requests | 26.9 KB / 3.2 MB transferred | Finish: 7.5 min | DOMContentLoaded: 1.22 s | Load: 1.4...

30. The domain “apis.murdoog.com” is also owned and operated by NaviStone.

31. The intercepted communications are encoded in a format called Base64. When

decoded, they appear as such:

```
{ "v": "4d27f1a2-866c-4a6e-8dff-0e25babe177b", "m": "08ec4766-4a7a-464d-a6c8-0b021c10124e", "csi": "2003644151", "se": "86d1748b-f3ea-48e2-9cf0-5a45c85d699b", "p": "e6cb9e61-fa6c-4e44-83eb-58f9ee2d5e6a", "u": "https://www.moosejaw.com/moosejaw/shop/home____", "pn": "/moosejaw/shop/home____", "t": "North Face Jackets | Patagonia Jackets | Arcteryx Jackets | Mountain Hardwear", "c": "https://www.moosejaw.com/moosejaw/shop/home____", "pr": "B2926D", "eid": "ns_seg_100", "sid": "30594e2641630c11abd0dd73b8c4061e", "s": 2, "vs": 1, "l": "Action", "v01": "Eid", "v02": "ns_seg_100" }
```



```
9cf0-5a45c85d699b", "p": "74ff4509-26a4-4c4c-88ce-68a9e3793d7a", "u": "https://www.moosejaw.com/moosejaw/shop/product_Moosejaw-Men-s-The-Jack-Pullover-Hoody_10273018_10208_10000001_1_", "pn": "/moosejaw/shop/product_Moosejaw-Men-s-The-Jack-Pullover-Hoody_10273018_10208_10000001_1_", "r": "https://www.moosejaw.com/moosejaw/shop/search_Mens-Hoodies____", "t": "Moosejaw Men's The Jack Pullover Hoody - at Moosejaw.com", "c": "https://www.moosejaw.com/moosejaw/shop/product_Moosejaw-Men-s-The-Jack-Pullover-Hoody_10273018_10208_10000001_1_", "pr": "B2926D", "eid": "ns_seg_100", "sid": "30594e2641630c11abd0dd73b8c4061e", "s": 3, "vs": 7, "l": "Action", "v01": "AddToCart", "v03": "CartClick", "v04": "/moosejaw/shop/product_Moosejaw-Men-s-The-Jack-Pullover-Hoody_10273018_10208_10000001_1_"}qem$g
```

33. When filling out forms, any PII the user provides is immediately, automatically, and secretly transmitted to NaviStone in real-time. Here, the user has just arrived on the “Checkout” page, and has not entered any information yet:

The screenshot shows the Moosejaw website's checkout process. The page is titled "Moosejaw" and features a navigation bar with "RETURN ANY TIME as long as you're alive" and "SECURITY & PRIVACY are guaranteed". A "Sign In" button is present for existing customers. The main content is divided into two sections: "1. CONTACT INFO" and "2. ADDRESS INFO".

**1. CONTACT INFO**

Email  For order confirmation and tracking info

**2. ADDRESS INFO**

**SHIPPING ADDRESS**

First Name  Last Name

Phone Number  United States

Company Name (optional)  Street address

Street address line 2 (optional)  ZIP code  *Enter and we'll look-up your city and state.*

City  Choose a State

This is also my billing address

**BILLING ADDRESS**

First Name  Last Name

Phone Number  United States

**MY CART** *Details*

Subtotal: **\$50.00**  
 Shipping: **FREE**  
 Sales Tax: **\$0.00**  
**TOTAL: \$50.00**  
 You Earned: **\$5.00** *Rewards of*

[Place Secure Order](#)

ABOUT SSL CERTIFICATES

3 / 250 requests | 2.0 KB / 605 KB transferred | Finish: 7.16 s | DOMContentLoaded: 2.15 s | Load: 3.03 s

The browser developer tool is open, showing the Network tab with a waterfall chart and a table of requests:

Name	Status	Type	Initiator	Size	Time	Waterfall
C1DFC24D0458DD.js	200	script	Order:Shi...	1.0 KB	23 ms	
DFC24D0458DD?v...	200	script	C1DFC24...	1.0 KB	15 ms	
DFC24D0458DD?v...	200	script	C1DFC24...	1.0 KB	13 ms	

