Committee Report

REGULAR CALENDAR

October 29, 2020

HOUSE OF REPRESENTATIVES

REPORT OF COMMITTEE

The Committee on Commerce and Consumer Affairs to which was referred HB 1680-FN,

AN ACT relative to the collection of personal information by businesses. Having considered the same, report the same: RECOMMENDED FOR FUTURE LEGISLATION.

Rep. Greg Indruk

FOR THE COMMITTEE

Original: House Clerk
Cc: Committee Bill File

COMMITTEE REPORT

Committee:	**Commerce and Consumer Affairs**
Bill Number:	**HB 1680-FN**
Title:	**relative to the collection of personal information by businesses.**
Date:	**October 29, 2020**
Consent Calendar:	**REGULAR**
Recommendation:	**RECOMMENDED FOR FUTURE LEGISLATION**

STATEMENT OF INTENT

In 2018, over 80% of Granite State voters moved to add a Right to Privacy to the New Hampshire State Constitution. This bill seeks to similarly protect NH consumers in certain commercial transactions. While the bill and proposed amendment explore alternative ways to do so, they share at least two common goals; requiring disclosure of personal data collection and sale practices by covered businesses and empowering NH consumers to exercise control over the sale of their personal data to third parties and beyond. Such personal data can be used to discriminate against, conduct warrantless investigations, track, defraud, influence, and embarrass. Many other states and jurisdictions have already acted on this issue. The bipartisan majority believes it is incumbent upon this legislature to find a way to put control of personal data in the hands of NH consumers.

Vote 10-5.

Rep. Greg Indruk
FOR THE COMMITTEE

Original: House Clerk
Cc: Committee Bill File

REGULAR CALENDAR

Commerce and Consumer Affairs

HB 1680-FN, relative to the collection of personal information by businesses.**RECOMMENDED FOR FUTURE LEGISLATION .**

Rep. Greg Indruk for Commerce and Consumer Affairs. In 2018, over 80% of Granite State voters moved to add a Right to Privacy to the New Hampshire State Constitution. This bill seeks to similarly protect NH consumers in certain commercial transactions. While the bill and proposed amendment explore alternative ways to do so, they share at least two common goals; requiring disclosure of personal data collection and sale practices by covered businesses and empowering NH consumers to exercise control over the sale of their personal data to third parties and beyond. Such personal data can be used to discriminate against, conduct warrantless investigations, track, defraud, influence, and embarrass. Many other states and jurisdictions have already acted on this issue. The bipartisan majority believes it is incumbent upon this legislature to find a way to put control of personal data in the hands of NH consumers. **Vote 10-5.**

Original: House Clerk
Cc: Committee Bill File

1. HB 1581, relative to the labeling and sale of hemp products containing CBD.
   Recommended: 8-7; Van Houten

   OK to publish -- EAB

The bill is a public health bill which, in the absence of FDA regulations, seeks to provide labeling guidance for such products for consumer protection. There are 15 states where CBD is legal if labeling requirements are followed. The majority believes that legislation like this bill, in the interest of consumer knowledge & safety, needs to be pursued further.

2. HB 1588, establishing a mortgage mediation procedure.
   Recommended; Williams, 9-6

   OK to publish -- EAB

This bill would mandate a mortgage mediation process for mortgages moving into foreclosure. There have been, and certainly could be again, bad actors in the mortgage industry. And as we know our economy is cyclical with boom and bust periods. This bill is intended to help consumers who are negatively impacted if an economic slowdown threatens their ability to hold on to their home. However, many local and national banks already have proactive programs to help consumers experiencing challenges with paying their mortgage. The Fannie Mae and Freddie Mac federal programs, often financed through local banks, also have programs for people struggling with paying their mortgages. This consumer protection bill needs more work in order to fit into the network of protections for mortgage holders.

3. HB 1680, relative to the collection of personal information by businesses.
   Recommended; Indruk, 10-5

   OK to publish -- EAB

In 2018 over 80% of Granite State voters moved to add a Right to Privacy to the New Hampshire State Constitution. This bill seeks to similarly protect NH consumers in certain commercial transactions. While the bill and subsequent amendment explore alternative ways to do so, they share at least two common goas; requiring disclosure of personal data collection and sale practices by covered businesses and empowering NH consumers to exercise control over the sale of their personal data to third parties and beyond. Such personal data can be used to discriminate against, conduct warrantless investigations, track, defraud, influence, and embarrass. Many other states and jurisdictions have already acted on this issue. The bipartisan majority believes it is incumbent upon this legislature to find a way to put control of personal data in the hands of NH consumers.

4. HB 1690, prohibiting paper billing fees.
   Recommended; Butler, 9-6

   OK to publish -- EAB

The majority recognizes the inequity of charging for paper versions of bills for consumers who don't have online access, are uncomfortable using the internet, or want a paper version for archiving. However, the bill would have had limited effectiveness in preventing those fees, especially with the entities that fall outside of the Consumer Protection Act.

Voting Sheets

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

EXECUTIVE SESSION on HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: September 2, 2020

LOB ROOM: Remote Meeting

MOTION:

Interim Study (2nd yr) Recommended for Future Legislation

Moved by Rep. Indruk Seconded by Rep. Butler Vote: 10-5

Respectfully submitted,

Rep Joyce Weston, Clerk

HOUSE COMMITTEE ON

EXECUTIVE SESSION on

BILL TITLE: HB 1680-FN collection of personal information by businesses.

DATE: 9-2-20

LOB ROOM: Remote

MOTION: ☑ Recommended for Future Legislation

☐ Not Recommended for Future Legislation

Moved by Rep. Indruk Seconded by Rep. Butler Vote: 10-5

Respectfully submitted,

Rep. Joyce C. Weston
Committee Clerk

STATE OF NEW HAMPSHIRE
OFFICE OF THE HOUSE CLERK

8/27/2020 1:04:23 PM
Roll Call Committee Registers Report

2020 SESSION

Commerce and Consumer Affairs

Bill #: HB1680-FN Motion: Recommended AM #: _____ Exec Session Date: 9-2-20

Members	YEAS	Nays	NV
Butler, Edward A. Chairman	✓		
Williams, Kermit R. Vice Chairman	✓		
Gidge, Kenneth N.			✓
Abel, Richard M.	✓		
Bartlett, Christy D.	✓		
Herbert, Christopher J.			✓
McBeath, Rebecca Susan	✓		
Van Houten, Constance	✓		
Fargo, Kristina M.	✓		
Indruk, Greg L.	✓		
Weston, Joyce	✓		
Hunt, John B.		✓	
Sanborn, Laurie J.			✓
Osborne, Jason M.		✓	
Plumer, John R.		✓	
Barnes, Arthur E.	✓		
Potucek, John M.		✓	
Warden, Mark		✓	
TOTAL VOTE:	10	5	3

Sub-Committee Minutes

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

SUBCOMMITTEE WORK SESSION on HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: September 2, 2020

Subcommittee Members: Reps. Butler, Williams, Abel, Bartlett, McBeath, Van Houten, Fargo, Indruk, Weston, Hunt, J. Osborne, Plumer, Barnes, Potucek and Warden

Comments and Recommendations: Rep. Indruk - based on CA bill; amended to take smaller bite - opt-in for sale of information.

Respectfully submitted,

Rep. Joyce Weston
Subcommittee Clerk

HOUSE COMMITTEE ON

~~SUB~~COMMITTEE WORK SESSION on

BILL TITLE: HB 1680-FN relative to the collection of personal information by businesses.

DATE: 9-2-20

Subcommittee Members: Butler, Williams, Abel, Bartlett, McBeath, Van Houten, Fargo, Andrick, Weston, Hunt, Osborne, Plumer Barnes, Potucek, Warden

Comments and Recommendations:

Andrick - based on CA bill; amended to take smaller bite - opt-in for sale of info.

The full-committee work session was directly followed by the Executive Session vote.

Respectfully submitted,

Rep. Vogel C. Weston
Subcommittee Chairman/Clerk

Committee Report

CONSENT CALENDAR

March 4, 2020

HOUSE OF REPRESENTATIVES

REPORT OF COMMITTEE

The Committee on Commerce and Consumer Affairs to which was referred HB 1680-FN,

AN ACT relative to the collection of personal information by businesses. Having considered the same, report the same with the recommendation that the bill be REFERRED FOR INTERIM STUDY.

Rep. Kermit Williams

FOR THE COMMITTEE

Original: House Clerk
Cc: Committee Bill File

COMMITTEE REPORT

Committee:	Commerce and Consumer Affairs
Bill Number:	HB 1680-FN
Title:	relative to the collection of personal information by businesses.
Date:	March 4, 2020
Consent Calendar:	CONSENT
Recommendation:	REFER FOR INTERIM STUDY

STATEMENT OF INTENT

While the committee recognizes an ever-increasing concern about online privacy among our constituents, we felt that this bill would not be an effective tool to provide that privacy. An amendment was offered that would only apply to Internet Service Providers, or ISPs. ISPs provide internet access to customers, but the websites those customers access are the most likely entities to monetize that customer's personal information. Some companies that operate ISPs may offer websites or other businesses as well as internet access, but those businesses are normally separated in both access and corporate structure. The committee believes that more work needs to be done to find an effective solution for data privacy, and the solution may make more sense at a federal level since very little of the data privacy problem happens within New Hampshire's borders.

Vote 18-1.

Rep. Kermit Williams
FOR THE COMMITTEE

Original: House Clerk
Cc: Committee Bill File

CONSENT CALENDAR

Commerce and Consumer Affairs

HB 1680-FN, relative to the collection of personal information by businesses. REFER FOR **INTERIM STUDY.**

Rep. Kermit Williams for Commerce and Consumer Affairs. While the committee recognizes an ever-increasing concern about online privacy among our constituents, we felt that this bill would not be an effective tool to provide that privacy. An amendment was offered that would only apply to Internet Service Providers, or ISPs. ISPs provide internet access to customers, but the websites those customers access are the most likely entities to monetize that customer's personal information. Some companies that operate ISPs may offer websites or other businesses as well as internet access, but those businesses are normally separated in both access and corporate structure. The committee believes that more work needs to be done to find an effective solution for data privacy, and the solution may make more sense at a federal level, since very little of the data privacy problem happens within New Hampshire's borders. **Vote 18-1.**

Original: House Clerk
Cc: Committee Bill File

Rep Kermit Williams for Commerce. Per- and polyfluoroalkyl compounds, or PFAs, are substances found in many manufactured products from nonstick pans to clothing to firefighting foam. They are best known in New Hampshire for the contamination of groundwater that has infiltrated wells and municipal water systems, but there are other areas where PFAS contamination is an issue, including sewage treatment. This bill would create a committee to study how New Hampshire could require disclosure of PFAS content in products sold in the state, so consumers and businesses could be aware of the presence of potentially harmful material. Vote 12-8.

HB 1471, prohibiting banks from re-ordering transactions to increase overdraft fees. INEXPEDIENT TO LEGISLATE.

Rep Kermit Williams for Commerce. While this issue has been raised over the years as a potential problem for banking customers, the committee heard that most banks have their own rules prohibiting this practice, and other regulators such as the Consumer Financial Protection Bureau have policies about overdraft fees as well. The legislation would only apply to state-chartered banks and credit unions; many of the largest institutions popular with consumers are federally-chartered, so would be exempt from this legislation. Most banks will refund an occasional overdraft fee if the customer requests it. Vote 18-2.

HB 1482, relative to notification of security breaches. OUGHT TO PASS.

Rep Kermit Williams for Commerce. This bill requires immediate disclosure of a security breach to anyone affected. Under current law, disclosure can be delayed while an investigation takes place. The committee felt time is of the essence for consumers and others to change or cancel credit cards, reset passwords, or take other action after their information has been compromised. After notice has been given, additional details can be withheld to protect an investigation. Vote 19-1.

HB 1535, relative to installation of solar photovoltaic energy systems by condominium unit owners and owners subject to deed restrictions in a homeowners association. OUGHT TO PASS WITH AMENDMENT.

Rep Kermit Williams for Commerce. This bill, as amended, allows homeowners who have a suitable place for solar panels that is entirely under their control, owned by them and not part of shared infrastructure or common property, to be used to install a solar energy system. The committee felt that use of shared roofs or common land is a complex problem that should be decided by a condominium association, not state law. Vote 12-8.

HB 1680, relative to the collection of personal information by businesses. INTERIM STUDY.

Rep Kermit Williams for Commerce. While the committee recognizes an ever-increasing concern about online privacy among our constituents, we felt that this bill would not be an effective tool to provide that privacy. As amended, the bill would only apply to Internet Service Providers, or ISPs. ISPs provide internet access to customers, but the websites those customers access are the most likely entities to monetize that customer's personal information. Some companies that operate ISPs may offer websites or other businesses as well as internet access, but those businesses are normally separated in both access and corporate structure. The committee believes that more work needs to be done to find an

Voting Sheets

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

EXECUTIVE SESSION on HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: March 4, 2020

LOB ROOM: 302

MOTIONS: **REFER FOR INTERIM STUDY**

Moved by Rep. Williams Seconded by Rep. Hunt Vote: 18-1

CONSENT CALENDAR: YES

Statement of Intent: Refer to Committee Report

Respectfully submitted.

Rep Van Houten, Acting Clerk

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

EXECUTIVE SESSION on HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: 3/3/2020

LOB ROOM: 302

MOTION: (Please check one box)

☐ OTP ☐ ITL ☐ Retain (1st year) ☒ Adoption of Amendment # 2019-0560h (Ignore)

☐ Interim Study (2nd year) *(if offered)*

Moved by Rep. Indrisek Seconded by Rep. Muscatel Vote: 7-12

MOTION: (Please check one box)

☐ OTP ☐ OTP/A ☐ ITL ☐ Retain (1st year) ☐ Adoption of Amendment # _____

☒ Interim Study (2nd year) *(if offered)*

Moved by Rep. Williams Seconded by Rep. Hunt Vote: 18-1

MOTION: (Please check one box)

☐ OTP ☐ OTP/A ☐ ITL ☐ Retain (1st year) ☐ Adoption of Amendment # _____

☐ Interim Study (2nd year) *(if offered)*

Moved by Rep. _____ Seconded by Rep. _____ Vote: _____

MOTION: (Please check one box)

☐ OTP ☐ OTP/A ☐ ITL ☐ Retain (1st year) ☐ Adoption of Amendment # _____

☐ Interim Study (2nd year) *(if offered)*

Moved by Rep. _____ Seconded by Rep. _____ Vote: _____

CONSENT CALENDAR: ✓ **YES** ____ **NO**

Minority Report? _____ Yes _____ No If yes, author, Rep: _____ Motion_____

Respectfully submitted: Dan Hoxie

~~Rep Rebecca McBeath,~~ Clerk

OFFICE OF THE HOUSE CLERK

2/3/2020 1 51 28 PM
Roll Call Committee Registers Report

2020 SESSION

Commerce and Consumer Affairs

Bill #: 1650 Motion: Adopt AM #: 0560h Exec Session Date: 3/3/20

Members	YEAS	Nays	NV
Butler, Edward A. Chairman	✓		
Williams, Kermit R. Vice Chairman		✓	
Gidge, Kenneth N.		✓	
Abel, Richard M.		✓	
Bartlett, Christy D.	✓		
Herbert, Christopher J.		✓	
McBeath, Rebecca Susan	✓		
Van Houten, Constance	✓		
Fargo, Kristina M.		✓	
Indruk, Greg L.	✓		
Muscatel, Garrett D.	✓		
Weston, Joyce	✓		
Hunt, John B.		✓	
Sanborn, Laurie J.		✓	
Osborne, Jason M.		✓	
~~Costable, Michael~~ Lescelles		✓	
Plumer, John R.		✓	
Barnes, Arthur E.		✓	
Potucek, John M.		✓	
Warden, Mark			✓
TOTAL VOTE:	7	12	

OFFICE OF THE HOUSE CLERK

2/3/2020 1:51:28 PM
Roll Call Committee Registers Report

2020 SESSION

Commerce and Consumer Affairs

Bill #: 1680 Motion: Int. Study AM #: _____ Exec Session Date: 3/3/20

Members	YEAS	Nays	NV
Butler, Edward A. Chairman	✓		
Williams, Kermit R. Vice Chairman	✓		
Gidge, Kenneth N.	✓		
Abel, Richard M.	✓		
Bartlett, Christy D.	✓		
Herbert, Christopher J.		✓	
McBeath, Rebecca Susan	✓		
Van Houten, Constance	✓		
Fargo, Kristina M.	✓		
Indruk, Greg L.	✓		
Muscatel, Garrett D.	✓		
Weston, Joyce	✓		
Hunt, John B.	✓		
Sanborn, Laurie J.	✓		
Osborne, Jason M.	✓		
~~Costable, Michael~~ Lucy Weber	✓		
Plumer, John R.	✓		
Barnes, Arthur E.	✓		
Potucek, John M.	✓		
Warden, Mark			✓
TOTAL VOTE:	18	1	

Rep. Indruk, Hills. 34
February 7, 2020
2020-0560h
05/04

Amendment to HB 1680-FN

Amend the title of the bill by replacing it with the following:

AN ACT regulating the collection of personal information by broadband Internet access service providers and establishing a committee to study establishing broad data privacy rights in the state.

Amend the bill by replacing all after the enacting clause with the following:

1 New Chapter; Collection of Personal Information by Broadband Internet Access Service Providers. Amend RSA by inserting after chapter 359-Q the following new chapter:

CHAPTER 359-R

COLLECTION OF PERSONAL INFORMATION

BY BROADBAND INTERNET ACCESS SERVICE PROVIDERS

359-R:1 Definitions. In this chapter:

I. "Broadband Internet access service" means a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the service, excluding dial-up Internet access service.

