

# Committee Report

**REGULAR CALENDAR**

**March 2, 2021**

**HOUSE OF REPRESENTATIVES**

**REPORT OF COMMITTEE**

**The Majority of the Committee on Judiciary to which  
was referred HB 384-FN,**

**AN ACT prohibiting the sharing of location data.**

**Having considered the same, report the same with the  
following amendment, and the recommendation that  
the bill OUGHT TO PASS WITH AMENDMENT.**

**Rep. Kurt Wuelper**

**FOR THE MAJORITY OF THE COMMITTEE**

**MAJORITY  
COMMITTEE REPORT**

Committee:	<b>Judiciary</b>
Bill Number:	<b>HB 384-FN</b>
Title:	<b>prohibiting the sharing of location data.</b>
Date:	<b>March 2, 2021</b>
Consent Calendar:	<b>REGULAR</b>
Recommendation:	<b>OUGHT TO PASS WITH AMENDMENT 2021-0155h</b>

**STATEMENT OF INTENT**

This bill, as amended, prohibits any mobile application developer, telecommunications carrier, or other person from selling or permitting access to customer personal location data unless the customer expressly consents to that sale or access. The bill prohibits a provider from refusing to serve a customer, charging a customer a penalty, or offering a customer a discount if the customer does not consent to the use, disclosure, sale, or access. Nothing in this bill limits how your location data can be internally used by a service provider. The bill has broad exemptions for law enforcement, emergencies, and other legal processes. The majority believes where you are and where you have been an important element of our privacy and that information should be protected just as much as your birth date.

Vote 16-4.

Rep. Kurt Wuelper  
FOR THE MAJORITY

Original: House Clerk  
Cc: Committee Bill File

## REGULAR CALENDAR

Judiciary

**HB 384-FN**, prohibiting the sharing of location data. **MAJORITY: OUGHT TO PASS WITH AMENDMENT. MINORITY: INEXPEDIENT TO LEGISLATE.**

Rep. Kurt Wuelper for the **Majority** of Judiciary. This bill, as amended, prohibits any mobile application developer, telecommunications carrier, or other person from selling or permitting access to customer personal location data unless the customer expressly consents to that sale or access. The bill prohibits a provider from refusing to serve a customer, charging a customer a penalty, or offering a customer a discount if the customer does not consent to the use, disclosure, sale, or access. Nothing in this bill limits how your location data can be internally used by a service provider. The bill has broad exemptions for law enforcement, emergencies, and other legal processes. The majority believes where you are and where you have been an important element of our privacy and that information should be protected just as much as your birth date. **Vote 16-4.**

Original: House Clerk

Cc: Committee Bill File

**REGULAR CALENDAR**

**March 2, 2021**

**HOUSE OF REPRESENTATIVES**

**REPORT OF COMMITTEE**

**The Minority of the Committee on Judiciary to which  
was referred HB 384-FN,**

**AN ACT prohibiting the sharing of location data.**

**Having considered the same, and being unable to agree  
with the Majority, report with the following resolution:**

**RESOLVED, that it is INEXPEDIENT TO LEGISLATE.**

**Rep. Timothy Horrigan**

**FOR THE MINORITY OF THE COMMITTEE**

**MINORITY  
COMMITTEE REPORT**

Committee:	<b>Judiciary</b>
Bill Number:	<b>HB 384-FN</b>
Title:	<b>prohibiting the sharing of location data.</b>
Date:	<b>March 2, 2021</b>
Consent Calendar:	<b>REGULAR</b>
Recommendation:	<b>INEXPEDIENT TO LEGISLATE</b>

**STATEMENT OF INTENT**

The minority of the Judiciary Committee agrees with the majority that online privacy is an important issue for Granite Staters. This bill is, however, a crude and inflexible attempt to solve an extraordinarily complicated problem which in any case could best be addressed, and is being addressed, on a federal level. This bill, if passed, would accomplish little if anything aside from denying Granite State residents, visitors, and businesses access to valuable online location-based services. It would also destroy jobs by driving high-tech firms to other states or countries and by crippling the growth of the new "gig economy." Finally, this bill would impose fines which could literally run into the millions of dollars on businesses and individuals who inadvertently violate the vague provisions of this bill.

Rep. Timothy Horrigan  
FOR THE MINORITY

Original: House Clerk  
Cc: Committee Bill File

## REGULAR CALENDAR

Judiciary

**HB 384-FN**, prohibiting the sharing of location data. **INEXPEDIENT TO LEGISLATE.**

Rep. Timothy Horrigan for the **Minority** of Judiciary. The minority of the Judiciary Committee agrees with the majority that online privacy is an important issue for Granite Staters. This bill is, however, a crude and inflexible attempt to solve an extraordinarily complicated problem which in any case could best be addressed, and is being addressed, on a federal level. This bill, if passed, would accomplish little if anything aside from denying Granite State residents, visitors, and businesses access to valuable online location-based services. It would also destroy jobs by driving high-tech firms to other states or countries and by crippling the growth of the new "gig economy." Finally, this bill would impose fines which could literally run into the millions of dollars on businesses and individuals who inadvertently violate the vague provisions of this bill.

Original: House Clerk

Cc: Committee Bill File

Rep. Wuelper, Straf. 3  
January 28, 2021  
2021-0155h  
04/06

Amendment to HB 384-FN

1 Amend RSA 570-A:2-b, II(a) as inserted by section 1 of the bill by replacing it with the following:

2

3 II(a) No mobile application developer or a telecommunications carrier shall share a  
4 customer's location data, other than to fulfill an explicit request from such customer, unless the  
5 customer has affirmatively waived such right after being properly informed. For purposes of this  
6 section, continuing to use a service or website shall not be considered an affirmative waiver.



# Voting Sheets



Rep Kurt Wuelper, Clerk

STATE OF NEW HAMPSHIRE  
OFFICE OF THE HOUSE CLERK



1/22/2021 10:07:24 AM  
Roll Call Committee Registers  
Report

2021 SESSION

Judiciary

Bill #: HB 384 Motion: \_\_\_\_\_ AM #: 0155 Exec Session Date: 3/2/2021

<u>Members Attendance</u>	<u>YEAS</u>	<u>Nays</u>	<u>NV</u>
Gordon, Edward M. Chairman			
McLean, Mark Vice Chairman			
Sylvia, Michael J.			
Wuelper, Kurt F. Clerk			
Alexander, Joe H.			
Rice, Kimberly A.			
Silber, Norman J.			
Greene, Bob J.			
Kelley, Diane E.			
Tausch, Lindsay			
Trottier, Douglas R.			
Smith, Marjorie K.			
Berch, Paul S.			
Horrigan, Timothy O.			
DiLorenzo, Charlotte I.			
Chase, Wendy			
Kenney, Cam E.			
Langley, Diane M.			
McBeath, Rebecca Susan			
Paige, Mark			
Simpson, Alexis			
<b>TOTAL VOTE:</b>		<b>0</b>	