Now, the user has entered his name "John." A transmission is automatically, immediately, and secretly made to NaviStone:

The screenshot shows a web browser window with the URL <https://www.moosejaw.com/moosejaw/shop/OrderShippingBillingView?storeId=10208&catalogId=10000001&langId=-1&krypto=0Jrk5pTd4K1r5QISdrjro5CvK11PRvgeH2f3rbbqGRFZVPny3...>

**1. CONTACT INFO**  
 Existing customers sign in for easier checkout.  
 Email:  For order confirmation and tracking info

**2. ADDRESS INFO**  
**SHIPPING ADDRESS**  
 John Last Name  
 Phone Number United States  
 Company Name (optional) Street address  
 Street address line 2 (optional) ZIP code *Enter and we'll look-up your city and state.*  
 City Choose a State  
 This is also my billing address

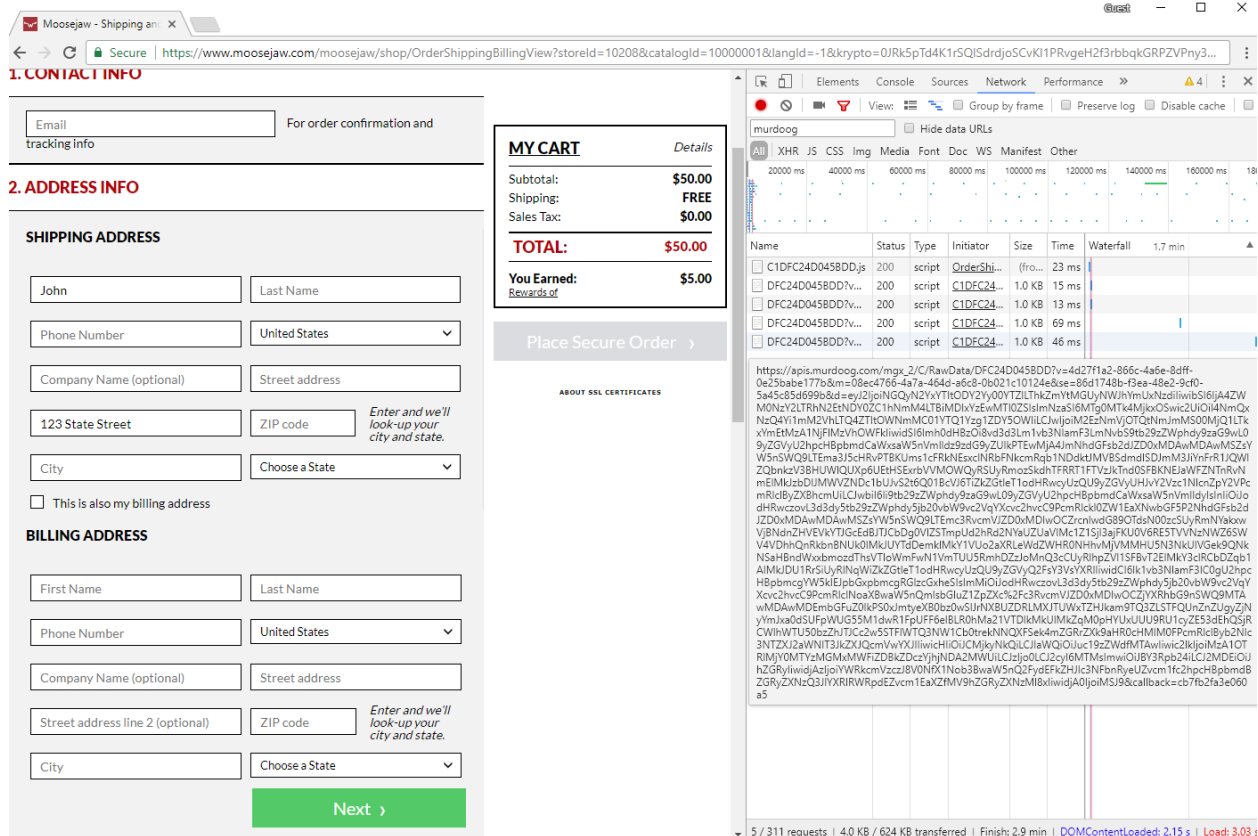
**BILLING ADDRESS**  
 First Name Last Name  
 Phone Number United States  
 Company Name (optional) Street address  
 Street address line 2 (optional) ZIP code *Enter and we'll look-up your city and state.*