II. "Customer" means an applicant for or a current or former subscriber of broadband Internet access service.

III. "Customer personal information" means:

(a) Personally identifying information about a customer, including but not limited to the customer's name, billing information, social security number, billing address and demographic data; and

(b) Information from a customer's use of broadband Internet access service, including but not limited to:

(1) The customer's web browsing history;

(2) The customer's application usage history;

(3) The customer's precise geolocation information;

(4) The customer's financial information;

(5) The customer's health information;

(6) Information pertaining to the customer's children;

(7) The customer's device identifier, such as a media access control address, international mobile equipment identity or Internet protocol address;

(8) The content of the customer's communications; and

(9) The origin and destination Internet protocol addresses.

IV. "Provider" means a person who provides broadband Internet access service.

359-R:2 Privacy of Customer Personal Information. A provider shall not use, disclose, sell, or permit access to customer personal information, except as provided in RSA 359-R:3, RSA 359-R:1, and 18 United States Code Section 2703.

359-R:3 Customer Consent Exception. Consent of a customer is governed by this section.

I. A provider may use, disclose, sell, or permit access to a customer's customer personal information if the customer gives the provider express, affirmative consent to such use, disclosure, sale, or access. A customer may revoke the customer's consent under this paragraph at any time.

II. A provider shall not:

(a) Refuse to serve a customer who does not provide consent under paragraph I, or

(b) Charge a customer a penalty or offer a customer a discount based on the customer's decision to provide or not provide consent under paragraph I.

III. A provider may use, disclose, sell, or permit access to information the provider collects pertaining to a customer that is not customer personal information, except upon written notice from the customer notifying the provider that the customer does not permit the provider to use, disclose, sell, or permit access to that information.

359-R:4 Other Exceptions. Notwithstanding RSA 359-R:2 and RSA 359-R:3, a provider may collect, retain, use, disclose, sell, and permit access to customer personal information without customer approval:

I. For the purpose of providing the service from which such information is derived or for the services necessary to the provision of such service;

II. To advertise or market the provider's communications-related services to the customer;

III. To comply with a lawful court order;

IV. To initiate, render, bill for, and collect payment for broadband Internet access service;

V. To protect users of the provider's or other providers' services from fraudulent, abusive, or unlawful use of or subscription to such services; and

VI. To provide geolocation information concerning the customer:

(a) For the purpose of responding to a customer's call for emergency services, to a public safety answering point; a provider of emergency medical or emergency dispatch services; a public safety, fire service or law enforcement official; or a hospital emergency or trauma care facility; or

(b) To a provider of information or database management services solely for the purpose of assisting in the delivery of emergency services in response to an emergency.

359-R:5 Security of Customer Personal Information. A provider shall take reasonable measures to protect customer personal information from unauthorized use, disclosure, or access.

I. In implementing security measures required by this section, a provider shall take into account each of the following factors:

(a) The nature and scope of the provider's activities;

(b) The sensitivity of the data the provider collects;

(c) The size of the provider; and

(d) The technical feasibility of the security measures.

II. A provider may employ any lawful measure that allows the provider to comply with the requirements of this section.

359-R:6 Notice Required. A provider shall provide to each of the provider's customers a clear, conspicuous, and nondeceptive notice at the point of sale and on the provider's publicly accessible website of the provider's obligations and a customer's rights under this chapter.

359-R:7 Applicability. The requirements of this chapter apply to providers operating within the state when providing broadband Internet access service to customers that are physically located and billed for service received in the state.

359-R:8 Enforcement and Remedies.

I. Any customer whose personal information has been used, disclosed, sold, or accessed in violation of this chapter may institute proceedings in any court of competent jurisdiction against the provider and shall be entitled to recover actual damages, $1,000 in total damages, or $100 for each violation, whichever is greater, as well as non-pecuniary damages.

II. A court shall award costs and reasonable attorneys' fees to a plaintiff who is the prevailing party in an action brought under paragraph I.

III. Any provider that violates this chapter shall be liable for a civil penalty of up to $1,000 per violation, or up to $7,500 per intentional violation, in a civil action brought by the attorney general.

2 Committee Established. There is established a committee to study establishing broad data privacy rights in the state.

3 Membership and Compensation.

I. The members of the committee shall be as follows:

(a) Three members of the house of representatives, one of whom shall be from the commerce and consumer affairs committee, and one of whom shall be from the science and technology committee, appointed by the speaker of the house of representatives.

(b) One member of the senate, appointed by the president of the senate.

II. Members of the committee shall receive mileage at the legislative rate when attending to the duties of the committee.

4 Duties.

I. The committee shall study:

(a) The ways in which the personal information of New Hampshire residents is digitally collected, stored, disclosed, or used for commercial purposes, and by which commercial entities.

(b) Existing protections, or the lack thereof, in New Hampshire law that require consumer consent before personal information can be digitally collected, stored, disclosed, or shared by commercial entities.

(c) How other states provide greater consumer privacy protection than New Hampshire, including restrictions on what digital information can be shared with third parties and when.

(d) How New Hampshire could strengthen consumer data privacy, including consent requirements and requirements that certain data be deleted.

II. The committee may solicit information from any person or entity the committee deems relevant to its study.

5 Chairperson; Quorum. The members of the study committee shall elect a chairperson from among the members. The first meeting of the committee shall be called by the first-named house member. The first meeting of the committee shall be held within 15 days of the effective date of this section. Three members of the committee shall constitute a quorum.

6 Report. The committee shall report its findings and any recommendations for proposed legislation to the speaker of the house of representatives, the president of the senate, the house clerk, the senate clerk, the governor, and the state library on or before November 1, 2020.

7 Effective Date.

I. Section 1 of this act shall take effect July 1, 2021.

II. The remainder of this act shall take effect upon its passage.

2020-0560h

AMENDED ANALYSIS

This bill:

I. Prohibits a provider of broadband Internet access service from using, disclosing, selling or permitting access to customer personal information unless the customer expressly consents to that use, disclosure, sale, or access.

II. Provides other exceptions under which a provider may use, disclose, sell, or permit access to customer personal information.

III. Prohibits a provider from refusing to serve a customer, charging a customer a penalty or offering a customer a discount if the customer does or does not consent to the use, disclosure, sale, or access.

IV. Requires providers to take reasonable measures to protect customer personal information from unauthorized use, disclosure, sale, or access.

V. Establishes a legislative committee to study establishing broad data privacy rights in New Hampshire.

Rep. Indruk, Hills. 34
February 7, 2020
2020-0560h
05/04

Amendment to HB 1680-FN

Amend the title of the bill by replacing it with the following:

AN ACT regulating the collection of personal information by broadband Internet access service providers and establishing a committee to study establishing broad data privacy rights in the state.

Amend the bill by replacing all after the enacting clause with the following:

1 New Chapter; Collection of Personal Information by Broadband Internet Access Service Providers. Amend RSA by inserting after chapter 359-Q the following new chapter:

CHAPTER 359-R

COLLECTION OF PERSONAL INFORMATION

BY BROADBAND INTERNET ACCESS SERVICE PROVIDERS

359-R:1 Definitions. In this chapter:

I. "Broadband Internet access service" means a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the service, excluding dial-up Internet access service.

II. "Customer" means an applicant for or a current or former subscriber of broadband Internet access service.

III. "Customer personal information" means:

(a) Personally identifying information about a customer, including but not limited to the customer's name, billing information, social security number, billing address and demographic data; and

(b) Information from a customer's use of broadband Internet access service, including but not limited to:

(1) The customer's web browsing history;

(2) The customer's application usage history;

(3) The customer's precise geolocation information;

(4) The customer's financial information;

(5) The customer's health information;

(6) Information pertaining to the customer's children;

(7) The customer's device identifier, such as a media access control address, international mobile equipment identity or Internet protocol address;

(8) The content of the customer's communications; and

(9) The origin and destination Internet protocol addresses.

IV. "Provider" means a person who provides broadband Internet access service.

359-R:2 Privacy of Customer Personal Information. A provider shall not use, disclose, sell, or permit access to customer personal information, except as provided in RSA 359-R:3, RSA 359-R:4, and 18 United States Code Section 2703.

359-R:3 Customer Consent Exception. Consent of a customer is governed by this section.

I. A provider may use, disclose, sell, or permit access to a customer's customer personal information if the customer gives the provider express, affirmative consent to such use, disclosure, sale, or access. A customer may revoke the customer's consent under this paragraph at any time.

II. A provider shall not:

(a) Refuse to serve a customer who does not provide consent under paragraph I; or

(b) Charge a customer a penalty or offer a customer a discount based on the customer's decision to provide or not provide consent under paragraph I.

III. A provider may use, disclose, sell, or permit access to information the provider collects pertaining to a customer that is not customer personal information, except upon written notice from the customer notifying the provider that the customer does not permit the provider to use, disclose, sell, or permit access to that information.

359-R:4 Other Exceptions. Notwithstanding RSA 359-R:2 and RSA 359-R:3, a provider may collect, retain, use, disclose, sell, and permit access to customer personal information without customer approval:

I. For the purpose of providing the service from which such information is derived or for the services necessary to the provision of such service;

II. To advertise or market the provider's communications-related services to the customer;

III. To comply with a lawful court order;

IV. To initiate, render, bill for, and collect payment for broadband Internet access service;

V. To protect users of the provider's or other providers' services from fraudulent, abusive, or unlawful use of or subscription to such services; and

VI. To provide geolocation information concerning the customer:

(a) For the purpose of responding to a customer's call for emergency services, to a public safety answering point; a provider of emergency medical or emergency dispatch services; a public safety, fire service or law enforcement official; or a hospital emergency or trauma care facility; or

(b) To a provider of information or database management services solely for the purpose of assisting in the delivery of emergency services in response to an emergency.

SUBCOMMITTEE WORK SESSION

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

SUBCOMMITTEE WORK SESSION on HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: February 7, 2020

Subcommittee Members: Reps. Williams, Sanborn, Abel, Plumer, Costable and Warden

Comments and Recommendations: Testimony from ACLU and Comcast. Consider public hearing of new amendment.

Respectfully submitted,

Rep. Edward Butler
Subcommittee Chairman

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

SUBCOMMITTEE WORK SESSION on HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: 2/7/2020

Subcommittee Members: Reps. Williams, Sanborn, Abel, Plumer, Costable, Warden, Herbert, Indruk and Butler

Comments and Recommendations:

testimony from ACLU + Comcast
considered public hearing of new
amendment

MOTIONS: OTP, OTP/A, ITL, Retained (1st Yr), Interim Study (2nd Yr)
(Please circle one)

Moved by Rep. _____ Seconded by Rep. _____ AM Vote:

Adoption of Amendment # _____

Moved by Rep. _____ Seconded by Rep. _____ Vote:

_____ Amendment Adopted _____ Amendment Failed

MOTIONS: OTP, OTP/A, ITL, Retained (1st Yr), Interim Study (2nd Yr)
(Please circle one)

Moved by Rep. _____ Seconded by Rep. _____ AM Vote:

Adoption of Amendment # _____

Moved by Rep. _____ Seconded by Rep. _____ Vote:

_____ Amendment Adopted _____ Amendment Failed

Respectfully submitted,

Rep. _____
Subcommittee Chairman/Clerk

Hearing Minutes

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

Continued PUBLIC HEARING ON HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: February 24, 2020

LOB ROOM: 302 Time Public Hearing Called to Order: 9:05 a.m.

Time Adjourned: 10:53 a.m.

Committee Members: Reps. Butler, Williams, Gidge, Abel, Bartlett, Herbert, McBeath, Van Houten, Fargo, Indruk, Muscatel, Weston, Hunt, Sanborn, J. Osborne, Costable, Plumer, Barnes, Potucek and Warden

Bill Sponsors:
Rep. Muscatel Rep. Indruk

TESTIMONY

Rep. Butler - We are hearing two bills significantly different than earlier versions.

1. **Rep Indruk** introduced the amended bill - Protects Consumer Choice about use of Customer's Private Information.
   - This issue needs t be handled by the state legislature because Federal Law/Regulation does not cover it.
   - See Amendment 2020-0560h dated 2/7/2020
   - Information not CPI can be used by broadband provider according to reasonable standard.

   Question: **Rep Van Houten** - Elaborate on opt out?
   Answer: Similar to California. May consider establishing commission to give adequate time for more than preliminary findings.
   Question: **Rep Herbert** - Commission necessary?
   Answer: This bill, as amended can stand on it's own.
   Question: **Rep Warden** - What is the intent on line 15?
   Answer: Satellite, Cable, etc. Notice required - Initial of sale of service and on website.

2. **Albert Scherr** - Informational Privacy Expert
   - Discussed privacy issues the Founders could not imagine.
   - 21st Century privacy of information.
   - This amendment puts simple, commonsense, reasonable protections in place.
   - Opt in/Opt out
   - Provider needs to get permission from consumer
   - Provider cannot reduce service because consumer does not give permission.
   - This amendment language mirrors FCC and Maine legislative language.
   - Is a proactive way to implement for business limitations in providers language addressing privacy limitations on government.
   - This bill is content neutral
   - It is a big reach to consumer
   - There is a first amendment problem.
   - Internet service providers are gateway to Internet and ISP is different than anyone else
   - The Federal Communication Act allows states to regulate ISPs.
   - The dormant commerce clause prohibits states from burdening interstate commerce.
   - This bill only covers actions within NH.

3. **Neal Kirk** - Weare
   - Significant economic component to provider

- Important consumers know this
- Opt out allows consumer protection
- Allows consumer to make reasoned decision.

Question: **Rep. Butler, Herbert, and Abel** - Loss of benefit from opt in/out?
Answer: NH better informed about this. Would not expect it to affect cost of providing services.

4. **Andrew Kingmon** - Boston, MA- Opposes
   - Correction: Federal rules have never been in effect.
   - Feds already have power to prosecute ISPs.
   - State AG right now has the same power.
   - Opt in/Opt out confuses consumers.

5. **Christina Fisher** - TechNet, Boston, MA - Opposes
   - Law is unsettled.
   - Encourage not going forward.
   - Impacts products and services.

   Question: **Rep Herbert** - Opt in/Opt out is there a better model?
   Answer: None exists now. NH should establish a study committee.

6. **Maura Weston & Russel Hanser** - NE Cable and Telecommunications Association
   - Claims it is not legal to regulate just one kind of business.
   - Unconstitutional
   - Harms consumer by frustrating and confusing consumers.
   - Says edge providers can access consumer date, but ISPs cannot.
   - This bill, part 2 imposes burdensome restrictions
   - Preempted by Federal Law

   Question: **Rep Van Houten** - Is this confusing or not. Can direct statements protect consumers?
   Answer: Largely about confusing consumers. There are 3 Federal laws now before Congress. There is a Federal framework in place. Says state actions that frustrate federal jurisdiction are prohibited.

7. **Daniel Lyons**
   - Creates playing field for advertisers
   - Reduces advertising revenue
   - Can lead to costs to consumer
   - Prefers Opt/Out only

8. **Benjamin Aron** - CTIA- The Wireless Association - Opposed
   - Consumers don't want this
   - Confuses consumers
   - Other types of business have greater access to consumer information than ISPs because most traffic is encrypted and not accessible by ISPs.

9. **Kevin Flynn** - BIA - Opposes
   - Concerned this will make NH an outlier
   - "Fishing for whales using Tuna nets"

   Rep Butler - Repeatedly hear that States need to act first as laboratory for federal actions.

10. **Jeanne Hruska** - ACLU-NH - Supports
    - Same entities testifying against this bill, also testified against federal laws
    - Reason to support the bill - ISPs bill consumers directly.
    - No such thing as single comprehensive privacy laws
    - RElationships with providers of different services
    - ISPs can identify types of sites consumer access
    - Need to protect all consumers
    - Lawsuits don't have merit because they are filed to delay implementation of ME State Laws and to scare off other states
    - If ME law upheld, it won't cause ISPs to leave the state.

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

PUBLIC HEARING ON HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE:

ROOM: 302 Time Public Hearing Called to Order:

Time Adjourned:

(please circle if present)

Committee Members: Reps. Butler, Williams, Gidge, Abel, Bartlett, Herbert, McBeath, Van Houten, Fargo, Indruk, Muscatel, Weston, Hunt, Sanborn, J. Osborne, Costable, Plumer, Barnes, Potucek and Warden

Bill Sponsors:
Rep. Muscatel Rep. Indruk

TESTIMONY

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

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

present Warden, Gidge, Plumer, Bartlett, Van Houten, Abel, Butler, Hunt, Indrunk, Herbert

HB 1680 continued Public Hearing
2/21/2020
clerk: Richard M. Abel

open hearing 9:05 am
close hearing 10:53 am

Rep. Butler Hearing 2 bills significantly different than earlier versions

① *HB 1680 Rep Indrunk introduced amended bill protects consumer choice about use of customer's private information. This issue needs to be handled by state legislature, because Federal law/regulation does not cover it. (See: Amendment 2020-5600h. dated 2/7/20 Information not CPI can be used by broadband provider according to reasonable standard. (Also see written testimony.)

Q. per Van Houten: Elaborate on Opt Out. A. Similar to California. May consider establishing Commission to give adequate time for more than preliminary findings.

Q. per Herbert: Commission necessary? A. This bill as amended can stand on its own.

Q. per Warden: what is Intent on line 15? A) Rep. Indrunk elaborated: satelite, cable, etc. Notice required: At initial point of sale of service, and on website.

② Albert Scherr, Representing himself. Information privacy expert. Discussed privacy issues the Founders could not imagine: 21st century privacy of information. This amendment to

simple, commonsense:

puts reasonable protections in place: opt in / opt out. Provider needs to get permission from consumer. Provider cannot reduce service because consumer does not give permission. This amendment language mirrors FCC and Maine legislative language. Is a proactive way to implement for business limitations in previous language addressing privacy limitations on government. This bill is content neutral. It is a big reach to consider there is a first amendment problem. Internet service providers are gateway to internet, an ISP and different than anyone else. The federal communications act allows states to regulate ISPs. The dormant commerce clause prohibits states from burdening interstate commerce. This bill only covers actions w/in NH only. Written testimony to come.