STATE OF NEW HAMPSHIRE  
OFFICE OF THE HOUSE CLERK



1/22/2021 10:07:24 AM  
Roll Call Committee Registers  
Report

2021 SESSION

Judiciary

Bill #: HB 384 Motion: \_\_\_\_\_ AM #: \_\_\_\_\_ Exec Session Date: /2021

<u>Members Attendance</u>	<u>YEAS</u>	<u>Nays</u>	<u>NV</u>
Gordon, Edward M. Chairman			
McLean, Mark Vice Chairman			
Sylvia, Michael J.			
Wuelper, Kurt F. Clerk			
Alexander, Joe H.			
Rice, Kimberly A.			
Silber, Norman J.			
Greene, Bob J.			
Kelley, Diane E.			
Tausch, Lindsay			
Trottier, Douglas R.			
Smith, Marjorie K.			
Berch, Paul S.			
Horrigan, Timothy O.			
DiLorenzo, Charlotte I.			
Chase, Wendy			
Kenney, Cam E.			
Langley, Diane M.			
McBeath, Rebecca Susan			
Paige, Mark			
Simpson, Alexis			
<b>TOTAL VOTE:</b>		<b>0</b>	

# Public Hearing

HOUSE COMMITTEE ON JUDICIARY

PUBLIC HEARING ON HB 384

**BILL TITLE:** prohibiting the sharing of location data.

**DATE:** 2/19/2021

**LOB ROOM:** Remote                      **Time Public Hearing Called to Order:** 1:00 PM  
**Time Adjourned:**

**Committee Members:** Reps. Gordon, McLean, Wuelper, Sylvia, Alexander Jr., Rice, Silber, Greene, D. Kelley, Tausch, Trottier, M. Smith, Berch, Horrigan, DiLorenzo, Chase, Kenney, Langley, McBeath, Paige and Simpson

**Bill Sponsors:** Rep

TESTIMONY

\* Use asterisk if written testimony and/or amendments are submitted.

\*Rep.

# House Remote Testify

## Judiciary Committee Testify List for Bill HB384 on 2021-02-19

Support: 15 Oppose: 10 Neutral: 0 Total to Testify: 1

Export to Excel

<u>Name</u>	<u>City, State</u> <u>Email Address</u>	<u>Title</u>	<u>Representing</u>	<u>Position</u>	<u>Testifying</u>	<u>Non-Germane</u>	<u>Signed Up</u>
Kingman, Andrew	Essex, MA andrew.kingman@us.dlapiper.com	A Member of the Public	State Privacy and Security Coalition	Oppose	Yes (3m)	No	2/18/2021 5:30 PM
Oswald, Christopher	Washington, DC coswald@ana.net	A Lobbyist	ANA and the Joint Advertising Trade Associations	Oppose	No	No	2/18/2021 8:22 PM
Mott-Smith, Wiltrud	Loudon, NH wmottsm@worldpath.ney	A Member of the Public	Myself	Support	No	No	2/18/2021 9:26 PM
See, Alvin	Loudon, NH absee@4Liberty.net	A Member of the Public	Myself	Support	No	No	2/18/2021 9:54 PM
Weston, Maura	Concord, NH mauraweston@comcast.net	A Lobbyist	The New England Cable and Telecommunications Association	Oppose	No	No	2/19/2021 7:28 AM
Hennessey, Jason	Amherst, NH jayhennspam@yahoo.com	A Member of the Public	Myself	Support	No	No	2/19/2021 12:24 PM
Lewicke, John	Mason, NH john.lewicke@leg.state.nh.us	An Elected Official	Myself	Support	No	No	2/19/2021 1:54 PM
Sargent, Elizabeth	Concord, NH esargent@sheehan.com	A Lobbyist	NH Association of Chiefs of Police	Oppose	No	No	2/19/2021 10:21 AM
Howard Jr., Raymond	Alton, NH brhoward@yahoo.com	An Elected Official	Myself	Support	No	No	2/19/2021 8:23 AM
Baker, Kyle	Concord, NH krb@rypgranite.com	A Lobbyist	Internet Coalition	Oppose	No	No	2/19/2021 8:41 AM
McGillen, Michael	Auburn, NH mm64@comcast.net	A Member of the Public	Myself	Oppose	No	No	2/19/2021 11:33 AM
Murdough, Ryan	Washington NH, NH rmurdough@washingtonnh.org	A Member of the Public	Myself	Oppose	No	No	2/19/2021 11:34 AM
Lekas, Tony	Rep. Tony.Lekas@gmail.com	An Elected Official	Hillsborough 37	Support	No	No	2/10/2021 1:35 PM



Fordey, Nicole	nikkif610@gmail.com	A Member of the Public	Myself	Oppose	No	No	2/13/2021 8:28 PM
Lascaze, Joseph	joseph@aclu-nh.org	A Member of the Public	Myself	Support	No	No	2/14/2021 2:09 PM
Krohn, Suzanne	suzanne.c.krohn@gmail.com	A Member of the Public	Myself	Support	No	No	2/15/2021 10:50 AM
Krohn, Matthew	makrohn@gmail.com	A Member of the Public	Myself	Support	No	No	2/15/2021 11:14 AM
Gould, Rep. Linda	lgouldr@myfairpoint.net	An Elected Official	Myself	Support	No	No	2/15/2021 2:15 PM
Frost, Sherry	sherry.frost@leg.state.nh.us	An Elected Official	Myself	Oppose	No	No	2/15/2021 2:43 PM
McGuire, Daniel	danmcguire@gmail.com	A Member of the Public	Myself	Support	No	No	2/15/2021 6:32 PM
Pauer, Eric	secretary@BrooklineGOP.org	A Member of the Public	Myself	Support	No	No	2/17/2021 12:32 PM
DeMark, Richard	Meredith, NH demarknh114@gmail.com	A Member of the Public	Myself	Oppose	No	No	2/17/2021 4:45 PM
Groetzinger, Tonda	Farmington, NH groetzinger6@aol.com	A Member of the Public	Myself	Support	No	No	2/18/2021 2:09 PM
kurk, neal	weare, NH rep03281@aol.com	A Member of the Public	Myself	Support	No	No	2/18/2021 4:48 PM
Hruska, Jeanne	Concord, NH Jeanne@aclu-nh.org	A Lobbyist	ACLU-NH	Support	No	No	2/18/2021 4:49 PM

# Testimony



Tammy Cota, Executive Director  
1 Blanchard Court, Suite 101  
Montpelier, VT 05602  
802-279-3534  
[tammy@theinternetcoalition.com](mailto:tammy@theinternetcoalition.com)  
[www.theinternetcoalition.com](http://www.theinternetcoalition.com)

February 19, 2021

Honorable Edward Gordon, Chair  
House Judiciary Committee  
LOB Room 208  
107 North Main Street  
Concord, NH 03301

**Re: IC must respectfully oppose HB 384, Sharing of Location Data**

Dear Chairman Gordon:

By way of introduction, the Internet Coalition (IC) is a national trade association that represents members in state public policy discussions. The IC also serves as an informational resource, striving to protect and foster the Internet economy and the benefits it provides consumers.

IC understands the challenges when attempting to regulate technological complex areas in a balanced way, that allows growth of innovation while simultaneously protecting consumers from harm. IC supports well-thought out, narrowly defined geolocation laws that adequately solve a specific issue, provide remedies in an effective way and are flexible enough to allow for innovation to flourish while avoiding limiting an entire segment of data.

Therefore, IC must **respectfully oppose HB 384**, which is too broadly worded, could unintentionally hamper user experiences and disrupt many harmless conveniences that users have come to expect online. The bill is unnecessary, offers little additional or effective consumer protections and companies would be bombarded with unscrupulous lawsuits since the bill would expose them to private rights of action, even for minor or unknown infractions.