**MY CART** *Details*  
 Subtotal: **\$50.00**  
 Shipping: **FREE**  
 Sales Tax: **\$0.00**  
**TOTAL: \$50.00**  
 You Earned: **\$5.00**  
[Reorder](#)

**Place Secure Order**

**Network Developer Tool:**  
 Shows a list of requests. The selected request is a script named `C1DFC240458DD7...` with a size of 1.0 KB and a time of 23 ms. The response is a large block of Base64-encoded data starting with `https://apis.murdoog.com/mgx_2/C/RawData/DFC240458DD7v=4d27f1a2-866c-4a6e-8dff-0e25babe177b8m=08ec4766-4a7e-464d-a6c8-0b021c10124e8se=86d1748b-f3ea-48e2-9cf0-5a45c85d699b&d=eyJ2oiNGQyN2YxYTl0ODY2y00YTZlThk2emY1MGUyNWJhYmUxNzdlilwibS6ijA4ZW...`

Now, the user has entered his address at “123 State Street.” Again, another transmission is automatically, immediately, and secretly made to NaviStone:



34. By intercepting these communications, NaviStone is able to learn the identity of the visitor. As NaviStone boasts, it is capable of matching “60-70% of your anonymous site traffic to Postal names and addresses.”<sup>11</sup>

**Other Allegations Common To All Claims**

35. Defendants, as corporations, are “persons” pursuant to 18 U.S.C. § 2510(6).

36. Plaintiff’s and Class Members’ keystrokes, mouseclicks, and other interactions with Moosejaw.com are “electronic communications” as defined by 18 U.S.C. § 2510(12).

37. Throughout the entirety of the conduct upon which this suit is based, Defendants’ actions have affected interstate commerce.

38. Defendants’ actions are and have been intentional as evidenced by, *inter alia*,

<sup>11</sup> *Id.*



their design and implementation of the software wiretap on Moosejaw.com, and their disclosures and uses of the intercepted communications for profit.

**CLASS ACTION ALLEGATIONS**

39. Plaintiff seeks to represent a class all persons whose electronic communications were intercepted through the use of NaviStone's wiretap on Moosejaw.com.

40. Members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the millions. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendants.

41. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to, whether Defendants intentionally intercepted electronic communications in violation of 18 U.S.C. § 2511(1)(a); whether Defendants intentionally disclosed the intercepted electronic communications in violation of 18 U.S.C. § 2511(1)(c); whether Defendants intentionally used, or endeavored to use the intercepted electronic communications to de-anonymize website visitors in violation of 18 U.S.C. § 2511(1)(d); whether Moosejaw procured NaviStone to intercept or endeavor to intercept electronic communications in violation of 18 U.S.C. § 2511(1)(a); whether NaviStone procured Moosejaw to intercept or endeavor to intercept electronic communications in violation of 18 U.S.C. § 2511(1)(a); whether NaviStone's wiretaps, including the software codes described herein, are an "electronic, mechanical, or other device" as defined by 18 U.S.C. § 2510(5); whether NaviStone's wiretaps are primarily useful for the purpose of the surreptitious interception of

electronic communications in violation of 18 U.S.C. § 2512; whether NaviStone violated 18 U.S.C. § 2512 by intentionally creating the wiretap codes, by possessing those wiretaps, by advertising them on the NaviStone website, and by distributing them to Moosejaw for installation on Moosejaw's website; whether Moosejaw violated 18 U.S.C. § 2512 by receiving the wiretaps from NaviStone, which were transported through interstate commerce, by possessing those wiretaps, and by further distributing them through the software codes embedded on Moosejaw.com; whether each class member is entitled to the remedies specified under 18 U.S.C. § 2520, including but not limited to statutory damages of \$10,000 per class member.