(3) Neal Fink - significant economic component to providers.
Important consumers know this impact opt out allows consumer protection allows consumer to make reasoned decision.

Q. Reps & Both Houses, Loss of benefit from opt in/out? A. NH better informed about this. Would not expect it to affect cost of providing services.

(4.) Andrew Kingman - oppose.
Concern: Federal rules have never been in effect. Feds already have power to prosecute ISPs. State AG right now has same power - opt in/out confuses consumers.

(5.) Christina Fisher, opposes. Law unsettled. Encourage not going forward - a ~~skeptical~~. Impede products and services.
Q. Herbert: opt in/out - ~~is~~ is ~~there~~ there a better model? A. None exists now. Says NH should establish study committee.

(6.) * NE Cable & Telecomm Society
Written testimony - claims not legal to regulate just one kind of business. Unconstitutional. Harms consumers by frustrating and confusing consumers; ~~consumer choice~~
(See written testimony #6.)
Says edge providers can access consumer data, but ISPs cannot.) This bill, part 2, imposes burdensome restrictions. Preempted by federal law.
Q. Rep Van Houten ? Is this confusing or not? ~~Sen~~ Can direct statements protect consumers. A. Largely about confusing consumers. 3 Federal laws now before Congress - says there is a federal framework in place. ~~Says~~ State actions that frustrate ~~federal restrictions~~ federal jurisdiction are prohibited.

(7.) * creates Unlevel playing field for advertisers
(See written testimony #7.)
Reduces advertising revenue. Can lead to costs to consumers.

Prefers opt out only.

(8) * (See written testimony) opposed. consumers don't want this; confuses consumers. other types of businesses have greater access to consumer information than ISPs, because most traffic is encrypted and not accessible by ISPs.

(9) BIA. Concerned this will make NH an outlier.

"Fishing for whales using tuna nets."

Rep. Potter comment:

Repeatedly hear that States need to act first as laboratory for federal action.

(10) * Written testimony.

- same entities testifying against this bill, also testified against federal laws.

- Reason to support bill: ISPs bill consumers directly. No such thing as single comprehensive privacy laws. Relationships with providers of different services. ISPs can identify types of sites Consumers access. Need to protect all consumers. Lawsuits don't have merit because they are filed to delay implementation of ME state laws, and to scare off other states. If ME law upheld won't cause ISPs to leave State.

SIGN UP SHEET

To Register Opinion If Not Speaking

Bill # HB 1680-FN Date 2/21/2020

Committee COMMERCE

** Please Print All Information **

Name	Address	Phone	Representing	(check one) Pro	Con
Teresa Rosenberger	226-7000		NH Telephone Assn		X
Ellen Scarponi	703-7315		Consolidated		X

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

PUBLIC HEARING ON HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: January 23, 2020

LOB ROOM: 302 **Time Public Hearing Called to Order:** 3:40 p.m.

Time Adjourned: 5:15 p.m.

Committee Members: **Reps. Williams, Abel, Herbert, Van Houten, Fargo, Indruk. Muscatel, Weston, Hunt, Potucek and Warden**

Bill Sponsors:
Rep. Muscatel **Rep. Indruk**

TESTIMONY

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

*1. Rep **Greg Indruk** - Introduced bill
*2. Rep **Garrett Muscatel** - Introduced bill
Personal info out there. We are being tracked (see handwritten testimony)

Question: **Rep Williams** - Addition to CP Law. How enforced? Private Right of Action with limit of
$750.
Answer: Based on CA language. WA model does not have Private Right of Action.
Question: **Rep Williams** - Small dollar amount for each violation?
Answer: Per incident
Question: **Rep Williams** - Enforcement could be issue
Answer: **Rep Indruk** - Amendment has safe harbor provision.
Question: **Rep Warden** - Does this include government entities?
Answer: Exemption for government. We don't trust government more. It is just not our target.

3. **Neal Kurk** - Support
- Applies only to for-profit businesses
- $25 Million or 50,000 customers, or collect data primarily (50% of revenue from this)
- 40% of bill equals definitions
- Represents what most people want - complete transaction, nothing more.
  1. Gives right to know what business have collected about you
  2. Right to opt out of business selling to 3rd parties
  3. Right to require business to delete info
  4. Guarantee - no discrimination if exercise these rights.

  Major Carve-outs:
  1. Business under HIPPA
  2. Business under Gramm, Leach, Biley
- Puts companies doing business in CA having a CA website and other
- Amend to make nationwide
- If Congress legislates could protect NH citizens if same as CA
- CA bill is good and has high level of protection
- Wants to pass as CA wrote it.
-

Question: **Rep Williams** - What types of business?
Answer: Credit reporting exempted.

Question: **Rep Hunt** - Who is regulated?
Answer: Google, Amazon, etc. One of the three categories of business.
Question: **Rep Williams** - If exempt by Gramm, Leach, Biley, included? (GLBA)
Answer: Not a perfect bill, better if like CA
Question: **Rep Fargo** - What is the difference with the CA bill?
Answer: Not sure I can answer, but not increasing burden on business.
Question: **Rep Warden** - Mail houses?
Answer: Yes
Question: **Rep Hunt** - Opt in or Opt out?
Answer: Only opt in if under 16.
Question: **Rep Hunt** - Company has to say collecting?
Answer: On website, company policy.
Question: **Rep Hunt** - Enforceable? How do I know how they use the info?
Answer: They have to tell you and to tell you of opt outs.
Question: **Rep Hunt** - Facebook has long list of opt outs and you have to go through, but you still are relying on them. Can I sue if they don't?
Answer: Could be suit. Over time people will become aware and take action.
Question: **Rep Fargo** - What about those who have already given info? What happens after the bill passes?
Answer: Would allow you to prevent future use.

4. **John Garrigan** - Consumer Protection AG - No Position
   - 2 provisions of concern: RSA 359:R12:1 Allows for opinion of AG. Could require legal advice to private citizens. Can't do, only state agencies.
     RSA359:R:13 AG Required to adopt administrative rules. Resource and time intensive. Required to do by July 1.

Question: **Rep Williams** - If it becomes law, could do, but maybe conflict in statutes. But AG has done similar. could do.
Answer: Oppose enforcement provisions, explained difference between individual action and action with individual as victim.
Question: **Rep Hunt** - Opinion piece has to go?
answer: Leaves to wisdom of Legislature.

*5. **Stephanie Kinnett & David Collins** - Credit Unions - Oppose
   - GLBA
   - Existing Regulations already cover
   - Based off CA, inappropriate - not our state
   - Consumer education needed
   - State-by-state approach not good.

Question: **Rep Williams** - Aware of credit unions in CA, what are their opinions?
Answer: Waiting to have the rules finalized.

6. **Andrew Kingman** - State Privacy and Security Coalition - Opposes
   - 50,000 residents, not pieces of information
   - Enforcement - AG only for privacy provisions
   - No private right of action for privacy violations
   - 12 month look back period in this law
   - Displayed bill. Bill to correct. Some amendments, etc. Many pages displayed
   - Overly broad definition with privacy consequences
   - Initial compliance cost in CA was $55 Billion and $15 Billion over a decade
   - Some definition ("personal info") is too broad

Question: **Rep Williams** - CA AG provides opinion on how to comply?
Answer: Removed in last amendment.
Question: **Rep Williams** - Anything better?
Answer: Nevada, in some ways. There are other models coming. CCPA passed very quickly and had no ballot initiative.

*7. **Maura Weston** - NE Cable and Telecommunications Association - Opposed
- Some providers are small
- CA is a flawed model
- Cost of compliance is high and prevents from investing in better service
- Some concerns - Rights and obligations undermine consumer privacy, broad definition of "personal info", challenges to compliance, can shut down functionality.
- Notice provision problem is can invite bad actors, hackers
- Info collected for employment is not exempt. This goes beyond CCPA.
- Benefits lawyers, not individuals
- Will send info

*8. **Gerry Keegan** - CTIA - Opposes
- Sweeps too broadly. Can allow false access requests
- Impacts small and mid size businesses, not just big businesses
- CA law in effect for only 3 weeks

9. **Mike Carone** - Consumer Data Ind. Association - Opposed
- Not necessary legislation
- Rushed in CA
- Fraud and public record exemptions not good
- CA is not done yet
- Compliance costs undetermined
- NH shouldn't rush

Question: **Rep Williams** - Changes in CA and not in ours?
Answer: Yes, but hard to quantify, even had typos.

*10. **Christina Fisher** - Tech Net - Opposes
- Compliance costs
- Higher impact on small business and innovations.

Question: **Rep Williams** - Idea of end state of CA law?
Answer: No, colleague in CA sees as moving target. CA ballot initiative already filed.

*11. **Kevin Flynn** - BIA - Opposes
- California flawed

Question: **Rep Warden** - Small business be effected?
Answer: Drafted for Google, etc., but doesn't take much to pile up.
Question: **Rep Williams** - BIA generally supports privacy initiatives?
Answer: Business want to find a balance with rights on consumers with the ability to innovate, etc. and best practices.

*12. **Simon Thompson** - American council of Life Insurers - Written testimony only

*13. **Ryan Hale** - NH Bankers - Opposed
- Concerns about exemptions
- Vague how to apply to small institutions and banks
- Decrease in banks by 33% since 2010
- Passage of this will increase costs of compliance
- CA is still very fluid

Respectfully submitted,

Joyce/Connie

HOUSE COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS

PUBLIC HEARING ON HB 1680-FN

BILL TITLE: relative to the collection of personal information by businesses.

DATE: 1/23/20

ROOM: 302 **Time Public Hearing Called to Order:** 3:40

Time Adjourned: 5:15

(please circle if present)

Committee Members: Reps. Butler, Williams, McBeath, Gidge, Abel, Bartlett, Herbert, Van Houten, Fargo, Indruk, Muscatel, Weston, Hunt, Sanborn, J. Osborne, Costable, Plumer, Barnes, Potucek and Warden

Bill Sponsors:
Rep. Muscatel Rep. Indruk

TESTIMONY

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

(1)* Greg Indruck
(2) Garrett Muscatel } introduced bill.
Personal info out there - we're being tracked.
(See written testimony)
Q. Williams: Addition to CP law. How enforced?
Private Right of Action with limit of $750.
(A) Based on CA language. WA model does not have Private Right of Action
Q. William — Small $ amount for each violation.
A. Per incident
Q Williams - Enforcement could be issue.

(3) (1446)

(2) Garrett – Amendment has safe harbor provision

Q. Warden – Does this include gov't entities.

(A) Exemption for gov't. We don't trust gov't more. It's just not our target.

#

(3) Neal Kurk – support

applies only to for-profit businesses, $25 mil or 50,000 customers, or collect data primarily (50% of revenue from this?)

40% of bill = definitions

represents what most people want – complete transaction, nothing more

(1) gives rt to know what bus have collected about yo

(2) rt. to opt of of bus ~~sss~~ selling to 3rd parties

(3) rt to require bus. to delete info

(4) guarantee – no discrim if exercise these rights

major carve-outs —

bus under HIPPA

bus. " Grahmon Leaf Blighty

should be amended to done of CA bill – puts companies doing bus in CA having a CA website + other – amend to make nationwide // if Congress legislates could protect NH citizens if same as CA // CA bill is good + has high level of protection wants to pass as CA wrote it

HB ~~1446~~ 1680
(4)

Q - Wms - types of bus?
A credit reporting exempted
Q Hunt - Who is regulated?
A - Google, Amazon, etc. - one of the 3 categories of bus.
Q Wms - if exempt by Graham, Leech, Blighly, included?
A - not perfect bill, better if like CA
Q - Fargo - what dif w/ CA bill
A - not sure can answer, but not increasing burden on bus.
Q - Warden - mail houses?
A - yes
Q - Hunt opt-in or opt-out?
A only opt in if under 16
Q - Hunt - co has to say collecting?
A - on website, company policy
Q - Hunt - enforceable? How do I know how they use info?
A - have to tell you & to tell you of opt-outs
Q - Hunt - FCB has long list of opt-outs & you have to go through but you still relying on them / can I sue if don't?
A - ~~can~~ could be suit / over time people will become aware & take action
Q - Fargo - What about those who've already given info, what happens after bill passes
A - would allow you to prevent future use

HB 1416-80
(5)

(4) John Garrigan - Cons. Protection AG — no pos.
2 provisions of concern
RSA 359:R12:1 (rule making)
RSA 359:R:13
allows for opinion of AG - could require legal advice to private citizens - can't do, only state agencies
AG reg. to adopt admin. rules - resource & time intensive, reg. to do by July 1
Q - Wms. - if becomes law, could do, but maybe conflict in statutes, but AG has done similar - could do
A - oppose enforcement provisions, explained dif. betw. individual action & action w/ individual as victim
Q - Hunt - opinion piece has to go?
A - leaves to wisdom of legislature
(5) Stephanie Kinnett & (5p) David Collins - credit unions (opp.)
GLBA (Graham Leach)
existing regs already cover
based off CA inappropriate - not our state
consumer ed. needed
state-by-state approach not good
Q - Wm - aware of credit unions in CA - their opinions
A waiting to have rules finalized

HB 1680

(6)

(5) Andrew Kingman (opp.) - State Privacy & Security Coalition
correction - 50,000 residents, not pieces of info
enforcement - AG only for privacy provisions,
no ~~private~~ private rt. of action for privacy
violations
D - no lookback period in this law
displayed - bill, bill, to correct, some amendments etc. =>
many pages displayed
overbroad def. w/ privacy consequences
initial compliance cost in CA = $55B + 16B ever decade
some def ("personal info" for ex) too broad
Q Wm - CA AG provide opinion on how to comply
A - removed in last amendment
Q Wm. - anything better
A - Nevada, in some ways / other model coming /
CCPA passed very quickly & had no ballot
initiative

*(7) Maura Weston (opp) NE - Cable & Telecommunications Assoc.
some providers small
CA is flawed model
cost of compliance high & prevent ~~for~~ from
investing in better service

some concerns -
rts & obligations undermine consumer
privacy
broad def of "personal info"
challenges to compliance
Can shut down functionality

HB 1680
p (7)

notice provisions - problem, can invite bad actors, hackers
info collected for employment - not exempt
this goes beyond CCPA
benefits lawyers, not individuals
will send info

(8)* Gerry Keegan - CTIA (opp)
2 issues
sweeps too broadly - can allow false access request
impacts sm. + mid-size businesses, not just big
CA law in effect for only 3 wks

(9) Mike Carone - (opp) Consumer Data Ind. Assoc.
not necessary legislation - rushed in CA
fraud + public records exemptions not good
CA - not done yet / compliance costs undetermined
NH shouldn't rush
Q - Wm - dbgs in CA + not in ours?
A - yes, but hard to quantify, even had typos

(10)* Christina Fisher, Tech Net (opp)
compliance costs, higher impact on sm. bus. + innovations
Q - Wms. - idea of end state of CA law?
A - no, colleague in CA sees as moving target
CA ballot initiave already filed

HB 1680
P - 8

(11) Kevin Flynn - BIA (OPP)
CA - flawed
Q - Warden - sm. bus be effected?
A - drafted for Google, etc., but doesn't take much to pile up
Q - Wm - BIA gen. supports privacy initiatives?
A - bus want to find bal w/ rts of consumers w/ ability to innovate, etc. + best practices

(12) Simon Thompson - American Council of Life Insurers
written testimony only

(13) Ryan Hale, NH Bankers (OPP)
concerns about exemptions, vague how apply to small institutions, banks decrease in banks by 33% since 2010 - passage of this will increase costs of compliance
CA still very fluid

Rep. Indruk, Hills. 34
January 23, 2020
2020-0204h
05/10

Amendment to HB 1680-FN

Amend the introductory paragraph of RSA 359-R:1, III(a) as inserted by section 1 of the bill by replacing it with the following:

(a) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the states of New Hampshire and California, and that satisfies one or more of the following thresholds:

Amend RSA 359-R as inserted by section 1 of the bill by inserting after RSA 359-R:14 the following new section:

359-R:15 Compliance With California Consumer Privacy Act. Any business in compliance with section 1798.100 of the California Civil Code shall be deemed in compliance with this chapter.

As written, this bill would recognize at least three fundamental rights:[8]

- **The right to know** what personal information is collected
- **The right to have personal information deleted**
- **The right to opt-out** of the sale of personal information

An alternative though similar model is currently working its way through the Washington state legislature, where it just passed the senate 46-1[9] and won the support of Microsoft.[10] Still more models exist in Europe[11] and throughout the world. As posted last April on the official Microsoft blog:

> Much of the rest of the world has moved to enact stronger privacy protections, but in the United States, efforts to pass a federal privacy bill have long been stalled. While Microsoft remains a strong supporter of federal laws, it is clear that the states — the laboratories of democracy — have an important role to play and currently are leading the charge to enact consumer privacy laws. Last summer, California passed the first comprehensive privacy law in United States history, the California Consumer Privacy Act (CCPA). While the CCPA remains a work in progress, it was an important milestone worth celebrating. It will provide one out of every eight Americans with important new privacy rights.[12]

I'm hopeful we can expand that project to NH and I have faith this committee will approach this important subject with the care it so clearly requires.

With that, I am mindful of the committee's time and would like to afford others a chance to speak. I thank you for your consideration and look forward to discussing the topic further with you in sub-committee.

Sincerely,

Rep. Gregory Indruk
Hillsborough District 34

---

[8] https://www.oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

[9] https://www.seattletimes.com/seattle-news/politics/senate-passes-bill-to-create-a-european-style-consumer-data-privacy-law-in-washington/

[10] http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bill%20Reports/Senate/5376%20SBR%20WM%2019.pdf?q=20200122193946

[11] https://gdpr-info.eu/

[12] https://blogs.microsoft.com/on-the-issues/2019/04/29/our-support-for-meaningful-privacy-protection-through-the-washington-privacy-act/

(1)

January 22, 2020
HB 1680
Rep. Greg Indruk
Hillsborough 34

Dear Mr. Chairmen and members of the committee,

I'm before you today to introduce HB 1680, which aims to provide sorely needed privacy protections in the age of big data and vanishing anonymity. The bill, as drafted, is based on language which went into effect in California starting January first of this year.[1] Many companies are already complying with this language, at least in so far as it applies to California residents. We recognize this is the starting point of what is sure to be a fruitful conversation with stakeholders. We are prepared to offer amendments and to work with others to further refine the bill so we can protect NH consumers while also enabling the many benefits of big data and modern business models.