Mobile device location information is vital to the functioning of many apps, allowing them to tailor content to the user's location. Companies adhere to strong privacy policies which prohibit the sale of location data by apps. These privacy policies are enforceable by the Attorney General and the Federal Trade Commission. Users can view privacy policies and are made aware of their ability to control how the app interacts with their location data before downloading apps and during use of a service. Users can hand-tailor the location data settings on most devices and may restrict collection of location data per app at any time.

Precise geolocation information linked to someone specifically should be treated appropriately. However, excluding anonymized data sharing from the definition of "authorized use" would impact thousands of geolocation-based business models that use location data not linked to specific person. Banning or restricting positive and innocuous use of anonymized data would end valuable and widely used services like ridesharing, education, tourism, urban planning and telework applications. It may disable use of services like "find my device" and many applications involving photographs, free public wifi and mapping/navigation services.

The bill does not appear to only cover New Hampshire residents, but anyone located in the state. This could mean more location data would have to be collected for companies to attempt to comply with this law. This is a good example as to why IC believes location data legislation is best left to Congress. National laws would prevent a patchwork of various and possibly conflicting state laws, which would make it extremely difficult if not impossible for companies to legally operate across state lines.

Since this bill contains broad and problematic definitions, would interrupt consumers' online experiences, is unnecessary, would expose businesses to frivolous lawsuits and would deter innovation, we ask that you please **oppose HB 384**.

Please feel free to contact me if you have questions or would like to discuss this in more detail.

Sincerely,

A handwritten signature in black ink that reads "Tammy Cota". The signature is written in a cursive, flowing style.

Tammy Cota

cc: House Judiciary Committee members

# The State of New Hampshire

## ADMINISTRATIVE OFFICE OF THE COURTS

Christopher Keating  
Director

1 Granite Place, Suite N400  
Concord, NH 03301  
(603) 271-2521  
Fax: (603) 513-5454  
eMail: aoc@courts.state.nh.us  
TTY/TDD Relay: (800) 735-2964

February 15, 2021

The Honorable Edward Gordon, Chair  
House Judiciary Committee  
Legislative Office Building  
Concord, New Hampshire 03301

RE: HB 384 (prohibiting the sharing of location data)

Dear Representative Gordon:

I am writing to make you aware of a concern the Judicial Branch has with regard to the proposed effective date of House Bill 384. The current draft has a proposed effective date of 60 days after its passage. Under RSA 14:9-a “[e]ach law affecting judicial practice and procedure, or establishing or eliminating criminal prohibitions, civil causes of action or remedies, or limitations of actions, shall take effect on the January 1 following passage.” Because this law would establish criminal prohibitions, RSA 14:9-a provides that it should be effective no sooner than January 1, 2022.

The additional time is needed for the Judicial Branch to implement the collective changes that will be made to laws during this legislative session that impact criminal and civil cases. After each legislative session, the Judicial Branch must update the uniform charge table and the Judicial Branch’s Odyssey database, modify or create new forms, make necessary changes to the e-filing system, and notify and train judges and staff on the hundreds of changes that affect the court system. Implementation of these changes must accurately reflect the changes in law and be properly programed into the case management database and e-filing system. Given the number of changes that must be implemented, it takes several months to complete this effort.

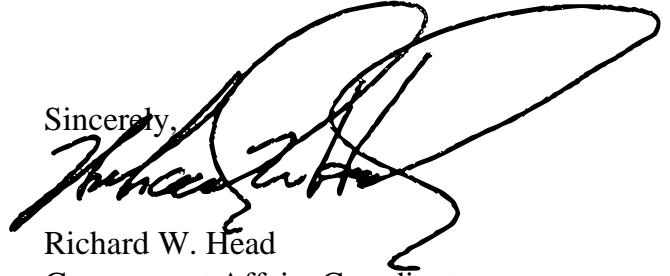
I am writing to request the bill be amended to change the effective date to January 1, 2022 which will allow the Judicial Branch sufficient time to implement all of the changes described in the bills that are passed in this session.

February 15, 2021

Page 2

Thank you for your consideration of this request. Please do not hesitate to contact me if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard W. Head", written over the word "Sincerely,".

Richard W. Head  
Government Affairs Coordinator  
Email: [rhead@courts.state.nh.us](mailto:rhead@courts.state.nh.us)  
Cell: 603-716-8235

cc: Representative Kurt Wuelper, Prime Sponsor  
[kurt.wuelper@leg.state.nh.us](mailto:kurt.wuelper@leg.state.nh.us)



**TECHNET**  
THE VOICE OF THE  
INNOVATION ECONOMY

**STATE  
PRIVACY &  
SECURITY  
COALITION**

February 19, 2021

The Honorable Representative Edward Gordon, Chair  
House Judiciary Committee  
LOB Room 208  
107 North Main Street  
Concord, NH 03301

***Re: HB 384 – Prohibiting the Sharing of Location Data***

Dear Chair Gordon and members of the Committee,

TechNet, the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy and represents over three million employees – including thousands here in New Hampshire, along with the State Privacy and Security Coalition, a cross-sectoral coalition of 29 companies and eight trade associations in the retail, technology, telecommunications, automobile, payment card, and online security sectors, respectfully oppose HB 384, which establishes a civil penalty for the unauthorized disclosure of electronic location information by application developers and service providers. HB 384 is unnecessary, confusing and harmful in its approach to the issue of consumer privacy by proposing technology-and-sector-specific prohibitions which, if passed, would make New Hampshire an outlier; no other state has such a broad and ambiguous law.

**HB 384 Does Not Reflect the Modern Online Ecosystem**

HB 384 is not a practical solution for New Hampshire. While it was drafted with good intentions, it does not translate into public policy that will increase protections for New Hampshire residents or allow businesses to easily understand and comply with its ambiguous mandates.

This legislation is problematic for many reasons but notably it because fails to make any distinction between personally identifiable information (PII) and aggregated/anonymized data. Often, companies are not actually sharing an individual's specific data, but anonymized datasets. The sharing of anonymized data underpins much of the modern Internet. Both GDPR and the California Consumer Privacy Act recognize this distinction and establish separate rules for anonymized (or deidentified) data.

Additionally, the bill does not recognize the critical role that service providers play in the modern online ecosystem. Service providers are businesses who have relationships with companies to perform specific services on behalf of the companies but are generally prohibited from using customer information for their own uses. Examples of these businesses which require location information to provide services include shipping fulfillment and payment card processing. Because this bill does not recognize such arrangements,



literally every transfer of information – even if it is for the business’ own purpose and not for an exchange of money – would fall within this bill’s scope, creating a regulatory scheme unrecognized in any other state.

In practical terms, this bill would result in small businesses who often use free services such as cookies to gather basic information about its customers (so that, for example, the business knows from where its customers are originating). These types of routine, non-invasive technologies would be prohibited under this legislation.

### **HB 384 is Vague and Not Feasible to Comply With**

While HB 384 defines “authorized use,” the term is not used anywhere in the operative provisions. Additionally, the definition does not contemplate the business-service provider relationship described above, where businesses frequently use information to provide goods and services that consumers have come to rely on. The result is that this bill would impose unreasonable and unwarranted limitations that would prevent companies from performing functions expected by customers.