42. The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other class members, visited Moosejaw.com and had his electronic communications intercepted and disclosed to NaviStone through the use of NaviStone's wiretap.

43. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class members he seeks to represent, he has retained competent counsel experienced in prosecuting class actions, and he intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and his counsel.

44. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendants' liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action

device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendants' liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

45. Plaintiff brings all claims in this action individually and on behalf of members of the Class against Defendants.

**Count I**  
**For Interception Of Electronic Communications In Violation Of The Wiretap Act,  
18 U.S.C. § 2511(1)(a)**

46. Plaintiff repeats the allegations contained in ¶¶ 1-45, above, as if fully set forth herein.

47. By implementing NaviStone's wiretaps on Moosejaw.com, each Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

**Count II**  
**For Disclosure Of Intercepted Electronic Communications In Violation Of The Wiretap  
Act, 18 U.S.C. § 2511(1)(c)**

48. Plaintiff repeats the allegations contained in ¶¶ 1-45, above, as if fully set forth herein.

49. By intentionally disclosing the intercepted electronic communications of the Plaintiff and Class Members to each other, and to other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants have violated 18 U.S.C. § 2511(1)(c).

**Count III**

**For Use Of Intercepted Electronic Communications In Violation Of The Wiretap Act,  
18 U.S.C. § 2511(1)(d)**

50. Plaintiff repeats the allegations contained in ¶¶ 1-45, above, as if fully set forth herein.

51. By intentionally using, or endeavoring to use, the contents of the Plaintiff's and Class Members' intercepted electronic communications to de-anonymize them, and for other purposes, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants have violated 18 U.S.C. § 2511(1)(d).

**Count IV**

**For Procuring In Violation Of The Wiretap Act, 18 U.S.C. § 2511(1)(a)**

52. Plaintiff repeats the allegations contained in ¶¶ 1-45, above, as if fully set forth herein.

53. By intentionally procuring NaviStone to intercept or endeavor to intercept electronic communications, Moosejaw violated 18 U.S.C. § 2511(1)(a).

54. By intentionally procuring Moosejaw to intercept or endeavor to intercept electronic communications, NaviStone violated 18 U.S.C. § 2511(1)(a).

**Count V**

**For Manufacture, Distribution, Possession And Advertising Of Electronic  
Communication Intercepting Devices  
In Violation Of The Wiretap Act,  
18 U.S.C. § 2512**

55. Plaintiff repeats the allegations contained in ¶¶ 1-45, above, as if fully set forth herein.

56. NaviStone's wiretaps, including the software codes described herein, are an "electronic, mechanical, or other device" as defined by 18 U.S.C. § 2510(5), are primarily useful

for the purpose of the surreptitious interception of electronic communications.

57. By intentionally creating the wiretap codes, by possessing those wiretaps, by advertising them on the NaviStone website, and by distributing them to Moosejaw for installation on Moosejaw's website, NaviStone violated 18 U.S.C. § 2512.

58. By receiving the wiretaps from NaviStone, which were transported through interstate commerce, by possessing those wiretaps, and by further distributing them through the software codes embedded on Moosejaw.com, Moosejaw violated 18 U.S.C. § 2512.

### **Relief Sought**

59. WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendants as follows:

- A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- B. For an order declaring that Defendants' conduct as described herein violates the statutes referenced herein;
- C. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- D. For all remedies specified in the Wiretap Act, 18 U.S.C. § 2520, including the actual damages suffered by the plaintiff, any profits made by Defendants as a result of the violations, statutory damages of whichever is greater of \$100 a day for each day of violation or \$10,000 for each class member, such preliminary and other equitable or declaratory relief as may be appropriate, punitive damages, and a reasonable attorney's fee and other litigation costs reasonably incurred;
- E. For prejudgment interest on all amounts awarded;
- F. For an order of restitution and all other forms of equitable monetary relief;
- G. For injunctive relief as pleaded or as the Court may deem proper; and
- H. For an order awarding Plaintiff and the Class their reasonable



# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [NaviStone Named in Second Class Action Lawsuit This Week Over Alleged 'Wiretapping' of Retail Website Users](#)

---