Some of you may ask, why is this needed? I would like to offer a few points for your consideration:

1) New Hampshire voters recently passed an amendment to the Constitution adding a right to privacy.[2] As is, this amendment only binds the hands of government entities; it leaves our residents open to commercial data surveillance, distribution and monetization- even though our voters have clearly expressed a deep preference for privacy.
2) **Data is valuable**.[3] As at least one 2020 presidential candidate is apt to say, data is the oil of the 21st century.[4] Yet, consumers are often unwittingly having their data mined, packaged and sold from sources and for purposes beyond their wildest imaginations- all without monetary compensation. It is clear to many of us that an obscure disclosure on the 30th page of a terms and services document is a weak substitute for knowing consent in the collection, sale and use of our valuable private information.
3) **Data is everywhere**. We can't avoid leaking data at nearly every turn. If you use a cell phone, view a web page, drive a modern car or subscribe to almost any service- you are leaking data. An absurdly abbreviated list of collected data categories would include:
    - Age and demographic information
    - Passwords
    - Account numbers
    - Social security numbers
    - Likes and dislikes
    - Browsing history
    - How fast one drives
    - Precise geolocation and frequent sites of visitation
    - Heart rate, weight and other health metrics
    - and on and on and on....

    We are gushing with valuable information, and that makes us targets.
4) **Data can be misused and mismanaged**. Data can be used to manipulate consumers, voters and citizens of all stripes.[5] It can be grouped together to reidentify information thought to be anonymous.[6] It can be used to discriminate in the sale or provision of vital services.[7] And the unauthorized disclosure of personal information can have devastating effects, ranging from financial fraud, identity theft, or extortion, to destruction of property, harassment, reputational damage, emotional stress, and even physical harm.

---

[1] http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

[2] https://www.nh.gov/glance/bill-of-rights.htm

[3] https://www.weforum.org/agenda/2017/09/the-value-of-data/

[4] https://www.fastcompany.com/90411540/andrew-yang-proposes-that-your-digital-data-be-considered-personal-property

[5] https://www.psychologytoday.com/us/blog/positively-media/201803/how-cambridge-analytica-mined-data-voter-influence

[6] https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html

[7] https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

SIGN UP SHEET

To Register Opinion If Not Speaking

Bill # HB 1680-FN Date 1/23/2020

Committee COMMERCE & CONSUMER AFFAIRS

** Please Print All Information **

Name	Address	Phone	Representing	(check one) Pro	Con
J. Michael Allerton	72 Concord Dover NH			✓	
BILL BAKER	5 GEORGE LN			✓	
Alvin See	Loudon		Self		✓
MIKE SKELTON	MANCHESTER		GREATER MANCHESTER CHAMBER		X
CURTIS J. BARRY	N.H. RETAIL ASSOCIATION	CURTIS@BARRYGR.COM			X
Marissa Chase	NH Association for Justice	mchase@nhaj.org		✓	
PAULA ROGERS	~~Anthem~~		ANTHEM		X
Christina Fisher	BOSTON, MA		TECHNET		X
ANDREW KINGMAN	BOSTON, MA		STATE PRIVACY + SECURITY COALITION		X
Teresa Rosenberger	Concord		NH Telephone Asso		X
Lindsay Nadeau	Orr+Reno - for NH Assoc. of Domestic Insurance Companies and the American Property Casualty Insurance Association				✓ ✓
DAN BARRETT	BOW, NH		NH AUTO DEALERS ASSOC.		✓

SIGN UP SHEET

To Register Opinion If Not Speaking

Bill # 1274 Date 1-23-20

Committee

** Please Print All Information **

Name	Address	Phone	Representing	(check one) Pro	Con
John Dumais	110 Start St.	(603) 315-4164	NH GROCERS		✓
Nicole Messina	[redacted] Rye			✓	
Rosemarie Rung	Hillsborough 21			✓	
Ch					

Testimony

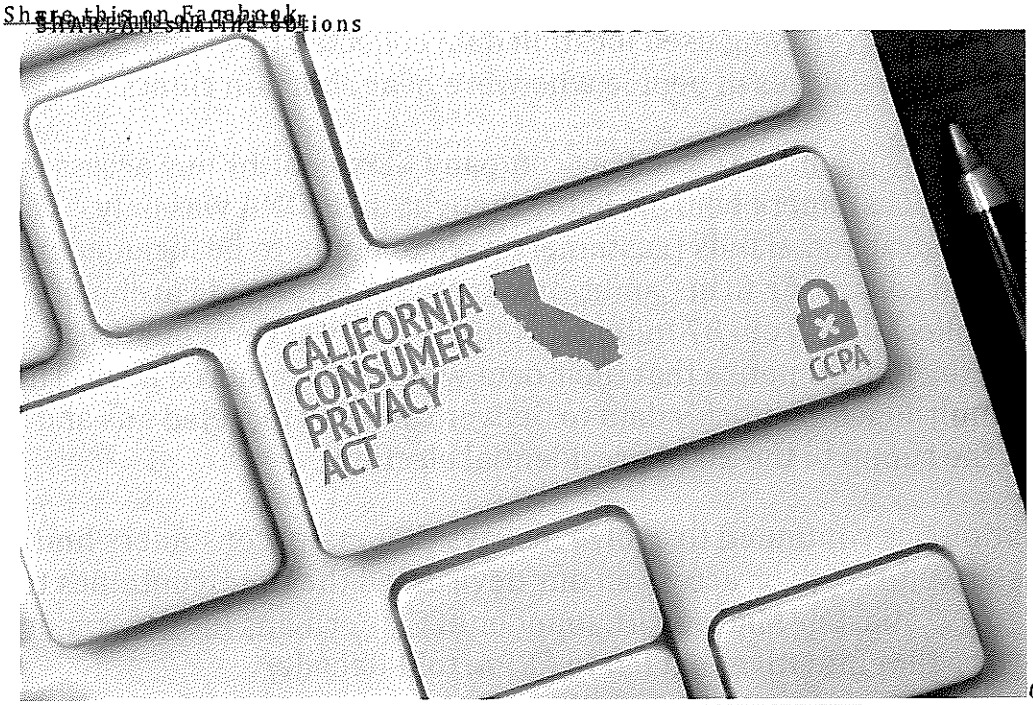
California's new privacy law, explained

The California Consumer Privacy Act gives Californians some control over their data, but only if they know how to take advantage of it.

By Sara Morrison Dec 30, 2019, 6:50pm EST

Share this story

- Share this on Facebook
- Share all share options



Cristian Storto/Shutterstock

OPEN SOURCED

Your data, whether it's your name, your location, or your shopping habits, has been a commodity for decades now. Collected, bought, sold, shared, transferred — however businesses get it, a lot of them have access to a lot of information about you. They use it in ways you never agreed to (and often that you're not even aware of), and they make a lot of money off of it. And there wasn't much you could do to stop them.

That's about to change ... to a point.

When the California Consumer Privacy Act, or CCPA (which you can read in full here), goes into effect on January 1, 2020, Californians will finally have certain rights over the data that companies like Facebook, Google, data brokers, and even Recode's parent company, Vox Media, collect from them. While these rights have limits, the very existence of this law is a victory for consumer privacy rights because it will introduce changes to a data collection industry that has gone unregulated and unchecked for so long.

For all the discussion about our online data and the privacy concerns surrounding it, it's sometimes hard to wrap your head around what companies really know about us, and what it means for us when they gather and sell this information. This data can be deeply personal. To give a few recent examples: Copley Advertising used location data collected from people's phones to send anti-choice ads to the devices of people who were near abortion clinics.

The consumer DNA testing company 23andMe gave drug company GlaxoSmithKline access to de-identified data from millions of customers who probably thought their DNA was only being used to discover their ancestral homelands (customers have to opt in to be included in research programs). And political consulting firm Cambridge Analytica exploited Facebook's developer tools to access and collect data from 87 million profiles — only several hundred thousand of which were given any kind of notice that their data was being gathered at all. The Trump campaign then used Cambridge Analytica's data to deliver carefully targeted ads and content at potential voters in the runup to the 2016 presidential election.

"The use of personal information has continued to evolve in ways that many consumers find increasingly offensive, as the drive to track us across all our devices, all the time, continues to be the focus for many businesses," Alastair Mactaggart, founder of Californians for Consumer Privacy and author of the 2018 ballot initiative that led to CCPA, told Recode.

If you don't live in California, you can still benefit from at least some of the law's requirements. At the very least, there is added transparency: Businesses must now notify consumers what personal information they collect about you and why. And some companies may give people all across the US the same opt-out and deletion rights they give to Californians because it's easier to roll out a widespread change.

That said, most experts and stakeholders told Recode the law is far from perfect. Some critics, like Eric Goldman, a professor and co-director of the High Tech Law Institute at the Santa Clara University School of Law, worry that the law will hurt the businesses that must comply with it. A report prepared for the state's office of the attorney general estimated that CCPA compliance will cost businesses $55 billion in initial charges.

"I think California consumers are going to be shocked by how rarely the CCPA helps them and how often it creates challenges for them," Goldman said. "Few consumers will ever take advantage of the rights created by the statute, but all consumers will implicitly pay more to help businesses cover their CCPA compliance costs."

If you want to take advantage of your rights, you first have to know what they are. The law's introduction lists the five rights it's meant to ensure, so let's start there. We'll use the new CCPA section of Vox Media's privacy policy as a real-world example.

1) The right of Californians to know what personal information is being collected about them

What this means: A business must tell you that it collects personal information about you either before or as that information is collected.

In the real world: Vox Media will now tell you in its privacy policy that it has collected several categories of personal information from users within the last 12 months, such as names, email addresses, and demographics. It also refers back to another section in the policy that details the information that it automatically collects whenever you interact with Vox Media's services, like what you are doing right now: reading an article on one of Vox Media's websites. That information includes things like your IP address and location.

Limitations/potential Issues: CCPA's definition of "personal information" includes everything from the obvious (your name) to the less obvious (your internet browsing history). If it can be linked back to you in some way, it's protected here. That's generally good for the consumer but makes it much more difficult for businesses to monitor and account for all of that data.

"Not all data is created equal, and therefore shouldn't be regulated in the same way," Ari Levenfeld, chief privacy officer at Quantcast, told Recode. "Data falls on a spectrum of sensitivity, ranging from personally identifiable information like names and email addresses, to less sensitive information such as pseudonymous data that is based on probabilistic, indirect identifiers like cookie IDs and IP addresses. The implications of exploiting or misusing the different types of data are fundamentally different, and therefore the regulations aimed at mitigating privacy risks should reflect those nuances."

2) The right of Californians to know whether their personal information is sold or disclosed and to whom

What this means: A business must tell you the types (though not the names) of third parties it shares your personal information with, but it's up to you to ask for this information. You also have the right to tell the business to delete your personal information and to not sell it (more on that later).

In the real world: You have the right to ask Vox Media for the categories of third parties that Vox Media has disclosed your personal information to, as well as what personal information was disclosed. You can do this by emailing vmprivacy@voxmedia.com or submitting a request through the online form.

Limitations/potential Issues: This is a part of CCPA that some critics say falls short on protecting people like you: In order to protect your personal information or to even know

what data businesses are gathering about you and selling to other companies, you have to take action on your own. It doesn't just happen by default. That's a problem, says Jennifer King, the director of privacy at the Center for Internet and Society at Stanford Law School.

"I think if we continue to legislate with this 'individual consumers are the ones who have to make all these choices for themselves' approach, and it's all on the burden of their shoulders to navigate this impossibly complicated ecosystem, these laws are only going to be somewhat effective," she said. "Not to completely criticize this law, because I think that it's important. It's a place to start," she added.

CCPA could cause issues for businesses as well because it leaves some things open to interpretation. Facebook, for example, sells ads based on its Pixel service, which is a line of code that businesses put on their websites that tracks users' behavior and links it to their Facebook accounts. What's tricky is that Facebook does not sell the actual data that Pixel gathers. Facebook makes money off of that data, but is that a sale? Facebook appears not to think so.

And some businesses are confused about how to interpret CCPA, according to Anneka Gupta, president and head of products and platforms at LiveRamp, a data processing company. "For example, we've heard that individuals and businesses are unclear about the exact definition of what constitutes 'selling data,'" she told Recode.

Vox Media's policy on data sales alludes to the uncertainty here: "We do not generally 'sell' personal information as the term 'sell' is traditionally understood."

3) The right of Californians to say no to the sale of personal information

What this means: Businesses must give you ways to opt out of having your personal information sold to or shared with third parties like advertisers or data brokers, and they must honor your opt-out request. They must also put a link to their opt-out page on their homepage advising you of this right.

In the real world: Vox Media provides two ways to opt out. You can email your request to vmprivacy@voxmedia.com, or click a link in the site footer that says "Do not sell my info." Here's what that looks like on Vox.com's homepage (highlight added):

You'll then be redirected to a contact form that requires you to disclose some personal information (ironic, but Vox Media has to know who you actually are in order to fulfill your request):

HELLO! WHY ARE YOU CONTACTING US TODAY?

I am a California resident and I have a personal information request

What would you like to do?*

Opt out of the sale of my info

Additional details:*

TELL US ABOUT YOU:

First and last name*:

Email address*:

Vox username (if you have one):

Exception: Businesses can still sell your information as long as personally identifiable details have been removed.

Limitations/potential Issues: You can tell a business you don't want it to sell your data, but there's no way to opt out of having that data collected in the first place. This means data collection kings like Google and Facebook can mostly continue on their merry way, even though the law was originally meant to rein both companies in.

"CCPA is focused on data brokers and other companies selling customer data," Roger Allan Ford, professor at the University of New Hampshire's Franklin Pierce Center for Law and Technology, told Recode. "That's a legitimate privacy problem, but the bigger problem comes from the ways that companies can gather and use information about consumers without buying or selling any data."

4) The right of Californians to access their personal information

What this means: Businesses must offer you ways to request a copy of the personal information they have collected about you, and they must provide it free of charge within 45 days of your request. You have the right to know the types of personal information (for example: name, email, or location) a business has collected, where it came from, why it was collected, the categories of third parties it has shared that information with, and the specific pieces of information it has collected. You can also tell them to delete that information.

In the real world: Vox Media's "right to know and delete" section gives you two ways to do this. Similar to the right to opt out, you can email vmprivacy@voxmedia.com or use Vox Media's contact form.

Limitations/potential Issues: Some businesses are still trying to figure out how to verify these requests.

"There seems to be confusion in ... how companies are to validate that the person is who they say they are," Gupta told Recode. "We do know there is a series of information that individuals are supposed to provide in order to validate their residency (name, address, phone number, email, identity verification materials, etc.), but there will need to be a significant amount of education around the type of proof needed for removal requests."

5) The right of Californians to equal service and price, even if they exercise their privacy rights

What this means: Businesses can't charge you extra or refuse to provide a service to you if you take advantage of your privacy rights under the new law. But they can offer bonuses or incentives in exchange for information.

In the real world: Vox Media's policy includes a "right to non-discrimination" that spells this out. It also has a "financial incentives" section that says it may pay customers for their personal information.

Exception: Loyalty programs, like those store cards that give you discounts on products in exchange for the information you provide to them (your name, email, items purchased), are not considered discriminatory.

What happens next

Once the law goes into effect, it must be enforced. That's up to the state attorney general's office. In certain cases, you might be able to sue businesses for privacy breaches, but only if a business's inadequate security measures caused your information to be disclosed, and it only covers the most sensitive stuff, like Social Security numbers, credit cards, or health information. Privacy advocates including the American Civil Liberties Union and the Electronic Frontier Foundation don't think CCPA goes far enough.

"It's not clear what enforcement will look like," Ford said. "Consumers can only sue for data breaches, which are a fairly small category of privacy problems. State enforcement of the rest of the law might help focus enforcement on real privacy problems rather than technical violations, but it might also mean the law winds up being under-enforced."

In the end, CCPA's legacy may not be the law itself, but the laws it inspires. California tends to be a national trendsetter when it comes to legislation. Several other states are already considering their own privacy laws. There are also several data privacy bills making their way through the federal government — in both chambers of Congress and from both sides of the aisle.

"While the CCPA is not perfect, it does provide a framework for approaching privacy in the age of technology," Levenfeld said. "The first-of-its-kind US law will lead to more comprehensive regulations in the future."

And Alastair Mactaggart is now collecting signatures for a new 2020 ballot initiative, called the California Privacy Rights Act, to address what he thinks CCPA is still missing. The law would tell consumers how and when automated decisions "significantly affect their lives" and it would create a new state agency to enforce the new laws.

"I believe consumers must be given even stronger rights to control their own information, all the time — not just the sale of information, which CCPA regulates effectively, but also the use of our most sensitive personal information," Mactaggart said.

January 22, 2020
HB 1680
Rep. Greg Indruk
Hillsborough 34

Dear Mr. Chairmen and members of the committee,

I'm before you today to introduce HB 1680, which aims to provide sorely needed privacy protections in the age of big data and vanishing anonymity. The bill, as drafted, is based on language which went into effect in California starting January first of this year.[1] Many companies are already complying with this language, at least in so far as it applies to California residents. We recognize this is the starting point of what is sure to be a fruitful conversation with stakeholders. We are prepared to offer amendments and to work with others to further refine the bill so we can protect NH consumers while also enabling the many benefits of big data and modern business models.