Without clarity as to how a company may determine whether a customer “explicitly requested” a service, companies would likely send customers mobile app pop-up consent notifications to obtain affirmative consent each time the relevant location information is shared. Customers will be inundated with pop-up consents to permit sharing and experience delays in service or functions they typically expect, since location information is often used for a variety of incidental or background business functions (i.e., processing shipping, collecting payment information, publicizing customer reviews, etc.). Further, deploying a consent mechanism is a complicated process to implement and, as a result, imposes significant costs on local businesses.

in addition to an unclear definition of “authorized use,” this bill contains an overbroad definition of “location information” such that any sharing of location information, regardless of the level of precision, will require a customer’s consent. As drafted, “location information” might range from broad areas such as city and state or ZIP code to more precise location. Companies would be required to obtain consent any time this information is collected through a mobile device and provided to another person, be it another company for a reasonable use or in a public forum such as a website or social media app – further impairing a company’s ability to provide services its customers expect but may not explicitly request.

Even more confusing and frustrating to consumers will be the fact that the bill attempts to govern not just NH residents, but anyone located in NH. When out-of-state families enter the state to go skiing or snowmobiling each weekend, they would be deluged with opt-in notifications from businesses they already have a relationship with and already expect to perform services on their behalf. This process would repeat each weekend as they exit and re-enter the state.

***Ironically, because the bill does not govern only New Hampshire residents, companies would likely have to collect more geolocation information about individuals in order to attempt to comply with this bill’s ambiguous mandates.***





Notably this bill only applies to location data collected by a mobile device physically present in a "town or city" and is silent on sharing the location of individuals or their devices when in unincorporated areas of New Hampshire.

### **HB 384's Vagueness Exposes Companies to Frivolous Litigation**

TechNet and SPSC's member companies are also strongly opposed to the inclusion of a private right of action that enables trial lawyers to sue their wireless providers and developers of applications for transactions that are routine and expected by consumers, but would be prohibited by this law. A private right of action would open companies up to untold amounts of litigation and could significantly hamper companies' ability to operate, even if they are making best efforts to comply. Many services and functions that New Hampshire residents know and rely on would no longer be accessible, as companies would likely remove or restrict functionality in the state to avoid the potential litigation risk. Further, the risk of legal exposure will have a chilling effect on entrepreneurs launching new products and developing new applications here.

While we appreciate the desire of the sponsor to protect the privacy of New Hampshire residents, companies also need the ability operate in accordance with the law while providing the services that consumers expect and rely on. This legislation fails to do both and therefore we strongly urge the Committee to not advance this legislation.

Thank you in advance for your consideration on these matters and please do not hesitate to reach out with any questions.

Sincerely,

Christopher Gilrein  
Executive Director, Massachusetts and the Northeast  
TechNet  
[cgilrein@technet.org](mailto:cgilrein@technet.org)

Andrew A. Kingman  
General Counsel  
State Privacy and Security Coalition  
[andrew.kingman@dlapiper.com](mailto:andrew.kingman@dlapiper.com)

## HB384 Testimony



February 18, 2021

The Honorable Rep. Edward Gordon  
Chairman of the New Hampshire  
House Judiciary Committee  
PO Box 112  
Bristol, NH 03222-0112

The Honorable Rep. Mark McLean  
Vice Chairman of the New Hampshire  
House Judiciary Committee  
43 Forest Hill Way  
Manchester, NH 03109-5145

The Honorable Rep. Kurt Wuelper  
Clerk of the New Hampshire  
House Judiciary Committee  
1336 Parker Mountain Road  
Strafford, NH 03884-6334

**RE: Letter in Opposition to New Hampshire HB 384**

Dear Rep. Gordon, Rep. McLean, and Rep. Wuelper:

On behalf of the advertising industry, we oppose New Hampshire HB 384,<sup>1</sup> and we offer these detailed comments summarizing our concerns about this overly restrictive legislation.

We and the companies we represent strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, legislative proposals like HB 384, that flatly prohibit legitimate transfers of specific data types, do not benefit consumers and instead stand to harm the businesses that support the economy. If enacted, HB 384 would take an approach to location data not seen in other privacy related laws or initiatives. The bill would also inadvertently harm New Hampshire consumers by depriving them of choices and access to valuable online products and services that are advertising-supported and provided for free or at a low cost. Recent surveys suggest that the average consumer benefits from a \$1,403 per year subsidy from ad-supported Internet services.<sup>2</sup> In addition, the bill includes a private right of action, which would serve to threaten innovation while creating a windfall for the plaintiff's bar without providing any real protection for consumers from privacy harms.

**To help ensure New Hampshire residents can continue to benefit from legitimate location data transfers and can continue to reap the benefits of a robust ad-supported online ecosystem, we recommend that the General Court undertake a study of the many practical and beneficial uses of consumer location data, as well as other jurisdictions' approaches to location data transfers before moving forward with enacting the overly broad restrictions set forth in HB 384.** As presently written, HB 384 falls short of creating a regulatory system that will work well for consumers or businesses.

---

<sup>1</sup> HB 384 (N.H. 2021) (hereinafter "HB 384"), located [here](#).

<sup>2</sup> Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at \$1,400/Year; Annual Value Jumps More Than \$200 Since 2016* (Sept. 28, 2020), located at <https://digitaladvertisingalliance.org/press-release/americans-value-free-ad-supported-online-services-1400year-annual-value-jumps-more-200>.

As the nation’s leading advertising and marketing trade associations, we collectively represent thousands of companies across the country, including many in New Hampshire. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend, and drives more than 80 percent of our nation’s digital advertising expenditures. We look forward to continuing to engage with the New Hampshire House Judiciary Committee (“Committee”) as it considers HB 384.

**I. HB 384’s Approach to Location Data Is Severe and Fails to Acknowledge Existing Protections for Such Data in the Marketplace**

**A. The Bill is Overly Restrictive and Would Limit Consumer Benefits and Choices**

HB 384 would unreasonably prohibit any sharing of location data to the detriment of consumers and businesses, with few exceptions.<sup>3</sup> Although the bill includes the defined term “Authorized use” that seems to suggest sharing of location data in certain instances is permissible, the defined term is neither used in the substantive provisions of the bill, nor does it provide a sufficient allowance for legitimate uses of location data that may not be tied exclusively to the purpose of providing a service explicitly requested by a consumer.<sup>4</sup>

HB 384’s approach to location data transfers is more extreme than any other state privacy law that has been enacted to date. For example, the California Consumer Privacy Act of 2018 does not ban transfers of location data; instead, it enables California consumers to opt out of sales of such information.<sup>5</sup> The California Privacy Rights Act of 2020 takes a similar approach by enabling Californians to limit the use and disclosure of precise geolocation information upon their request.<sup>6</sup> Even the General Data Protection Regulation, Europe’s omnibus privacy regulation, does not flatly ban transfers of generalized location data like HB 384 would, if enacted. The drafters of HB 384 should review their approach and more appropriately balance the privacy needs of consumers with the regime that they propose to put in place, which is overly broad.

**B. The Bill’s Prohibition Conflicts With Consumer Expectations and Deprives Consumers of the Benefits of the Data Economy**

HB 384 makes broad assumptions about what consumers want and expect from digital services, without fully taking into consideration that these vary among consumers—in general it strips consumers of choices about whether they prefer ad-supported digital products and services, or whether they would prefer to pay for them. Indeed, some customers do not have the means to pay subscription fees and would prefer these products be subsidized by data-driven advertising. It is important for legislative leaders to recognize that industry-level independent accountability already exists and has already acted many times in this area to bring companies into compliance with location standards.<sup>7</sup> By acknowledging existing privacy systems in place, HB 384’s drafters can focus resources on areas not covered elsewhere.

---

<sup>3</sup> *Id.* at Sec. 1(II)(a).

<sup>4</sup> *Id.* at Sec. 1(I)(a).

<sup>5</sup> California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.120.