Some of you may ask, why is this needed? I would like to offer a few points for your consideration:

1) New Hampshire voters recently passed an amendment to the Constitution adding a right to privacy.[2] As is, this amendment only binds the hands of government entities; it leaves our residents open to commercial data surveillance, distribution and monetization- even though our voters have clearly expressed a deep preference for privacy.
2) **Data is valuable**.[3] As at least one 2020 presidential candidate is apt to say, data is the oil of the 21st century.[4] Yet, consumers are often unwittingly having their data mined, packaged and sold from sources and for purposes beyond their wildest imaginations- all without monetary compensation. It is clear to many of us that an obscure disclosure on the 30th page of a terms and services document is a weak substitute for knowing consent in the collection, sale and use of our valuable private information.
3) **Data is everywhere**. We can't avoid leaking data at nearly every turn. If you use a cell phone, view a web page, drive a modern car or subscribe to almost any service- you are leaking data. An absurdly abbreviated list of collected data categories would include:
    - Age and demographic information
    - Passwords
    - Account numbers
    - Social security numbers
    - Likes and dislikes
    - Browsing history
    - How fast one drives
    - Precise geolocation and frequent sites of visitation
    - Heart rate, weight and other health metrics
    - and on and on and on....

    We are gushing with valuable information, and that makes us targets.
4) **Data can be misused and mismanaged**. Data can be used to manipulate consumers, voters and citizens of all stripes.[5] It can be grouped together to reidentify information thought to be anonymous.[6] It can be used to discriminate in the sale or provision of vital services.[7] And the unauthorized disclosure of personal information can have devastating effects, ranging from financial fraud, identity theft, or extortion, to destruction of property, harassment, reputational damage, emotional stress, and even physical harm.

---

[1] http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

[2] https://www.nh.gov/glance/bill-of-rights.htm

[3] https://www.weforum.org/agenda/2017/09/the-value-of-data/

[4] https://www.fastcompany.com/90411540/andrew-yang-proposes-that-your-digital-data-be-considered-personal-property

[5] https://www.psychologytoday.com/us/blog/positively-media/201803/how-cambridge-analytica-mined-data-voter-influence

[6] https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html

[7] https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

As written, this bill would recognize at least three fundamental rights:[8]

- **The right to know** what personal information is collected
- **The right to have personal information deleted**
- **The right to opt-out** of the sale of personal information

An alternative though similar model is currently working its way through the Washington state legislature, where it just passed the senate 46-1[9] and won the support of Microsoft.[10] Still more models exist in Europe[11] and throughout the world. As posted last April on the official Microsoft blog:

> Much of the rest of the world has moved to enact stronger privacy protections, but in the United States, efforts to pass a federal privacy bill have long been stalled. While Microsoft remains a strong supporter of federal laws, it is clear that the states — the laboratories of democracy — have an important role to play and currently are leading the charge to enact consumer privacy laws. Last summer, California passed the first comprehensive privacy law in United States history, the California Consumer Privacy Act (CCPA). While the CCPA remains a work in progress, it was an important milestone worth celebrating. It will provide one out of every eight Americans with important new privacy rights.[12]

I'm hopeful we can expand that project to NH and I have faith this committee will approach this important subject with the care it so clearly requires.

With that, I am mindful of the committee's time and would like to afford others a chance to speak. I thank you for your consideration and look forward to discussing the topic further with you in sub-committee.

Sincerely,

Rep. Gregory Indruk
Hillsborough District 34

---

[8] https://www.oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

[9] https://www.seattletimes.com/seattle-news/politics/senate-passes-bill-to-create-a-european-style-consumer-data-privacy-law-in-washington/

[10] http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bill%20Reports/Senate/5376%20SBR%20WM%2019.pdf?q=20200122193946

[11] https://gdpr-info.eu/

[12] https://blogs.microsoft.com/on-the-issues/2019/04/29/our-support-for-meaningful-privacy-protection-through-the-washington-privacy-act/

What Does the California Consumer Privacy Act (CCPA) Do?

The CCPA gives state residents the right to:

- Know what personal data is being collected about them.
- Know whether their personal data is sold or disclosed and to whom.
- Say no to the sale of personal data.
- Access their personal data.
- Request that a business delete any personal information about a consumer collected from that consumer.
- Not be discriminated against for exercising their privacy rights.

Who's Affected?

For-profit entities that collect Californians' personal data and meet at least one of the following:

- Annually buys, receives, sells or shares the personal information of 50,000 or more consumers, households or devices.
- Has annual gross revenue of more than $25 million.
- Derives 50% or more of its annual revenue from selling consumer personal information.

Source: Security Boulevard
http://www.ncsl.org/research/telecommunications-and-information-technology/hands-off-the-data.aspx

[Art.] 2-b. [Right of Privacy.] An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent.
December 5, 2018

HB 1680 - 01/23/20 HEARING
[NEW YORK TIMES
12/20/19

Opinion | THE PRIVACY PROJECT

How to Track President Trump

By Stuart A. Thompson and Charlie Warzel

DEC. 20, 2019

IF YOU OWN A MOBILE PHONE, its every move is logged and tracked by dozens of companies. No one is beyond the reach of this constant digital surveillance. Not even the president of the United States.

The Times Privacy Project obtained a dataset with more than 50 billion location pings from the phones of more than 12 million people in this country. It was a random sample from 2016 and 2017, but it took only minutes — with assistance from publicly available information — for us to deanonymize location data and track the whereabouts of President Trump.

A single dot appeared on the screen, representing the precise location of someone in President Trump's entourage at 7:10 a.m. It lingered around the grounds of the president's Mar-a-Lago Club in Palm Beach, Fla., where the president was staying, for about an hour.

The president had what he called a working dinner with Mr. Abe that night.

Note: Driving path is inferred. Satellite imagery: Maxar Technologies, Microsoft, Earthstar Geographics.

THE DEVICE'S OWNER was easy to trace, revealing the outline of the person's work and life. The same phone pinged a dozen times at the nearby Secret Service field office and events with elected officials. From computer screens more than 1,000 miles away, we could watch the person travel from exclusive areas at Palm Beach International Airport to Mar-a-Lago.

[Related: Where Even the Children Are Being Tracked — We followed every move of people in one city. Then we went to tell them.]

The meticulous movements — down to a few feet — of the president's entourage were recorded by a smartphone we believe belonged to a Secret Service agent, whose home was also clearly identifiable in the data. Connecting the home to public deeds revealed the person's name, along with the name of the person's spouse, exposing even more details about both families. We could also see other stops this person made, apparently more connected with his private life than his public duties. The Secret Service declined to comment on our findings or describe its policies regarding location data.

The vulnerability of the person we tracked in Mr. Trump's entourage is one that many if not all of us share: the apps (weather services, maps, perhaps even something as mundane as a coupon saver) collecting and sharing his location on his phone.

Americans have grown eerily accustomed to being tracked throughout their digital lives. But it's far from their fault. It's a result of a system in which data surveillance practices are hidden from consumers and in which

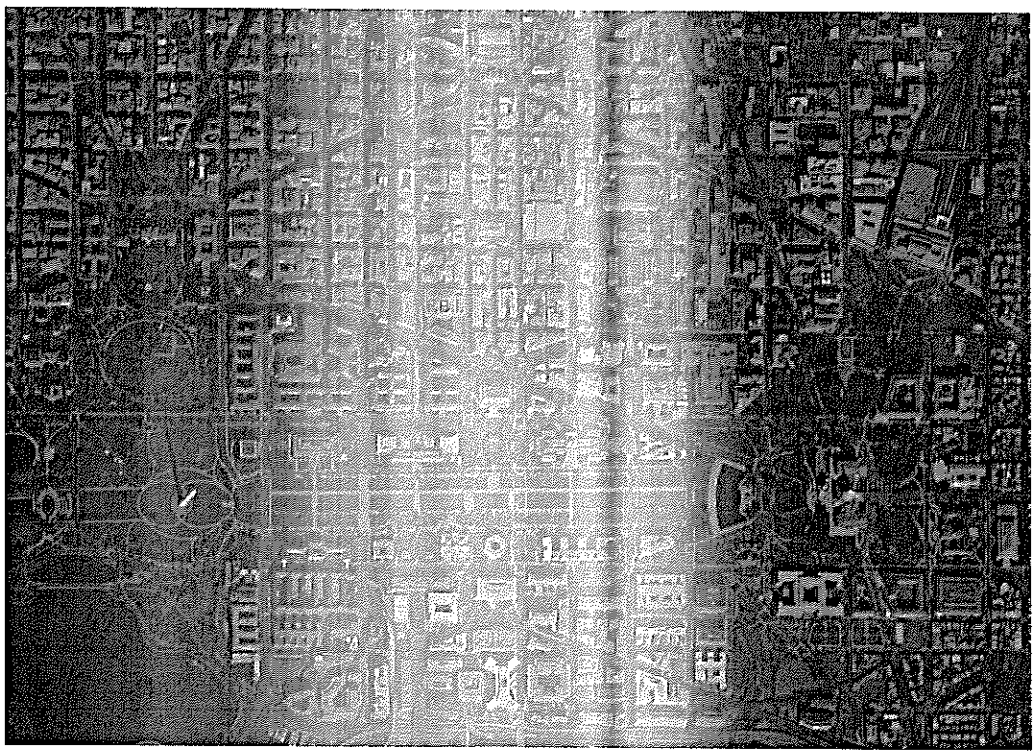
much of the collection of information is done without the full knowledge of the device holders.

Freaked Out?
3 Steps to Protect Your Phone

For the nation's security agencies, however, privacy is critical to the safety of military, defense and security operations across the country and abroad. If threats to that privacy have seemed abstract in the past, the trove of location data we have analyzed has brought them into sharp relief. Military and intelligence officials have long been concerned about how their movements could be exposed; now every move is. As a senior Defense Department official told Times Opinion, even the Pentagon has told employees to expect that their privacy is compromised:

"We want our people to understand: They should make no assumptions about anonymity. You are not anonymous on this planet at this point in our existence. Everyone is trackable, traceable, discoverable to some degree."

We were able to track smartphones in nearly every major government building and facility in Washington. We could follow them back to homes and, ultimately, their owners' true identities. Even a prominent senator's national security adviser — someone for whom privacy and security are core to their every working day — was identified and tracked in the data.



Note: Period of one month. Satellite imagery: Microsoft and DigitalGlobe

WHILE THE CONSTITUTION PREVENTS COMPANIES from sharing location data with the government without a warrant, there are no federal protections limiting how they use or share it privately. No such protections are

currently being debated before Congress — even though we found that we could track people through Congress's own halls as easily as any place else.

When we reached out to some lawmakers to show what we found, the outrage proved bipartisan.

"This is terrifying," said Senator Josh Hawley, Republican of Missouri, who has called for the federal government take a tougher stance with tech companies. "It is terrifying not just because of the major national security implications, what Beijing could get ahold of. But it also raises personal privacy concerns for individuals and families. These companies are tracking our kids."

"Tech companies are profiting by spying on Americans — trampling on the right to privacy and risking our national security," Senator Elizabeth Warren, a Democrat running for president, told us. "They are throwing around their power to undermine our democracy with zero consequences. This report is another alarming case for why we need to break up big tech, adopt serious privacy regulations and hold top executives of these companies personally responsible."

Agencies can limit how their employees use location-sharing apps and services, but that doesn't mean those guidelines will be strictly enforced — or extended to personal devices.

But no matter how comprehensive an organization's policies and regulations are, getting everyone to follow them is nearly impossible as many of these apps' surveillance practices are not visible to consumers.

"The human being is the weak link," said Martijn Rasser, a former Central Intelligence Agency officer who is now a senior fellow in the technology and national security program at the Center for a New American Security. "It's really difficult to enforce a lot of these rules and regulations. Sometimes, all it takes is one person to violate the rules to completely negate the purpose of having those rules in the first place."

Despite the sensitivity of this information, it is put to everyday use. Packaged with millions of other data points, location information is turned into marketing analysis and sold to financial institutions, real estate investors, advertising companies and others. Companies say they vet partners carefully and tend to work with larger players that have a clear business case for receiving the data.

Like all data, the vast location files are vulnerable to hacks, leaks or sale at any point along that process. The data we reviewed was provided to Times Opinion by sources who asked to remain anonymous because they were not authorized to share it and could face severe penalties for doing so.

Multiple experts with ties to the United States' national security agencies warned in interviews that foreign actors like Russia, North Korea, China and other adversaries may be working to steal, buy or otherwise obtain this kind of data. Only months ago, hackers working for the Chinese government allegedly targeted location data for people moving throughout Asia by breaking into telecom networks, according to a report by Reuters.

"People literally go to work every day, sit down at a desk, check the sports, send an email or two to their girlfriend and then start looking for databases they can steal," said James Dempsey, the executive director of the Berkeley Center for Law and Technology. "They just do that 9 to 5, every day."

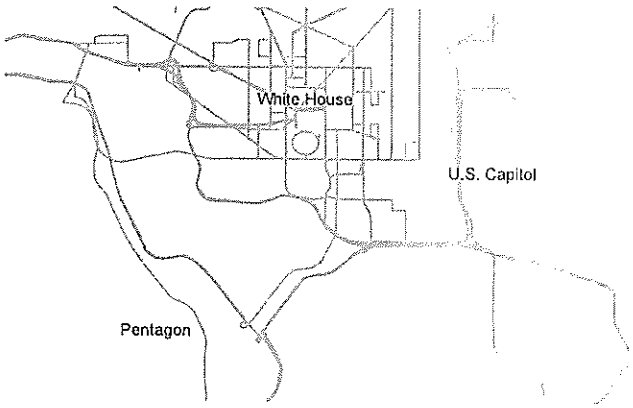
The American government may conduct similar intelligence operations against its adversaries, experts said, though under stricter legal frameworks.

Using the data, we identified people in positions of power by following smartphone pings as they moved around the White House, Capitol Hill, the Supreme Court and other government facilities. In many cases, the data trails led back to the smartphone users' homes. In this series, we did not name any of the identified people without their permission. And the data below has been obscured to protect device owners.

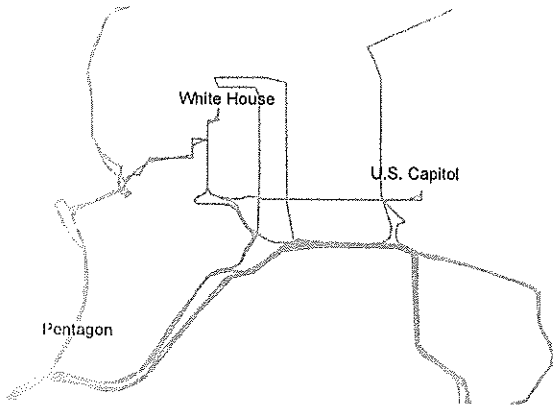
Senior Officials and Security Staff

Data has been obscured to protect device owners.

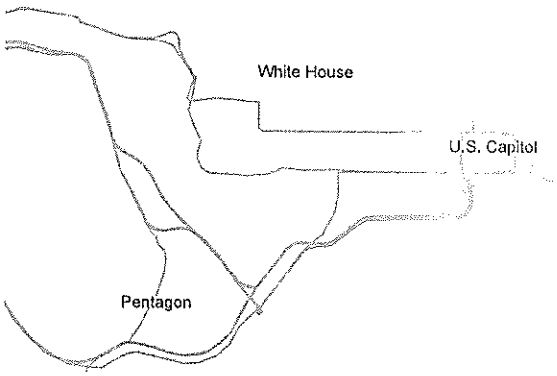
Secret Service agent



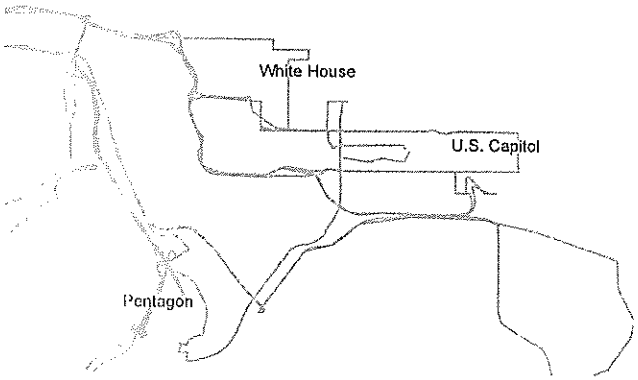
Secret Service agent



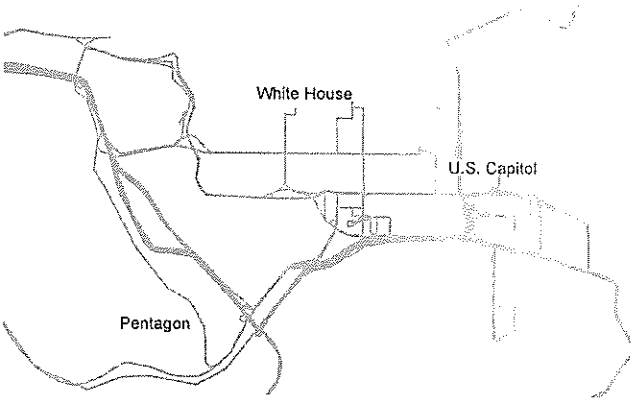
Technology at the Supreme Court



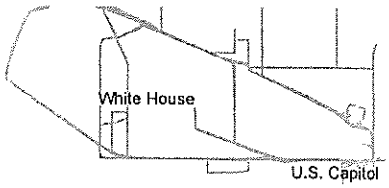
Department of Defense official



Director at a House committee



Advisor for a Senator



Pentagon

Note: Driving out" is inferred. Source: Microsoft, DigitalGlobe (satellite imagery)

CONNECTING A PING TO A PERSON was as easy as combining home and work locations with public information. A seemingly random set of movements turned into a clear individual pattern after we added just one other piece of information.

Plenty of corroborating information is already floating around dark corners of the web, given the frequent high-profile data breaches of the past decade. Consider what China already knows: In 2015, a federal database containing the personal information of more than four million people with security clearances was stolen by Chinese hackers presumed to be state actors.

"From those very detailed documents, they may gather a good deal of information about a person," said David S. Kris, a co-founder of the consulting firm Culper Partners and former assistant attorney general for the national security division of the Department of Justice. Mr. Kris said he was also included in the data that was hacked. "The more you can combine location-based data into a mosaic with other information, the more likely you are to gain real insight into an adversary."

Location data potentially gives any enemy an opening for attack. Russians, whose intelligence apparatus has worked for decades to disrupt American democracy, could simply leak location information to embarrass the government, the legal system or particular officials.

"Think about Russia's efforts to undermine public trust and confidence in our democratic institutions," Suzanne Spaulding, senior adviser at the Center for Strategic and International Studies and a former under secretary at the Department of Homeland Security, told us. "Think about all of the ways they could use location data to do that. Think about tracking judges everywhere they went and how you could use that to undermine confidence in our courts and our justice system."

After Ms. Spaulding raised the danger of tracking judges, we checked the data file for courthouse employees. In minutes, we found dozens of potential targets by watching smartphones sharing their precise locations inside Washington courthouses. One person whose movements we traced has a role in the technology division, which controls servers containing data for the Supreme Court.

For people with political power, knowing those locations could put their safety — and our national security — at risk. Experts told Times Opinion that foreign governments could use the data to monitor sensitive sites and identify people with access to them, and their associates.

"Not everybody in the department has a national security position, not everybody has access to classified or higher-level stuff," the senior Defense official said. "But everyone in the department is of some interest or value to a lot of adversaries just by virtue of being a member of the Defense Department, just by working at the Pentagon."

Satellite imagery: Imagery

THE POSSIBILITIES FOR BLACKMAIL ARE ENDLESS. Once stolen, details on sexual interests and extramarital affairs can provide opportunities for extortion. Targets could be coerced in ways large and small, compelled to make decisions or take actions for a foreign government. Or the locations themselves could provide valuable intelligence about security practices, contacts, schedules and the identities of people in prominent and sensitive posts, with access to state secrets or critical infrastructure.

With no training and far more limited technical tools than those of a state intelligence service, we were able to use the location data — date, time and length of stay — to make basic inferences. By determining whether two people were in the same place at the same time, it was easy to zero in on spouses, co-workers or friends. Cataloguing their movements revealed even more associations, creating the map of a robust social network that would be nearly impossible to determine through traditional surveillance. In cases where it was difficult to identify an individual, associations offered more clues about workplaces and interests.

In one case, it proved difficult to confirm the identity of a man listed in public records who had a common name. Examining his associations revealed that he met multiple times with someone carrying another phone that was being tracked. That person was, we soon learned, his brother. That piece of information doubled the pool of digital breadcrumbs to follow, ultimately helping confirm both of their identities.

Now consider elections. Bad actors could monitor candidates and elected leaders for intelligence that could be leaked or used to blackmail them. There are also no regulations limiting how long location data can be stored. Data swept up today may prove valuable in the future, as everyday citizens rise to positions of authority and influence only to have their precise movements from years gone by reviewed for damaging insights.

Defense contractors and employees at secure locations like power plants are all at risk.

Satellite imagery: Vexcel Imaging, Microsoft and DigitalGlobe

We found smartphone pings at all of these sorts of sites. In one case, someone who spent their weekdays at the Pentagon visited a mental health and substance abuse facility multiple times.

Even just commuting to work can be risky for people in prominent positions. "The easiest way to figure out how to get to you is know you always have the same routine," said Mr. Rasser, the former Central Intelligence Agency officer. He said he mixes up his own routine, partly because the C.I.A. emphasized such methods when he joined.

The threats will only grow as more data is collected and shared. More apps will enter the marketplace using tracking technology. And companies are becoming more sophisticated at collecting location data, adding signals from Wi-Fi networks and Bluetooth beacons. They also often rely on one-time consent or disclosures that don't explicitly state what's collected or shared.

Experts emphasized how location data has joined many other kinds of sensitive information in the espionage toolkit, showing how intelligence agencies must continually adapt to the digital age.

"We need to learn to operate with fewer secrets," Ms. Spaulding said.

Even areas once thought to be secure showed up in the data. Personal phones aren't generally allowed inside the C.I.A. or the National Security Agency. But while no pings registered inside the C.I.A. headquarters, we found thousands of pings in the parking lots outside, with trails that led to the homes of likely employees.

Satellite imagery: Microsoft and DigitalGlobe

Similarly, there were no blackout areas in many sensitive government buildings. We observed thousands of pings inside the Pentagon, on military bases, in F.B.I. headquarters and in Secret Service facilities across the country. (Intelligence facilities also have secure areas where certain electronic devices aren't permitted.)

The risks posed by location-tracking remain largely unaddressed by the government. Beginning last year, the Department of Defense prohibited geolocation features and functionality from being used by its workers on devices in "operational areas" like foreign military bases. For all other locations, the department said it would consider the risks and issue specific recommendations to personnel.

For now, the department does not issue guidance to employees about downloading specific apps, including those that might share location data with third parties. "Instead, we focused on certain core characteristics of

the geolocation functionality and identified what risks those characteristics posed," a department spokesman, Lt. Col. Uriah L. Orland, said in an email.

Agencies with a need for heightened security are left in a vulnerable position. Phones are ubiquitous, and so long as granular location tracking remains legal, even the Defense Department must play along. "We cannot stop our workforce of 3.6 million people from living their everyday lives," a senior department official told us.

We haven't identified any serving elected representatives in our data, but we found a former House representative and dozens of prominent public officials, including chiefs of staff, security officials and subcommittee staff members.

Given their proximity to public figures with public schedules and their presence at training sites and field offices, Secret Service agents were particularly easy to identify. With little difficulty, we were able to track a Secret Service agent who spent most of his daytime hours in the West Wing of the White House. He also joined President Trump at the National Cathedral the day after the inauguration.

Satellite imagery: Microsoft and DigitalGlobe

WHILE THE DATA REVIEWED by Times Opinion is from three years ago, similar information is being collected daily and often resold to third parties, meaning anyone with current access to such data could feasibly, in near real time, track people within arm's reach of the president or other powerful figures.

"If you want to take action against someone, you have to find them first," said Mr. Kris, the former Department of Justice official. "I'm wary of breathless, pearl-clutching, speculative, sensationalistic counterintelligence concerns. This doesn't strike me as falling into that category. I think there is a legitimate concern here."

Leaked location data may open the door to other cyber vulnerabilities. Foreign actors could learn movement details and infer meeting locations, which could be used to conduct a type of scam where targets receive fake emails — posing as a friend you just met with or a business you just visited — including a phony link meant to steal your password or install malware.

"Location tracking data of individuals can be used to facilitate reconnaissance, recruitment, social engineering, extortion and in worst-case scenarios, things like kidnapping and assassination," warned Kelli Vanderlee, manager of intelligence analysis at the cybersecurity company FireEye.

Those are not theoretical threats. The phone of the Washington Post journalist Jamal Khashoggi, who was assassinated in 2018, was allegedly compromised, possibly allowing his location data to be used to follow him.

Last year, Strava, a company that makes a fitness app, released a global map showing 700 million activities that clearly revealed American military bases abroad. The Department of Defense issued its recent guidance after discovering the problem. The data reviewed by Times Opinion revealed several points on domestic military bases as well, showing how some of the nation's most secure armed sites can be exposed.

"An adversary can still glean a lot from your whereabouts on the base itself," said Mr. Rasser, the former C.I.A. officer. "If you're always at a certain part of the base, at a certain time, you can start piecing together what the function of that corner of the base could be based on the person's job duties."

Using base locations as a guide, Times Opinion accurately surmised the job title of a commander in the U.S. Air Force Reserve. He regularly traveled to the Pentagon and visited Joint Base Andrews, perhaps best known as the home of the president's airliner, Air Force One.

Satellite imagery: Microsoft and DigitalGlobe

It's not necessary for someone to visit sensitive locations to be open to scrutiny or criticism. Location data could become a powerful political tool, exposing the private lives of wealthy elites who prefer to adopt a more egalitarian persona. It is not difficult to imagine efforts to undermine a political campaign by exposing travels through private airports or visits to expensive restaurants and luxurious spas.

The sources who provided the trove of location information to Times Opinion did so to press for regulation and increased scrutiny of the location data market. Some solutions exist that could help improve privacy while ensuring businesses can still perform some of the analysis they do today, like limiting the ability to identify individual paths, changing how long the information is stored and limiting how it's sold.

So far, Washington has done virtually nothing to address the threats, and location data companies have every reason to keep refining their tracking, sucking up more data and selling it to the highest bidders.

Stuart A. Thompson (stuart.thompson@nytimes.com) is a writer and editor in the Opinion section. Charlie Warzel (charlie.warzel@nytimes.com) is a writer at large for Opinion. Alex Kingsbury contributed reporting. Lora Kelley, Ben Smithgall and Vanessa Swales contributed research. Graphics by Stuart A. Thompson. Additional production by Jessia Ma and Gus Wezerek. Note: Visualizations have been adjusted to protect device owners.

COMMENT

ONE NATION, TRACKED

AN INVESTIGATION INTO THE SMARTPHONE TRACKING INDUSTRY FROM TIMES OPINION

Your Privacy Center

California residents

Access or Delete My Personal Information

California residents can see additional choices about their information on file, including the right to access or delete their personal information.

Do Not Sell My Personal Information

Unless you give us explicit permission, we don't sell data that directly identifies you. We may sell data among the AT&T companies or to other companies. When we do, it's for limited reasons with strict privacy controls. As a California resident, you can make choices about that sharing here.

For more information about your choices and preferences, please see the Choices & Controls section of Privacy Policy.

California Residents' Privacy Rights

The California Consumer Privacy Act of 2018 ("CCPA") provides California residents with rights to receive certain disclosures regarding the collection, use, and sharing of "Personal Information," as well as rights to access, delete, and restrict the sale of certain Personal Information we collect about them. You may submit a request to exercise these rights by visiting our Individual Rights Request Page or calling us at 1-844-963-0138.

The CCPA defines "Personal Information" to mean "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." If you are a California resident, you have a right not to receive discriminatory treatment for the exercise of the privacy rights conferred by the CCPA.

Residents of the State of California also have the right to request information regarding third parties to whom the company has disclosed certain categories of personal information during the preceding year for the third parties' direct marketing purposes under California's "Shine the Light" law (Cal. Civ. Code §1798.83). Personal information under this California law means "any information that when it was disclosed identified, described, or was able to be associated with an individual." We do not disclose this type of personal information to third parties for their own purposes and we permit you to opt-out of any disclosures of non-identifiable personal information. However, if you are a California resident and would like to inquire further, please email Comcast_Privacy@comcast.com.

We do not knowingly allow others to collect personally identifiable information about your online activities over time and across third-party websites when you use our online Services. Because definitions and rules for a 'Do Not Track' standard have not yet been established, including whether such signals must be user-enabled, Comcast does not yet respond to "Do Not Track" signals sent from browsers. For more information about cookies and other online tracking technologies, please visit our Cookie Notice; to manage your preferences, please visit the Xfinity Privacy Preferences Center.

Your California Privacy Rights

If you live in California and have an established business relationship with us, you can request a list of the personal information we have shared with third parties for their direct marketing purposes. The list will also give you information about the entities that received your information. You can make a request one time each year, by emailing or writing to us at the address below. Please indicate that you are making a California Shine the Light inquiry, and we will respond within 30 days.

The California Consumer Privacy Act ("CCPA") provides California residents with the following privacy rights:

- Right to Know: Consumers have a right to request information about the personal information that we collect, use, disclose, and sell.
- Right to Delete: Consumers have a right to request the deletion of personal information that we have collected from them, though we may be permitted to retain personal information for certain purposes.
- Right to Opt-out of Sales: We do not sell your information with third parties in exchange for money. We do share your information with third parties to enhance your experiences with us, to improve our ability to serve you and to keep you aware of our products, services, and offers. California law may treat some such disclosures as sales, and consumers have a right to direct us not to sell their personal information.
- Right to Opt-out of Financial Incentive Programs that we may offer.
- Non-Discrimination: We may not discriminate against you for exercising your rights under the CCPA. We may, however, provide a different level of service or charge a different rate if the difference is reasonably related to the value of your information.

If you are a California resident, or an authorized agent acting on behalf of a California resident, and would like to exercise one of these rights, please visit our website here or call us at 1-800-394-1326. For help submitting a request in one of our stores, please visit the customer service desk. Please note that we may require additional information from you in order to honor your request, and there may be circumstances where we will not honor your request, as permitted under the CCPA. For example, if you request deletion, we may need to retain certain personal information to comply with our legal obligations.

If you would like to exercise your right to opt out of the sale of your personal information, please click here: Do Not Sell My Personal Information.

Some of the tracking tools used on our websites, mobile applications, and other digital services may involve the sharing of personal information with third parties in exchange for their support in enhancing your experiences with us, improving our ability to serve you, or keeping you aware of our products, services, and offers. To exercise your choices regarding those tools, please read the Our Tracking Tools section below, particularly the section on controlling our tracking tools.

Walmart

California Privacy Rights

What Are Your California Privacy Rights?

Last Updated: January 1, 2020

California Consumer Privacy Act

If you are a California resident, you can make certain requests regarding your personal information. We will fulfill each of these requests to the extent required by law.

1. You can ask us what personal information we have about you, including a list of categories of your personal information that we have sold and a list of categories of your personal information that we have shared with another company for a business purpose.
2. You can ask us to delete your personal information.
3. You can ask that we stop selling your personal information.

More information on each of these requests is below.

1. What personal information do you collect about me? If you make this request, we will return to you (to the extent required by law):

- The categories of personal information we have collected about you.
- The categories of sources from which we collect your personal information.
- The business or commercial purpose for collecting or selling your personal information.
- The categories of third parties with whom we share personal information.
- The specific pieces of personal information we have collected about you.
- A list of categories of personal information that we have sold, along with the category of any other company we sold it to. Any of the categories of personal information that we collect could be included in a sale to other companies, including those within our corporate family. If we have not sold your personal information, we will inform you of that fact.
- A list of categories of personal information that we have disclosed for a business purpose, along with the category of any other company we shared it with.

You can ask us to provide you with this information up to two times in a rolling twelve-month period. When you make this request, the information provided may be limited to personal information we collected about you in the previous 12 months.

2. Delete My Personal Information: You have the right to ask that we delete your personal information. Once we receive a request, we will delete the personal information (to the extent required by law) we hold about you as of the date of your request from our records and direct any service providers to do the same. In some cases, deletion may be accomplished through de-identification of the information. If you choose to delete your personal information, you may not be able to use certain website or in-store functions that require your personal information to operate. Deleting your personal information will not cancel memberships you have purchased.

3. Stop Selling My Personal Information: We do not sell your personal information for monetary consideration. However, under some circumstances a transfer of personal information to a third party,

or within our Walmart family of companies, without monetary consideration may be considered a "sale" under California law. For purposes of California law, all categories of personal information, except for background and criminal information, biometric information, and government identifiers, are transferred to third parties or within our family of companies. Such transfers may be considered a sale. If you submit a request to stop selling your personal information, we will stop making such transfers. If you are a California resident, to opt-out of the sale of your personal information, click "Do Not Sell My Personal Information" at the bottom of our home page to submit your request.

We will not discriminate against you for exercising your rights. This generally means we will not deny you goods or services, charge different prices or rates, provide a different level of service or quality of goods, or suggest that you might receive a different price or level of quality for goods. Please know, if you ask us to delete or stop selling your data, it may impact your experience with us, and you may not be able to participate in certain programs or membership services which require usage of your personal information to function.

To exercise the California privacy rights described above, please click "Request My Personal Information" at the bottom of our home page or call 1-800-Walmart (1-800-925-6278).

To exercise these California privacy rights for personal information at Vudu, please visit vudu.com and click the "Do Not Sell My Personal Information" or "Request for Personal Information" links on the home page or call 888-555-8838.

Your California Privacy Rights - Shine the Light

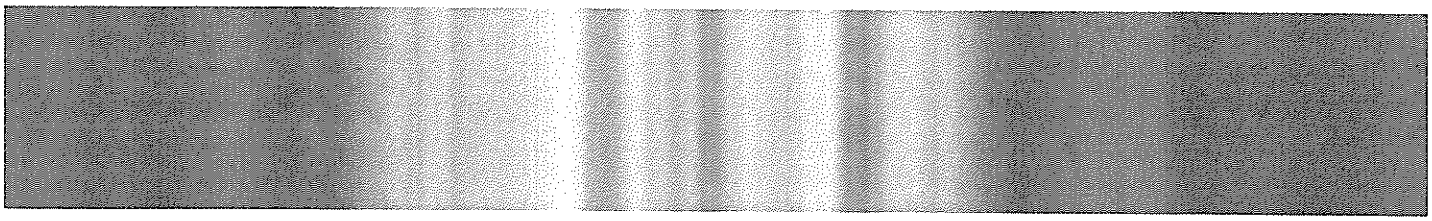
The following rights apply to California residents.