<sup>6</sup> California Privacy Rights Act of 2020, Sec. 10, § 1798.121.

<sup>7</sup> Better Business Bureau, *DAAP Decisions and Guidance*, located at <https://bbbprograms.org/programs/all-programs/daap/DecisionsAndGuidance>.

Consumers have long been provided the opportunity to provide permission to location collection, use, and sharing for advertising. The major mobile platforms require consumer consent for the collection, use, and transfer of location data, effectively enabling consumers to control this on their own, and at the device or application level. Consumers have thus become accustomed to being able to exercise a choice to enable uses of location data that will benefit them and can be controlled by them. Sharing location data allows consumers to receive relevant advertisements at the right time and in the right place, and as discussed in more detail in Section III below, subsidizes the vast and varied content, products, and services they can access online.

HB 384 would take consumers' ability to exercise choice away from them, as well as all of the consumer benefits associated with location data transfers. One such benefit is the use of aggregate location data to combat the spread of COVID-19. HB 384 would restrict this beneficial, and privacy-protective use of location data by making a decision for consumers to prohibit all transfers of such data. The bill's blanket prohibition of virtually all location data transfers would therefore severely limit what consumers can experience online, regardless of their varying desires and expectations, and these critically important uses.

## **II. HB 384 Should Not Include a Private Right of Action**

HB 384 states that “[a]ny customer whose location data has been shared in violation of this chapter may bring a private action in a court of competent jurisdiction.”<sup>8</sup> We strongly believe that the responsibility for enforcing violations of privacy laws should be vested in the state alone, and HB 384 should not permit individuals to bring private lawsuits for violations. Including a private right of action in HB 384 would not adequately protect consumers from privacy harms and could have acutely detrimental effects on innovation and the state's economy.

Incorporating a private right of action in HB 384 would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions would flood New Hampshire's courts with frivolous lawsuits driven by opportunistic trial lawyers searching for technical violations, rather than focusing on actual consumer harm. Private right of action provisions are completely divorced from any connection to actual consumer harm and provide consumers little by way of protection from detrimental data practices.

Additionally, including a private right of action in HB 384 would have a chilling effect on the state's economy by creating the threat of steep penalties for companies that are good actors but inadvertently fail to conform to technical provisions of law. Private litigant enforcement provisions and related potential penalties for violations represent an overly punitive scheme that do not effectively address consumer privacy concerns or deter undesired business conduct. A private right of action would expose covered entities to extraordinary and potentially enterprise-threatening costs for technical violations of law rather than drive systemic and helpful changes to business practices. It would also encumber covered entities' attempts to innovate by threatening them with expensive litigation costs, especially if those companies are visionaries striving to develop transformative new technologies. The threat of an expensive lawsuit may force smaller companies to agree to settle claims against them even if they are convinced they are without merit.

Beyond the staggering cost to New Hampshire businesses, the resulting snarl of litigation could create a chaotic and inconsistent enforcement framework with conflicting requirements based

---

<sup>8</sup> HB 384, Sec. 1(V).

on differing court outcomes. Overall, a private right of action would serve as a windfall to the plaintiff's bar without focusing on the business practices that actually harm consumers. We therefore encourage legislators to reconsider the private right of action in HB 384. Enforcement responsibility for privacy-related legal violations should be with the state Attorney General alone. This approach would lead to strong outcomes for consumers while better enabling entities covered by the bill to allocate funds to developing processes, procedures, and plans to facilitate compliance with the new data privacy requirements.

### **III. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth**

Throughout the past three decades, the U.S. economy has been fueled by the free flow of data—including location data. One driving force in this ecosystem has been data-driven advertising. Advertising has helped power the growth of the Internet for years by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

Transfers of data over the Internet enable modern digital advertising, which subsidizes and supports the broader economy and helps to expose consumers to products, services, and offerings they want to receive. Digital advertising enables online publishers to offer content, news, services and more to consumers for free or at a low cost. In a September 2020 survey conducted by the Digital Advertising Alliance, 93 percent of consumers stated that free content was important to the overall value of the Internet and more than 80 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.<sup>9</sup>

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.<sup>10</sup> Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.<sup>11</sup>

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience.

---

<sup>9</sup> Digital Advertising Alliance, *SurveyMonkey Survey: Consumer Value of Ad Supported Services – 2020 Update* (Sept. 28, 2020), located at [https://digitaladvertisingalliance.org/sites/aboutads/files/DAA\\_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf](https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf).

<sup>10</sup> John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

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

Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the Federal Trade Commission noted in its comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.<sup>12</sup> It is in this spirit—preserving the ad supported digital and offline media marketplace while helping to design appropriate privacy safeguards—that we provide these comments.

\* \* \*

We and our members support protecting consumer privacy. We believe HB 384 takes an overly restrictive approach to location data transfers that will unnecessarily impede New Hampshire residents from receiving helpful services and accessing useful information online. We therefore respectfully ask you to reconsider the bill and instead convert it to a study so New Hampshire citizens can benefit from the General Court’s careful consideration of other approaches to location data transfers. We would also very much welcome the opportunity to further engage with Committee leaders and the bill sponsors about our industry self-regulation efforts that are continually seeking to enhance privacy protections around the collection and use of consumer location data.

Thank you in advance for consideration of this letter.

Sincerely,

Dan Jaffe  
Group EVP, Government Relations  
Association of National Advertisers  
202-269-2359

Alison Pepper  
Executive Vice President, Government Relations  
American Association of Advertising Agencies, 4A's  
202-355-4564

Christopher Oswald  
SVP, Government Relations  
Association of National Advertisers  
202-269-2359

David Grimaldi  
Executive Vice President, Public Policy  
Interactive Advertising Bureau  
202-800-0771

David LeDuc  
Vice President, Public Policy  
Network Advertising Initiative  
703-220-5943

Clark Rector  
Executive VP-Government Affairs  
American Advertising Federation  
202-898-0089

---

<sup>12</sup> Federal Trade Commission, *In re Developing the Administration’s Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at [https://www.ftc.gov/system/files/documents/advocacy\\_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400\\_ftc\\_comment\\_to\\_ntia\\_112018.pdf](https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf).



*New England Cable & Telecommunications Association, Inc.*  
*The Enterprise Center • 121 Loring Avenue • Suite 340 • Salem, MA 01970*  
*Tel: 781.843.3418*

*New England Cable & Telecommunications Association, Inc.*

**Statement of the New England Cable & Telecommunications Association, Inc. regarding House bill 384  
AN ACT relative to limiting robocalls by automatic dialing devices.**

**February 19, 2021**

The New England Cable & Telecommunications Association (NECTA) is a five-state regional trade association representing substantially all private cable telecommunications companies in New Hampshire. Our members, including Atlantic Broadband, Charter and Comcast, are New Hampshire's leading broadband and communications providers with over 450,000 customers in more than 184 communities.

NECTA members take customer privacy very seriously and work hard to protect the privacy of New Hampshire residents; however, companies also need the ability operate in accordance with the law while providing the services that consumers expect and rely on. NECTA supports well-thought out, narrowly defined geolocation policy designed to solve a specific issue and to not hamper innovation and new technologies. Respectfully, NECTA opposes HB384 because it does not accomplish these goals, is unnecessary, and exposes companies to private rights of action, which incentivizes frivolous lawsuits for minor or unknown infractions.

House bill 384 is too broad in its wording, which could result in hindering consumer experiences and disrupting many harmless conveniences that users have come to expect online. For example, geolocation data is vital to the functioning of many apps, allowing them to tailor content to the user's location. This bill's language is unclear as to what constitutes a service explicitly requested by a consumer. The bill's language is ambiguous as to whether such use is limited to the primary purpose of a mobile application, such as navigation software needing a user's location to provide data, or does the explicit consumer request also apply to secondary uses, such as tracking a user's speed while driving to the desired location?

Furthermore, operating systems and applications are increasingly giving consumers more granular and real-time controls over what type of data is shared and how often. Users can control geolocation sharing on most devices allowing them to decide how location data is shared upon downloading of an app or later in a device's settings. This bill does not account for the expectations that consumers have of certain services being provided, which this bill would make difficult if not impossible to provide. Geolocation data is used to authenticate streaming video and live streaming television as one example. Other common popular consumer benefits include knowing whether it will rain from a weather app, getting directions to a favorite restaurant or tracking steps or a jogging route for exercise purposes. If companies could not share this data, the user experience would be significantly altered or interrupted.

House bill 384 also does not make any distinction between aggregated/anonymized data and personally identifiable information (PII). Usually, companies are not actually sharing an individual's specific data, but anonymized datasets. The sharing of anonymized data underpins much of the modern Internet, and when there is proper anonymization, individuals face no risk of privacy breach. Both the European Union's General Data Protection Regulation and the California Consumer Privacy Act understand this distinction and establish separate rules for anonymized data. Anonymized data is used to improve traffic safety and flow by measuring traffic counts and patterns, speed, and traffic violations to name a few. Wireless providers use anonymized data



to determine network capacity and coverage needs. Consumer usage patterns help determine where improvements and capital investment in wireless facilities is needed. Excluding anonymized data sharing from the definition of authorized use would impact thousands of geolocation-based business models including valuable services like ridesharing, education, tourism, urban planning and telework applications. That would impact a multitude of valuable and widely used services including “find my device” features and most applications involving photographs, free public Wi-Fi and mapping/navigation services. In short, the consequences of this bill could be severely detrimental.

HB384 is unnecessary because geolocation information is already protected. The Federal Trade Commission’s privacy framework classifies precise geolocation as sensitive personal data, and companies must get opt-in consent prior to using or disclosing this information. The FTC has brought enforcement actions against companies that have misrepresented consumer control regarding collection and use of geolocation data. Federal law and regulations also generally require telecommunications carriers to obtain opt-in consent prior to sharing mobile call location information.

Not only unnecessary, HB384 could also hinder a company’s ability to combat fraud and misuse. Using AI, location data is used to identify fraudulent transactions. For instance, if a consumer logs into her online account from England, but her cell phone location data shows that she is in Manchester, an alarm goes off to alert of possible fraud. However, if that same consumer’s phone shows she is in England, that is a sign of a traveler. If a primary driver behind this bill is to prevent criminals from accessing a user’s location data, the criminal code is better positioned to address this issue than a blanket prohibition against sharing this data. Interestingly, this bill does not provide any authority to the Attorney General to investigate.

NECTA also opposes the inclusion of a private right of action that will allow individuals to sue a company if they feel their data has been shared in violation of this bill. This unspecific wording would encourage frivolous lawsuits exposing companies to untold amounts of litigation and could significantly hamper companies’ ability to operate even if they are making good faith efforts to comply.

This type of legislation is best left to Congress to prevent a patchwork of laws among states that will make it more difficult to do business across state lines. Congress should establish uniform privacy rules that offer consumers a greater sense of security and enhance consumer confidence.

Thank you for your time and consideration of these comments. Please do not hesitate to contact me with any questions.

Sincerely,

---

Timothy Wilkerson  
President, NECTA



*New England Cable & Telecommunications Association, Inc.*  
*The Enterprise Center • 121 Loring Avenue • Suite 340 • Salem, MA 01970*  
*Tel: 781.843.3418*

*New England Cable & Telecommunications Association, Inc.*

**Statement of the New England Cable & Telecommunications Association, Inc. regarding House bill 384  
AN ACT relative to limiting robocalls by automatic dialing devices.**

**February 19, 2021**

The New England Cable & Telecommunications Association (NECTA) is a five-state regional trade association representing substantially all private cable telecommunications companies in New Hampshire. Our members, including Atlantic Broadband, Charter and Comcast, are New Hampshire's leading broadband and communications providers with over 450,000 customers in more than 184 communities.

NECTA members take customer privacy very seriously and work hard to protect the privacy of New Hampshire residents; however, companies also need the ability operate in accordance with the law while providing the services that consumers expect and rely on. NECTA supports well-thought out, narrowly defined geolocation policy designed to solve a specific issue and to not hamper innovation and new technologies. Respectfully, NECTA opposes HB384 because it does not accomplish these goals, is unnecessary, and exposes companies to private rights of action, which incentivizes frivolous lawsuits for minor or unknown infractions.

House bill 384 is too broad in its wording, which could result in hindering consumer experiences and disrupting many harmless conveniences that users have come to expect online. For example, geolocation data is vital to the functioning of many apps, allowing them to tailor content to the user's location. This bill's language is unclear as to what constitutes a service explicitly requested by a consumer. The bill's language is ambiguous as to whether such use is limited to the primary purpose of a mobile application, such as navigation software needing a user's location to provide data, or does the explicit consumer request also apply to secondary uses, such as tracking a user's speed while driving to the desired location?

Furthermore, operating systems and applications are increasingly giving consumers more granular and real-time controls over what type of data is shared and how often. Users can control geolocation sharing on most devices allowing them to decide how location data is shared upon downloading of an app or later in a device's settings. This bill does not account for the expectations that consumers have of certain services being provided, which this bill would make difficult if not impossible to provide. Geolocation data is used to authenticate streaming video and live streaming television as one example. Other common popular consumer benefits include knowing whether it will rain from a weather app, getting directions to a favorite restaurant or tracking steps or a jogging route for exercise purposes. If companies could not share this data, the user experience would be significantly altered or interrupted.

House bill 384 also does not make any distinction between aggregated/anonymized data and personally identifiable information (PII). Usually, companies are not actually sharing an individual's specific data, but anonymized datasets. The sharing of anonymized data underpins much of the modern Internet, and when there is proper anonymization, individuals face no risk of privacy breach. Both the European Union's General Data Protection Regulation and the California Consumer Privacy Act understand this distinction and establish separate rules for anonymized data. Anonymized data is used to improve traffic safety and flow by measuring traffic counts and patterns, speed, and traffic violations to name a few. Wireless providers use anonymized data

to determine network capacity and coverage needs. Consumer usage patterns help determine where improvements and capital investment in wireless facilities is needed. Excluding anonymized data sharing from the definition of authorized use would impact thousands of geolocation-based business models including valuable services like ridesharing, education, tourism, urban planning and telework applications. That would impact a multitude of valuable and widely used services including “find my device” features and most applications involving photographs, free public Wi-Fi and mapping/navigation services. In short, the consequences of this bill could be severely detrimental.

HB384 is unnecessary because geolocation information is already protected. The Federal Trade Commission’s privacy framework classifies precise geolocation as sensitive personal data, and companies must get opt-in consent prior to using or disclosing this information. The FTC has brought enforcement actions against companies that have misrepresented consumer control regarding collection and use of geolocation data. Federal law and regulations also generally require telecommunications carriers to obtain opt-in consent prior to sharing mobile call location information.