- We share personal information with others outside of Walmart for direct marketing of their products only if we have your affirmative consent (opt in). See *"How Do We Share Your Personal Information Outside Walmart?"*
- We share personal information with other businesses within our corporate family, such as Sam's Club, Vudu, Moosejaw.com, or Hayneedle.com. You may ask us for more information about this sharing and whether it affects you by contacting us at the address below. *See "How Do We Use Your Personal Information?"*

Contact our Customer Service Team or write the Walmart Privacy Office with any questions or comments about this Policy or about how we handle your personal information. The Privacy Office's address is:

Walmart Corporate
Privacy Office, MS #0160
702 SW 8th Street
Bentonville, AR 72716-0160

View the full Walmart Privacy Policy



Walmart

Social

Our Story
Newsroom
Ask Walmart

Global Responsibility
Investors
Suppliers

Walmart Museum

Shop Walmart.com
Shop SamsClub.com

Privacy & Security | Fraud | California Privacy Rights | California Supply Chains Act | Frequently Asked Questions | Contact Us | Policies | Recalls | Terms of Use | Do Not Sell My Personal Information | Request My Personal Information

HB 1680
#56

New Hampshire
Credit Unions

Creating Cooperative Power

COMMITTEE ON COMMERCE AND CONSUMER AFFAIRS
PUBLIC HEARING
JANUARY 23, 2020

STATEMENT IN OPPOSITION
HB 1680

AN ACT RELATIVE TO THE COLLECTION OF PERSONAL INFORMATION BY BUSINESSES

The Cooperative Credit Union Association, Inc. ("Association") is the state credit union trade association, serving 14 federally and state-chartered credit unions that are cooperatively owned by 713,000 consumers as members. On behalf of the New Hampshire credit union movement, the Association opposes HB 1680, *An Act Relative to the Collection of Personal Information by Businesses*, which seeks to expand consumer privacy rights and business obligations.

The New Hampshire credit union community has a longstanding priority to protect the security of member information. The increasing problems arising over the theft of sensitive information resulting from data security breaches is alarming. The frequency of both minor and major data compromises has been growing at a significant rate and has severe consequences on Granite State consumers, credit union members, and the financial institutions which must maintain such information to process payment and other transactions.

New Hampshire credit unions recognize and support the consumer protection goals of HB 1680, and are encouraged by this Committee's focus on this important issue. However, it is the position of the Association that passage of extensive privacy legislation, resulting in a patchwork of state statutory mandates in this area, is not ripe or warranted at this time.

The provisions of HB 1680 are reflective of the provisions of the California Consumer Privacy Act ("CCPA") before key amendments were made to the CCPA. As states consider privacy legislation in the previous and current sessions, the majority of the amendments made to the CCPA are included. For example, the CCPA amendments include an employment exemption for personal information a business collects about an individual acting as a job applicant, employee, officer, or other role. In general, the CCPA amendments are important, make technical and operational fixes, and should be included as a minimum starting point for privacy legislation in the New Hampshire if and when state legislation advances.

The issue of consumer privacy and the protection of personal financial information is high on the radar of consumers today, and has been an utmost priority of New Hampshire credit unions since their inception. In today's increasingly technological and digital world, the issue presents as a balance between the benefits to consumers of technological advancements, including ease of access to products and services as well as customized and convenient business experiences, and

845 Donald Lynch Blvd., Marlborough, MA 01752-4704 • Tel. 508.481.6755 • 800.842.1242 • Fax: 508.481.3586

the privacy of their personal information. Simultaneously, the businesses that either directly or indirectly come into custody of such information are expected to increase their gatekeeping role while remaining transparent about how such information is used before the consumer.

While today's data privacy concerns are more generally focused on and targeted towards large tech companies such as Facebook, Google, and even international conglomerates such as Huawei, this amplified microscopy on the handling of privacy information increasingly impacts financial institutions, including credit unions, where strict data privacy laws have been in place and successful for decades. These laws establish a framework that balance consumer control over personal information with operational feasibility and data security. Meanwhile, other sectors of the economy have been operating with few or no privacy restrictions, giving rise to the current focus on consumer concerns about the collection, use, and sharing of their personal information.

Current State of Privacy Laws Impacting Credit Unions

The recent passage of broad and all-encompassing laws and regulations such as the General European Data Regulation ("GDPR") and the CCPA have brought these privacy issues into the legislative spotlight and policymakers have taken note, with this Committee as no exception, leading ultimately to the current proposal. The CCPA was passed in 2018 as a sweeping data privacy law, giving California consumers significant expanded rights as to the collection and use of their personal information by businesses.

The CCPA layers on top of existing state and federal financial information privacy laws. As part of the passage of the CCPA, promulgating regulations were to be adopted to further the Act's purposes. After a series of public hearings and a public comment period, regulations remain in the proposal stage and have not yet been finalized.

Additionally, New Hampshire credit unions continue to be responsible stewards of members' financial information. Credit unions have long been subject to the strictest of laws requiring privacy protections for personal financial information. Credit unions are subject to the federal provisions of the Gramm-Leach-Bliley Act ("GLBA") codified at 15 U.S.C. §§6801-6809, including the Financial Privacy Rule. Compliance with the GLBA is mandatory, and financial institutions are required to have a policy in place to protect the financial information of their consumers regardless of whether that financial institution discloses nonpublic information or not.

Additionally, New Hampshire credit unions are subject to the provisions of the Fair Credit Reporting Act ("FCRA"), the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), and are governed by the rules and regulations of the National Credit Union Administration ("NCUA") relative to the safeguarding of member information. 12 C.F.R. Part 748. Both state and federal regulators examine credit unions for compliance with GLBA, FCRA, and NCUA rules and ensure that adequate measures are in place to protect consumers' financial information during regular examinations.

New Hampshire credit unions support cohesive and balanced privacy protections for credit unions and members. Strict and clear provisions are necessary for credit unions to rely upon for entities or information covered by existing financial information privacy laws such as the GLBA

and FCRA. New Hampshire credit unions are concerned that varying state, federal, and international data privacy laws will create a patchwork of data privacy standards, and further complicate existing compliance efforts for credit unions serving consumers in multiple jurisdictions. It is the position of the Association, therefore, that additional state legislation in this area is therefore unnecessary and unwarranted.

Analysis and Impact of HB 1680

The thrust of this pending proposal is to establish statutory parameters around the protection of consumers' personal information by businesses involved in the collection or sale of such information. The proposal addresses required disclosures to consumers, methods of such disclosure, necessary form of disclosure notices, consumer rights to request deletion of personal information, exceptions to the rule, a private right of action, and necessary rulemaking. HB 1680 specifically would grant consumers the right to request that a business disclose the type of personal information it collects, the purpose for which it is collected, and the categories of third parties with which it is shared. Additionally, the bill authorizes consumers to opt out of the sale of their personal information. The bill also establishes a private right of action and provides for further enforcement by the attorney general.

While such terms as "consumer," "personal information," and "business" are defined in the proposed legislation, initial concerns with HB 1680 relate to potentially incomplete or unclear definitions. For example, the definition of a "consumer" includes a natural person resident of New Hampshire. "Resident" or "residency," a specifically defined legal construct by jurisdiction, is undefined. If an individual consumer applies for credit union membership and provides an out-of-state address, it is impossible to determine whether that individual is in fact a resident of New Hampshire or another state. It is not a reach to contemplate operational difficulties in this area for businesses who only have access to the information that is provided to them by the consumer, resulting in a compliance impossibility for delivering the required disclosures.

Additionally, while provisions relating to data level exemptions for "personal information collected, processed, sold, or disclosed" and deletion of data, such as the exception to maintain data for a legal obligation purpose or if it is necessary to perform a service requested by the member, are helpful, they are in contrast to requirements under the GDPR. This contrast again presents operational difficulties for credit unions seeking to comply with all applicable rules and regulations.

Conclusion

Overall, credit unions remain concerned with the adoption of a patchwork, state-by-state privacy framework, and urge the Committee to consider the current state of privacy legislation both nationwide and internationally, as well as well-established statutory requirements already in place for financial institutions, and reconsider the need for such broad-reaching privacy legislation in the Granite State at this time.

In consideration of the above points, New Hampshire credit unions oppose HB 1680 and its proposed privacy provisions. The Association appreciates the opportunity to provide input to the Committee, and respectfully requests that the Committee reconsider advancement of HB 1680 at this time.

HB 1680
#5b

SERVICE CREDIT UNION

Corporate Office

3003 Lafayette Road
Portsmouth, NH 03801

January 23, 2020

Commerce and Consumer Affairs Committee
New Hampshire House of Representatives
107 North Main St
Concord, NH 03301

Statement in opposition to HB 1680

Dear Members of the committee,

You have a bill before you, HB 1680, which would enact state-level consumer privacy rights and business obligations regarding notifications to consumers. The drafted bill closely aligns with the California Consumer Privacy Act (CCPA), passed in 2018. As a company already affected by the CCPA, Service Credit Union is not in favor of HB 1680 moving forward at this time. Credit unions and banks are already governed by federal-level privacy standards, a state-by-state approach to privacy regulation will be very challenging for businesses to comply with, and the consumer education around privacy rights is still lacking. We believe member privacy and transparency in information sharing is very important, and we know that these are issues that are going to get a lot of attention in the coming years. However with the CCPA implementing regulations still being finalized, we advise waiting to develop this type of legislation in our state.

The Gramm-Leach-Bliley Act (GLBA) is the main U.S. privacy regulation that governs our credit union today. GLBA requires that we disclose to all our members certain categories of third parties that we share information with and whether or not they can limit this sharing. GLBA also establishes data protection standards; we are required to have a security program that ensures the security and confidentiality of member information. The federal Right to Financial Privacy Act also provides consumers with a layer of confidentiality, preventing financial institutions from sharing their non-public personal information with law enforcement agencies unless very specific conditions are met (such as if the information is legally requested through a subpoena). Due to these existing laws governing member notification and information security, we have time to learn more from the CCPA's implementation process before we tackle this challenging topic in our own state.

Our credit union has branches abroad in Germany which has made us subject to the General Data Protection Regulation (GDPR), which went into effect in May of 2018; this has given us experience with the costs and time associated with implementing new privacy laws. The GDPR is similar in some ways to the CCPA in that it provides consumers with similar rights: the right to deletion, the right to request information, the right to data portability. In order to comply with this law and respond to members who wish to exercise their new rights, our company invested a substantial amount of money into new systems, developing new procedures, expanding our own knowledge on this topic, and ensuring we have controls over member information within our own network; we easily surpassed $100,000 in these efforts, and that is not including

the cost of paying the employees working on this. Implementing this privacy legislation was easily a full time job for two senior staff members for 8 to 12 months. I would anticipate this bill adding a lot of regulatory burden on mid- to large-sized companies which is why it is very important that we take the time to get it right.

To expand on some of the particular issues that arise with privacy regulation, an immediate challenge that businesses face is truly knowing where an individual is a resident. Someone who is temporarily abroad and active in the military may identify as a resident of New Hampshire. For this individual, we may only have their temporary overseas address on file. We would not be able to discern what state this member is a resident of from the information that the individual has provided to us. This creates difficulties in the California-model privacy acts which require a notice *at or before collection of information*. Again, if we are dealing with different standards from different states, this issue only becomes more complex. A privacy rule at the federal level would cover businesses and consumers under one umbrella, versus states developing varying standards.

Another challenge that we already saw in implementing the GDPR is the lack of consumer awareness and understanding of that regulation. Our staff have provided a lot of information and education to our overseas members to help them understand what these new right even mean to them. Similar education will be needed for New Hampshire and other stateside residents. They may be dealing with companies who have different privacy notices for residents of different states, which can become confusing to navigate.

As stated before, the proposed bill before the committee is based on the California Consumer Privacy Act, which has yet to be enacted with implementing regulations and is still being clarified and refined. Our main concerns with this bill moving forward have been presented in the details above; they can be summarized simply in saying that a state-by-state patchwork model of privacy regulations presents a logistical nightmare for the entities with members and customers in multiple states

At this time in the rulemaking process, I recommend that our state refrains from moving forward on this bill and watches the proposed privacy bills at the federal house and senate level as well as how the California model evolves. We can observe their process and then choose to take action after absorbing whatever lessons can be learned in that outcome.

Thank you very much for your time; I would be happy to discuss this topic further and can be reached at 603-430-6955 or at skinnett@servicecu.org.

Sincerely,

Stephanie Kinnett

Stephanie Kinnett
Assistant Vice President of Regulatory Compliance
Service Credit Union

Testimony of
GERARD KEEGAN
CTIA

In Opposition to New Hampshire House Bill 1680

Before the
New Hampshire House of Representatives Commerce and Consumer Affairs Commerce

January 23, 2020

Chair Butler and members of the committee, on behalf of CTIA, the trade association for the wireless communications industry, thank you for the opportunity to testify on consumer data privacy. Consumer privacy is an important issue. Protecting against identity theft, online fraud, and data breaches requires constant vigilance by providers, device manufacturers, app developers, and consumers. The wireless industry works to protect consumer privacy and safeguard your data every day, however, CTIA opposes House Bill 1680.

State legislation that sweeps too broadly could have a negative effect. HB1680 is based on a California law that was hastily passed in 2018, without sufficient consultation with impacted stakeholders, and that contains many ambiguities. California legislators enacted certain amendments last year - some with one-year sunsets to continue work in 2020 and 2021 - and may seek other additional amendments to the law this year. The California Attorney General is also engaged in a rulemaking process to interpret its provisions. In addition, the sponsor of the original law is now proposing a ballot initiative to add further provisions to the law and change other provisions. As such, the California law is a moving target, and attempts to follow California means that we will have the beginning of a patchwork of state laws that will confuse consumers and burden businesses. New Hampshire should not rush to follow California.

HB1680 creates broad access requirements that are in tension with data security principles, as they

may encourage companies to centralize—rather than segregate—consumer data in one location, pool consumer data about particular requesting consumers in one location, and/or maintain consumer data in personally identifiable form, all to be able to comply with consumer requests. These practices inherently carry risks, such as making the data a more attractive target to identity thieves and cybercriminals. They can also be burdensome. In the United Kingdom, a white hat hacker was able to get his fiancée's credit card information, passwords, and identification numbers by making a false request.[1] Similar scenarios will likely happen in California and in New Hampshire if the state enacted HB1680.

It is also unclear how requirements to have consumers delete their data will turn out in practice. These requirements may undermine important fraud prevention activities by allowing bad actors to suppress information. Additionally, there is a concern that bad actors could request deletion of data that would flag them as wrongdoers. Businesses may also have to delete data that will help them track the quality of service or to improve their products.

Moreover, the broad opt-out provisions in the bill may jeopardize the availability or quality of free or low-cost goods and services, which rely on the use of personal data that is subject to safeguards, such as pseudonymization. Online news sites, content providers, and apps are often provided to consumers free of charge because they are supported by advertising. These content providers should not be forced to continue to offer free services to consumers who opt-out of disclosing online identifiers to advertisers. While consumers should always be provided meaningful notice and choice before their personal data is used, that choice should be balanced against the numerous benefits to consumers. Furthermore, the private right of action included in the bill will expose businesses – both large and small – to costly litigation.

---

[1] Leo Kelion, *Black Hat: GDPR privacy law exploited to reveal personal data*, BBC (August 8, 2019).

While it is clear that these provisions create risk for consumers and cost for businesses, it is not as clear that their benefits outweigh these risks. In Europe, consumers get reams and reams of data when they submit access requests, and they are constantly bombarded with pop-up windows as they browse the internet. Does this enhance their privacy or make their data more secure?

The stakes involved in consumer privacy legislation are high. Being too hasty to regulate could have serious consequences for consumers, innovation, and competition. Regulation can reduce the data that is available for research and for promising new solutions by putting too many constraints on the uses and flow of data. We are starting to see indications of this in Europe, where sweeping new privacy regulations took effect in 2018 and investment in EU technology ventures has declined.[2] Similarly, the United States leads Europe in the development of Artificial Intelligence, and experts believe that Europe's new data protection laws will increase this competitive disadvantage.[3]

Any new state privacy law will contribute to a patchwork of regulation that will confuse consumers and burden businesses that operate in more than one state. Should the data of consumers who live in border cities and towns like Nashua or Hanover be treated differently when they cross the New Hampshire border? Should businesses with operations in multiple states segregate the data of New Hampshire citizens?

Much of the focus in the privacy debate thus far has been on compliance costs and the impact on larger companies, but regulation impacts business of all sizes. As part of the California Attorney General's

---

[2] Jia, Jian and Zhe Jin, Ginger and Wagman, Liad, "The Short-Run Effects of GDPR on Technology Venture" *Investment, National Bureau of Economic Research* (November 2018).
[3] Daniel Castro and Eline Chivot, *Want Europe to have the best AI? Reform the GDPR, IAPP Privacy Perspectives* (May 23, 2019).

regulatory process, the office commissioned an economic impact study.[4] The study found that the total cost of initial compliance with the law would be approximately $55 billion or 1.8% of the state's gross domestic product.[5]

In addition, the study found that any business that collects personal information from more than 137 consumers or devices a day would meet the law's thresholds - the same thresholds as HB1680 - while between 50 to 75% that earn less than $25 million in revenues will have to comply with the law.[6] It also found that "[s]mall firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises."[7] These compliance costs include new business practices, operations and technology costs, training requirements, recordkeeping requirements, and other legal fees. It goes on to further state that "conventional wisdom may suggest that stronger privacy regulations will adversely impact large technology firms … however evidence from the EU suggests the opposite may be true."[8] The study found that many smaller firms have struggled to meet compliance costs. The EU regulation of privacy seems to have strengthened the position of the dominant online advertising companies, while a number of smaller online services shut down rather than face compliance costs.

The scope of the law will likely impact smaller companies and firms. For example, a company or firm that may not meet the applicable thresholds may still be required to comply with the law if the company processes data for an entity that must comply. In that instance, an IT processing firm that

---

[4] *See* Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, Berkeley Economic Advising and Research, LLC (August 2019).
[5] *Id* at 11.
[6] *Id* at 11 and 20.
[7] *Id* at 31.
[8] *Id* at 31.

processes consumer data for a larger business must be capable of responding to access and data deletion requests.

Consumer privacy is an important issue. State-by-state regulation of consumer privacy will create an unworkable patchwork that will lead to consumer confusion. That is why CTIA strongly supports ongoing efforts within the federal government to develop a uniform national approach to consumer privacy. The stakes involved in consumer privacy legislation are high. Taking the wrong approach could have serious consequences for consumers, innovation, and competition. Moving forward with broad and sweeping state legislation would only complicate federal efforts while imposing serious compliance challenges on businesses and ultimately confusing consumers. As we support a comprehensive federal privacy law, we oppose further fragmentation that would also arise from passage of HB1680.