Not only unnecessary, HB384 could also hinder a company’s ability to combat fraud and misuse. Using AI, location data is used to identify fraudulent transactions. For instance, if a consumer logs into her online account from England, but her cell phone location data shows that she is in Manchester, an alarm goes off to alert of possible fraud. However, if that same consumer’s phone shows she is in England, that is a sign of a traveler. If a primary driver behind this bill is to prevent criminals from accessing a user’s location data, the criminal code is better positioned to address this issue than a blanket prohibition against sharing this data. Interestingly, this bill does not provide any authority to the Attorney General to investigate.

NECTA also opposes the inclusion of a private right of action that will allow individuals to sue a company if they feel their data has been shared in violation of this bill. This unspecific wording would encourage frivolous lawsuits exposing companies to untold amounts of litigation and could significantly hamper companies’ ability to operate even if they are making good faith efforts to comply.

This type of legislation is best left to Congress to prevent a patchwork of laws among states that will make it more difficult to do business across state lines. Congress should establish uniform privacy rules that offer consumers a greater sense of security and enhance consumer confidence.

Thank you for your time and consideration of these comments. Please do not hesitate to contact me with any questions.

Sincerely,

---

Timothy Wilkerson  
President, NECTA

Subject: Testimony FOR HB384: location privacy

Dear Hon. House Judiciary members,

This is my written testimony IN SUPPORT of HB384, Location Privacy, to accompany my oral testimony at the hearing on Feb 19.

### **Executive Summary**

Cellphone companies, apps, and perhaps car manufacturers are exploiting the trust of their customers by selling those customers' live location to other companies that then sell it again (and so forth), to the point where the original companies have no idea who is using it and little to no protections are in place for the privacy of those customers. This is in violation of those customers' expectations of privacy and with no informed consent, since companies go out of their way to hide this practice. When these practices came to light, the companies said they would stop. They didn't.

The availability of this information could lead to real harm for individuals, not just in their loss of privacy but also because stalkers, burglars, and insurance companies can purchase the info from any of the many resellers. Due to a security flaw at one of them, anyone in the world could anonymously find the location of any US phone just by having its number. Documented victims so far include a judge and state police officers.

Because all of the major cellphone companies engage in this practice, legislation is needed to protect the privacy of NH citizens. HB384 accomplishes this by only allowing location information to be shared in the way expected by the customer: as part of fulfilling their request or providing them service. We cannot afford to wait for the federal govt, which, at the behest of Telecommunications Industry lobbyists, already rolled back the few privacy protections that were in place.

### **Who am I**

My name is Jason Hennessey; a resident of Amherst, NH. I have extensive experience with modern computing technologies, working in the technology industry for over 15 years. I also have a BS in Computer Science from Rivier University (Nashua, NH), a PhD in Computational Sciences and Statistics from South Dakota State University and completed 4 years of postdoctoral studies in Computer Science at Boston University where I co-taught a course in Computer Security.

I have published several peer-reviewed scientific papers covering topics in privacy, security and computing systems in widely respected venues<sup>1</sup>.

### **Collection of private location information is pervasive**

Many do not realize that at least as of 2 years ago, all of the major cellphone companies in the US are constantly collecting and selling their customers' location information to networks of resellers, often with little or no controls in place or even the ability to track who the information was sold to. For example, T-Mobile sold it to 80 companies<sup>2</sup>. This became public in 2018 when a county sheriff was found to be tracking a judge and state police officers<sup>3</sup>. Cellphone providers committed to ending the practice, though several months later, they hadn't<sup>4</sup>.

On top of that, many mobile apps on Smart Phones sell the location of their users. One investigation found 70 companies to whom a set of popular apps were directly uploading exact location information; one weather app sent its users' locations to 40 companies by itself<sup>5</sup>! Many cars with infotainment or navigation systems can also track location.

After this location information is uploaded to exchanges, it's unclear who can access it.

### **Privacy issues with location information**

The Supreme Court has said that the location data cell-phone providers keep "provides an intimate window into a person's life, revealing not only their particular movements but through them his familial, political, professional, religious, and sexual associations."<sup>6</sup>

On top of general privacy concerns, the unregulated marketplace for personal location data could be exploited by stalkers, burglars, insurance companies, and other entities to directly harm individuals.

On top of that, the fact that almost everyone is being tracked simultaneously could be used to determine who a person's private associates were.

We have no idea who is buying this information; as far as we know it's available on the open market. These companies may or may not have any filtering or protections in place. An NY Times article<sup>7</sup> discusses how one of these location resellers that targeted law enforcement (Securus) performed no verification that requests were lawful.

A bug in one of the location sharing contractors, LocationSmart allowed anyone on the Internet to track anyone else in realtime with just a phone number anonymously.<sup>8</sup> This was discovered by a university student in his spare time; imagine what someone dedicated could do.

### **Lack of informed consent**

NH residents making use of cellphones, apps and cars generally have an expectation of privacy that is being violated by these location sharing practices. Perhaps this is why the companies that engage in them obscure these practices through long privacy policies (Verizon: 22 pages, AT&T: 27) that do not explicitly mention the sale of location information. I have not been able to find a way for customers to opt out of this selling of location, despite searching for it.

### **This legislation is a good answer**

HB384 limits the sharing of location when not being used to benefit the person. This reflects most people's expectation and addresses the exploitation of NH citizens.

In 2020, NH Senate Judiciary recommended OTP on an almost identical bill, SB732, however due to COVID the bill did not move further.

### **NH cannot wait for federal legislation**

Telecom lobbyists will say that we should wait for Federal legislation, however they successfully fought efforts to do just that in 2017 when they were able to have the privacy protections that included location information repealed<sup>9</sup>, aided by over \$123m spent on federal lobbying in just 2016<sup>10</sup>. NH

citizens deserve protection against this exploitation now. Other states like Maine and California have enacted extensive privacy protections for their residents.

### **Addressing concerns**

**Uber/Lyft:** One concern raised by a lobbyist during the public hearing was that companies like Uber wouldn't be able to share location information about customers with their drivers. This doesn't agree with HB384's definition of *Authorized Use*, since the sharing of this information would be to provide the service the customer requested.

**Cookies:** Another concern raised by a lobbyist is that this bill could create problems for free apps that use computer "cookies". Because cookies are set by a server on the client, which later returns that cookie to the server, it is not clear how they could be impacted by this legislation.

**Annoying opt-ins:** Another concern raised was that HB384 would require those entering NH to have to consent to their location being shared, despite the person being unaware of this law. One person went so far as to raise the case of someone from NH who commutes to Massachusetts needing to consent each time they crossed the border. This is unfounded.

These concerns convey an entitlement that these companies feel they have to exploit their unsuspecting customers' location information. No consent is needed if a person's location information is only being shared to fulfill their request or isn't being shared with third parties at all.

### **Summary**

The only commerce HB384 will substantially affect is the sale of the private location information of NH citizens, many times without their informed consent.

HB384 protects the physical well being of NH citizens against criminals who might exploit this information to rob, stalk or otherwise harm them by purchasing their realtime location from any of the myriad, unregulated companies that trade in this information.

Respectfully Submitted,  
Jason Hennessey representing myself, a concerned citizen.  
Amherst, NH

- 1 Jason's publications can be found on Google Scholar: [https://scholar.google.com/scholar?hl=en&as\\_sdt=0%2C30&q=author%3A%22Jason+Hennessey%22](https://scholar.google.com/scholar?hl=en&as_sdt=0%2C30&q=author%3A%22Jason+Hennessey%22)
- 2 Cellphone Carriers Face \$200 Million Fine for Not Protecting Location Data. NY Times, 2020. <https://www.nytimes.com/2020/02/28/technology/fcc-cellphones-location-data-fines.html>
- 3 Service Meant to Monitor Inmates' Calls Could Track You, Too. NY Times, 2018. <https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html>
- 4 Carriers Swore They'd Stop Selling Location Data. Will They Ever? Wired, 2019. <https://www.wired.com/story/carriers-sell-location-data-third-parties-privacy/>
- 5 Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. NY Times, 2019. <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>
- 6 CARPENTER v. UNITED STATES. US Supreme Court Opinion, 2017. [https://www.supremecourt.gov/opinions/17pdf/16-402\\_h315.pdf](https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf)
- 7 Service Meant to Monitor Inmates' Calls Could Track You, Too. NY Times, 2018. <https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html>
- 8 A Security Flaw in a Free Web Service Let Anyone Anonymously Track U.S. Cell Phones. Fortune, 2018. <https://fortune.com/2018/05/19/locationsmart-hacker-track-cell-phones/>
- 9 U.S. Senate votes to overturn Obama broadband privacy rules. Reuters, 2017. <https://www.reuters.com/article/usa-internet-idINKBN16U2IC>
- 10 INFLUENCE GAME: Telecom lobbying muscle kills privacy rules. AP News, 2017. <https://apnews.com/article/22f858a75c4e4d408b970cfe28c72bbe>

Bill as  
Introduced



HB 384-FN - AS INTRODUCED

2021 SESSION

21-0478  
04/10

HOUSE BILL **384-FN**

AN ACT prohibiting the sharing of location data.

SPONSORS: Rep. Wuelper, Straf. 3; Rep. M. Smith, Straf. 6; Rep. Verville, Rock. 2; Rep. Gould, Hills. 7; Rep. T. Lekas, Hills. 37; Rep. Wallace, Rock. 12; Rep. Testerman, Merr. 2

COMMITTEE: Judiciary

ANALYSIS

This bill prohibits the sharing of location data by a mobile application developer, telecommunications carrier, or other person.

Explanation: Matter added to current law appears in **bold italics**.  
Matter removed from current law appears [~~in brackets and struck through~~].  
Matter which is either (a) all new or (b) repealed and reenacted appears in regular type.

21-0478  
04/10

STATE OF NEW HAMPSHIRE

*In the Year of Our Lord Two Thousand Twenty One*

AN ACT prohibiting the sharing of location data.

*Be it Enacted by the Senate and House of Representatives in General Court convened:*

1 New Section; Wiretapping and Eavesdropping; Sharing Location Data Prohibited. Amend RSA 570-A by inserting after section 2-a the following new section:

570-A:2-b Sharing Location Data Prohibited.

I. In this section:

(a)(1) "Authorized use" means the sharing of a customer's location data:

(A) For the purpose of providing a service explicitly requested by such customer;

(B) Exclusively for the purpose of providing a service explicitly requested by such customer; and

(C) Where such data is not collected, shared, stored, or otherwise used by a third party for any purpose other than providing a service explicitly requested by such customer.

(2) "Authorized use" shall not include any instance in which a customer's location data is shared in exchange for products or services.

(b) "Customer" means a current or former subscriber to a telecommunications carrier or a current or former user of a mobile application.

(c) "Location data" means information related to the physical or geographical location of a person or the person's mobile communications device, regardless of the particular technological method used to obtain this information.

(d) "Mobile application" means a software program that runs on the operating system of a mobile communications device.

(e) "Mobile application developer" means a person that owns, operates, or maintains a mobile application and makes such application available for the use of customers for a fee or otherwise.

(f) "Mobile communications device" means any portable wireless telecommunications equipment that is utilized for the transmission or reception of data, including location data, and that is or may be commonly carried by or on a person or commonly travels with a person, including in or as part of a vehicle a person drives.

(g) "Share" means to make location data available to another person, for a fee or otherwise.

(h) "Telecommunications carrier" means a service offered to the public for a fee that transmits sounds, images, or data through wireless telecommunications technology.

II.(a) No mobile application developer or a telecommunications carrier shall share a customer's location data where such location data was collected while the customer's mobile communications device were physically present in the town or city.

(b) No person who receives location data that is shared in violation of subparagraph (a) shall share such data with another person.

III. A mobile application developer, telecommunications carrier, or other person who shares a customer's location data with another person in a manner prohibited by this section shall be guilty of a violation and subject to a fine of \$1,000. A mobile application developer, telecommunications carrier, or other person who is convicted of multiple violations of this section shall be subject to a maximum fine \$10,000 for each person whose location data was shared in violation of this section.

IV. This section shall not apply to:

(a) Information provided to a law enforcement agency in response to a lawful process;

(b) Information provided to an emergency service agency responding to an emergency communication or any other communication reporting an imminent threat to life or property;

(c) Information required to be provided by a federal, state, or local law enforcement agency; or

(d) A customer providing the customer's own location data to a mobile application.

V. Any customer whose location data has been shared in violation of this chapter may bring a private action in a court of competent jurisdiction. If a court of competent jurisdiction finds that a person has violated a provision of this section, the court may award actual damages and reasonable attorney's fees and costs incurred in maintaining such civil action.

2 Effective Date. This act shall take effect 60 days after its passage.

LBA  
21-0478  
12/10/20

**HB 384-FN- FISCAL NOTE  
AS INTRODUCED**

AN ACT prohibiting the sharing of location data.

**FISCAL IMPACT:**     State                     County                     Local                     None

STATE:	Estimated Increase / (Decrease)			
	FY 2021	FY 2022	FY 2023	FY 2024
<b>Appropriation</b>	\$0	\$0	\$0	\$0
<b>Revenue</b>	\$0	Indeterminable Increase	Indeterminable Increase	Indeterminable Increase
<b>Expenditures</b>	\$0	Indeterminable Increase	Indeterminable Increase	Indeterminable Increase
<b>Funding Source:</b>	<input checked="" type="checkbox"/> General Assessment Revenue <input type="checkbox"/> Education <input type="checkbox"/> Highway <input checked="" type="checkbox"/> Other - Penalty			

**METHODOLOGY:**

This bill prohibits the sharing of data by a mobile application developer, telecommunications carrier, or other person. The Judicial Branch indicates the potential fiscal impact to the Branch from this bill is in the filing of additional violation offenses and civil actions for damages, costs and attorneys' fees. The Branch does not have information on the number of additional violation level offenses that will result from the proposed bill and is unable to anticipate the additional costs or the amount of fine revenue that will be collected. Regarding private actions for sharing location data in violation of proposed RSA 570-A:2-b, including claims for damages, costs and reasonable attorneys' fees, such cases would likely be classified as complex civil cases in the superior court. The Branch has no information on which to estimate how many new complex civil cases will be brought because of the proposed bill. The estimated average cost to Branch for both types of cases follows:

Judicial Branch	FY 2021	FY 2022
Violation Level Offense	\$53	\$53
Complex Civil Case	\$794	\$794
Appeals	Varies	Varies

It should be noted that these average case cost estimates are based on data that is more than ten years old and does not reflect changes to the courts over that same period of time or the impact these changes may have on processing the various case types. The Judicial Branch received an appropriation in the operating budget to update its cost data in 2020, but due to the COVID state of emergency, this analysis has been delayed.

It is assumed any fiscal impact would occur after July 1, 2021.

**AGENCIES CONTACTED:**

Judicial Branch