As mentioned, the only state to enact a comprehensive privacy law is California. This law just took effect three weeks ago, and it is still a moving target: the legislature recently passed amendments, the Attorney General has yet to promulgate final regulations, and a new ballot initiative would make further substantive changes to the law. It is simply not clear that we have found a good formula for regulating privacy. Accordingly, we caution New Hampshire and any state from rushing to follow California down this unproven, untested, and unknown path. As such, CTIA opposes HB1680 and would urge the committee to report that the bill is Inexpedient to Legislate Thank you for the opportunity to testify today.

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

INTERNET COALITION

NetChoice

STATE PRIVACY AND SECURITY COALITION

January 23, 2020

Rep. Edward Butler
House Committee on Commerce and Consumer Affairs
New Hampshire State Legislature
33 North Street
Concord, NH 03301

Re: HB 1680- Collection of Personal Information by Businesses

Dear Chair Butler and members of the Committee:

On behalf of the hundreds of the nation's leading technology and innovation companies our organizations represent, the associations listed below write to express our opposition to HB 1680 (Muscatel) pertaining to the collection of personal information by businesses. We appreciate the desire of the Sponsor to address consumer privacy protections. However, we urge New Hampshire to support federal efforts to create a comprehensive privacy law instead of contributing to a growing patchwork of state legislation.

As you are likely aware, on June 28, 2018, California enacted California Consumer Privacy Act (CCPA), a well-intentioned, but materially flawed new law, that seeks to protect the data privacy of technology users and others by imposing new rules on companies that gather, use, and share personal data. Unfortunately, CCPA was rushed through the California legislative process to avoid a potential ballot fight. Due to a hard deadline to withdraw the initiative, there was little time for substantive policy negotiations about a law that has a tremendous impact on businesses not only in California but across the nation. This has resulted in a law that was enacted just 18 months ago being amended via eight different legislative vehicles. And it is still not final.

While California has worked to address some of problematic provision included in the initial version of CCPA, many challenges remain. One example of a problematic provision is the CCPA's reference to households and devices in the definition of personal information. This reference run counter to the CCPA's privacy protective goals and should be removed. As drafted, one member of a household – whether they are an abusive spouse or a roommate – has the ability

to request access to all of the specific pieces of personal information – including credit card account information, precise geolocation data, or even shopping records – about another member of their household. This has anti-privacy consequences for mundane, everyday behavior, such as requesting information from a grocery delivery store which could inadvertently expose a household member's purchase of birth control or a pregnancy test. As another example, if one household member makes a request to delete all data associated with a household, another household member would be subsequently unable to access their household information. This is just one example of many.

An additional problem with the legislation as drafted is that HB 1680 is nearly identical to the original version of CCPA which passed the Legislature in 2018. As such, the bill does not conform to the most recent version of CCPA today, which is likely to significantly change at least twice between now and November of 2020. In addition to amendments that passed the legislature last year, the Attorney General has engaged in a rulemaking procedure which may reinterpret key provisions of the law and add new obligations. Further complicating matters, this fall the sponsor of the 2018 ballot initiative has filed a new privacy ballot initiative, to correct perceived errors in the law and impose new obligations on businesses. This suggests that the privacy debate will continue to change over the next several years, and the true impact of the CCPA will not be known for some time. It is clear that California is not a workable model for other states to pass at this time.

Our organizations are also concerned with a patchwork approach that imposes different privacy and security obligations in different states. Privacy laws can be difficult and costly for some of the largest businesses to comply but it's even worse for small businesses and start-ups. If you also factor in multiple states with multiple different laws, the end result can be crippling. The California Attorney General's office estimated that initial, direct compliance costs for CCPA to be $55 billion, with up to another $16 billion over the next decade (2020-30), depending on the number of California businesses coming into compliance, and with smaller firms likely facing a disproportionately higher share of compliance costs relative to larger enterprises. These numbers should be a warning to lawmakers as they consider any data privacy legislation.

Our organizations ask you to consider holding HB 1680 as California continues to implement CCPA. It is important to wait and learn of any unintended consequences that California will likely face as the first state to pass consumer data privacy legislation. Additionally, New Hampshire should avoid creating a separate and conflicting privacy law that would only increase compliance costs on businesses and start-ups.

Thank you for the opportunity to weigh in on HB 1680 and as the Committee deliberates, please consider our organizations and our member companies a resource. Thank you in advance for your consideration on these matters. Please do not hesitate to reach out with any questions.

Sincerely,

Christina Fisher
Executive Director, Northeast
TechNet
cfisher@technet.org
508-397-4358

Tammy Cota, Executive Director
Internet Coalition
802-279-3534
tammy@theinternetcoalition.com
www.theinternetcoalition.com

Andy Kingman,
Senior Managing Attorney, DLA Piper
General Counsel, State Privacy & Security Coalition
(774) 313-9543
Andrew.Kingman@dlapiper.com

Carl Szabo, Vice President and General Counsel
Netchoice
202-420-7485
cszabo@netchoice.org

Business and Industry Association
New Hampshire's Statewide Chamber of Commerce

122 North Main Street, Concord, NH 03301
Tel: 603.224.5388 • Fax: 603.224.2872 • Web: www.BIAofNH.com

Testimony of Kevin Flynn
Business and Industry Association
HB 1680 Relative to the collection of personal information by businesses
January 23, 2020

Dear Mr. Chair and members of the House Commerce Committee:

I am Kevin Flynn, Director of Communications and Public Policy at the Business and Industry Association, New Hampshire's statewide chamber of commerce. I am here today to convey BIA's opposition to HB 1680.

HB 1680 would make New Hampshire an outlier, creating laws that change the way e-commerce, digital data retention, and consumer internet usage is done here versus other states. This bill has the potential to be onerous and costly to comply with, impractical in its application, and confusing for businesses and consumers alike.

The language of HB 1680 seems to take cues from the new California Consumer Protection Act. While it appears to be drafted to target only large businesses, it will very likely encompass most small- and medium-sized businesses that retain customer data or rely on the internet for business operations. It would take fewer than 150 web visits or 14 credit card transactions an hour to fall within the parameters of the bill.

According to the California Department of Finance, the estimated cost of CCPA compliance to the private sector in their state will be $55 billion, with an estimated cost of $50,000 in compliance costs per business regardless of their size. If implemented here, such compliance costs would be a drag on New Hampshire's economy. Also, creating a private right of action is costly and unnecessary.

In conclusion, we believe there shouldn't be a patchwork of different regulations businesses and consumers must navigate when they use the internet in New Hampshire versus other states. HB 1680 will make it harder for businesses in New Hampshire to operate in a manner both they and their customers are accustomed.

Thank you for your consideration of BIA's position on this legislation.

(18)

ACLI
Financial Security for Life.

January 23, 2020

The Honorable Ed Butler
Chair
House Committee on Commerce & Consumer Affairs
The New Hampshire General Court
LOB Rm 202
107 North Maine Street
Concord, New Hampshire 03301

RE: Opposition to ***HB 1680 – An Act Relative to the Collection of Personal Information by Business***

Dear Chairman Butler and Members of the Committee:

These comments are submitted on behalf of the American Council of Life Insurers. The American Council of Life Insurers (ACLI) is a national trade association with 209 member companies licensed to do business in New Hampshire.

The insurance industry is a consumer privacy leader in support of clear obligations in the appropriate collection, use and sharing of sensitive personal information. The financial services sector has and continues to respect consumer privacy. Insurers have ably managed consumers' sensitive medical and financial data for well over a century. Insurers must collect and use personal information to perform essential business functions – for example, to underwrite applications for new insurance policies, to pay claims submitted under these policies, and to provide longevity protection through retirement products. And our industry's commitment to appropriate use and safeguarding of consumer information has helped establish what has become a comprehensive federal and state regulatory framework governing the use and disclosure of personal information for the insurance industry. Therefore, the financial services industry would be uniquely affected by the establishment of new general privacy requirements at the individual state level. This proposal would add to the mix of existing privacy laws for insurers additional complexities and expenses of implementation and will inevitably result in conflicting scopes, definitions, notice requirements and consumer rights.

Consumers and companies need privacy requirements that are consistent and equivalent across state borders, provide equal protections to all consumers regardless of where they are located, support growth and innovation, and which provide legal transparency. Differing privacy standards will lead to consumer confusion, differing consumer rights and protections, obstruct the flow of information, and impede interstate commerce. Differing state privacy approaches are confusing and frustrating to consumers facing divergent rights to control over their personal information based upon where they live or with whom they are doing business. These conflicts must be taken into consideration as you work to develop comprehensive obligations regarding the use of personal information which applies equally and uniformly to all industries.

There are complexities to instituting the wholesale change contemplated by this proposal. One essential question to ask as you review this proposal is how the current financial services privacy regulatory system will be harmonized with new comprehensive law?

House Bill 1680 is modeled after the California Consumer Privacy Act of 2018 (CCPA), a comprehensive data privacy law which grants consumers sweeping new rights to govern use of their personal information. The California law was passed in 4 days, behind the scenes, with no public input. It was rushed and the result is evident. Some of the purported consumer protection disclosure requirements render consumers' personal information even more vulnerable. The severe impact to entities forced to completely overhaul their business practices in order to comply with the law was not given much, if any, thought. As a result, there were nearly 40 bills proposed in California last session by various interest groups to attempt to fix the law. CCPA was recently amended during the final hours of the California legislative session. And yet, both legislators and the consumer advocate proponents of the legislation are seeking additional significant changes both by a ballot initiative as well as legislation in 2020.

House Bill 1680 does not include any of the 2019 business to business personal information exemptions and would need an employment exemption for personal information a business collects during the employment process and throughout employment process. This proposal also does to include any of the California Privacy Rights Act of 2020 amendments which are critical to improving the bill. Finally, it includes a private cause of action for data breach. We recommend eliminating this provision as a private right of action undermines agency enforcement, results in disparate outcomes for consumers and hinders innovation and consumer choice.

New Hampshire may want to consider taking action similar to a recently proposed resolution in Arizona, *Resolution 2013*, which advocates for a single, comprehensive federal standard for consumer data privacy regulation.

We are committed to working with the committee on trying to solve some of these complexities to find solutions that protect consumer privacy and, at the same time, enable innovation and business growth and opportunities for the Commonwealth.

Camille Simpson
Regional Vice President, State Relations
American Council of Life Insurers

(13)

NH Bankers ASSOCIATION

HB 1680, relative to the collection of personal information by businesses.
Testimony of the New Hampshire Bankers Association
Presented by Ryan Hale, Vice President/Government Relations
House Commerce and Consumer Affairs Committee
Thursday, January 23, 2020

Chairman Butler and honorable members of the House Commerce and Consumer Affairs Committee, my name is Ryan Hale and I'm Vice President, Government Relations for the NH Bankers Association. The NH Bankers represents 37 member banks which employ nearly 6,000 employees.

I'm here today to express our concerns with HB 1680, relative to the collection of personal information by businesses, as currently written. HB 1680 would establish a New Hampshire consumer privacy statute similar to the recently enacted California Consumer Privacy Act or CCPA.

HB 1680 as well as the CCPA creates a statutory framework which is similar in nature to existing federal law for financial institutions that require businesses to protect personal information it collects as well as providing consumer disclosures.

Protecting personal information is something banks feel strongly about and have been doing for many years. It's an area banks are constantly scrutinized by regulators during regular examinations as well as by law makers at both the state and federal level. Currently, banks must comply with a long list of federal privacy and data protection laws including the Gramm-Leach Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA) to name a few.

While we do appreciate the sponsors attention to this issue and his attempt to carve out banks and financial institutions, the NH Bankers still have concerns.

It remains unclear to us if banks are entirely exempt. The exception in the bill only applies to information that is collected, processed, sold, or disclosed pursuant to GLBA. However, that language does not align with the scope of GLBA, which instead, regulates a bank's use and treatment of nonpublic personal information. Accordingly, it creates ambiguity regarding the full extent of the exemption.

More specifically, the issue banks may run into with this language is identifying what personal information they've collected falls under the GLBA exception and what information would not. The vagueness of this language could force banks to inventory the personal information they collect likely causing a significant increase in cost of compliance.

We also have questions on whether or not this would apply to our smallest of institutions. The definition of businesses would likely only apply to our largest of institutions. However, with the current exception, banks are exempt from the definition of businesses. Does that mean even our smallest of institutions could be subjected to certain provisions of this bill? Does that mean the smallest banks could be subjected to a private right of action? Again, the exception is unclear to us.

It's important to point as we did last week in our testimony on HB 1588, since 2010 New Hampshire has lost 33% of its banks due to mergers and acquisitions. This rate is much higher than the national rate of 25%. One

NH Bankers ASSOCIATION

of the main reasons driving banks to mergers and acquisitions is the continued increase in cost of compliance. By adding more in some ways duplicative regulatory burdens on already highly regulated industry could likely force more state-chartered banks into the arms of national banks reducing local option for New Hampshire consumers.

I do understand the sponsor is looking to change this bill to a study committee and take a deep dive into the issue. As an industry that has been on the front lines of protecting personal information for years, we would be more than happy to work with the study committee as they look to address the issue.

I thank the Committee for considering our concerns and I'm happy to take questions at this time.

February 21, 2020 INDRUK (1)

HB 1680 – Amendment 2020-0560h

What does the amendment do?:

The amendment replaces the introduced text in its entirety and establishes vital privacy protections for the customers of broadband internet service providers (ISPs). In essence, the amendment empowers consumers to control how their personal information is used- thus aligning consumer expectations and business practices. These protections mirror those put in place, after lengthy comment and review, by the FCC in 2016[1]. As the FCC stated in the final rule:

> *The privacy framework … focuses on transparency, choice, and data security, and provides heightened protection for sensitive customer information, consistent with customer expectations.*
>
> *These rules do not prohibit broadband providers from using or sharing customer information, but rather are designed to protect consumer choice while giving broadband providers the flexibility they need to continue to innovate.*

Unfortunately, these vital consumer protections were overturned by Congress in 2017[2]. As such, it is now up to this body to protect NH consumers.

Specifically, this amendment:

1) Defines "Consumer Personal Information" (CPI), which is a special class of information deserving of heightened- opt in-protections: CPI includes:
    a. Personally identifying information, including but not limited to:
        i. A customer's name
        ii. Billing information
        iii. Social Security Number
        iv. Billing address
        v. Demographic data
    b. Information from a consumer's use of broadband internet access service, including but not limited to:
        i. Web Browsing history
        ii. Application usage history
        iii. Precise Geolocation Data
        iv. Financial Information
        v. Health Information
        vi. Information pertaining to the customer's children
        vii. Device identifiers, including MAC or IP address

---

[1] 81 FR 87274: https://www.govinfo.gov/content/pkg/FR-2016-12-02/pdf/2016-28006.pdf

[22] S.J.Res.34- 115th Congress (2017-2018): https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34/text

viii. The content of communication

ix. The origin and destination of IP addresses

2) Prevents the use, disclosure, sale or granting of access to "customer personal information", except in the following circumstances:

   a. If the customer gives express, affirmative consent for such use, disclosure, sale or access

   b. For the purpose of providing the service from which the information was derived or for the services necessary to the provision of such service

   c. To comply with a lawful court order

   d. To initiate, render, bill for, and collect payment for broadband internet access service

   e. To protect users from fraudulent, abusive or unlawful use of or subscription to such services

   f. To provide geolocation information:

      i. For the purpose of responding to a customer's call for emergency services

      ii. To a provider of information or database management services solely for the purpose of assisting in the delivery of emergency services in response to an emergency.

3) Allows for the use, disclosure, sale or granting of access to information that is NOT customer personal information, unless the customer opts out. That is, any information that is NOT CPI – and thus deserving of special heightened protections—can be used unless the customer revokes permission (opts OUT).

4) Requires providers to take reasonable measures to protect customer personal information from unauthorized use, disclosure or access.

5) Requires clear, conspicuous and non-deceptive notice of the provider's obligations and customer's rights. The notice must be provided to all customers at the point of sale and made available on the provider's public website.

6) Prevents discrimination against customers who exercise their privacy rights under this law. As the FCC noted in the 2016 privacy rule:

   a. ..."take-it-or-leave-it" practices offer no choice to consumers. The record supports our finding that such practices will harm consumers, particularly lower-income customers...We therefore conclude that prohibiting such practices will ensure that consumers will not have to trade their privacy for broadband services."

7) Establish a committee to study:

   a. The ways in which personal information is digitally collected, stored, disclosed or used for commercial purposes in the state- andy by which commercial entities

   b. How other states provide greater consumer privacy protection

   c. How NH can strengthen consumer privacy protections

INDRUK (1)

FCC findings- ISP (BIAS) privacy order 2016

The FCC's 2016 Internet Privacy Rule[1]was issued after careful analysis of public comment, including comments from ISPs and related trade associations. The findings presented in the final ruling reflect this analysis and present a thorough defense of each provision of that order. As many components of that order are incorporated amendment 0560h, that analysis is instructive. Below are pertinent excerpts from the final rule:

Why ISP customers require special protections:

- "Internet access is a critical tool for consumers—it expands our access to vast amounts of information and countless new services. It allows us to seek jobs and expand our career horizons; find and take advantage of educational opportunities; communicate with our healthcare providers; engage with our government; create and deepen our ties with family, friends and communities; participate in online commerce; and otherwise receive the benefits of being digital citizens."
- "Broadband providers provide the "on ramp" to the Internet. These providers therefore have access to vast amounts of information about their customers including when we are online, where we are physically located when we are online, how long we stay online, what devices we use to access the Internet, what Web sites we visit, and what applications we use."
- Furthermore, as Mozilla explains, "[b]ecause these are paid services, [the broadband provider has] the subscriber's name, address, phone number and billing history. The combination gives ISPs a very unique, detailed and comprehensive view of their users that can be used to profile them in ways that are commercially lucrative."
- "A number of broadband providers, their associations, as well as some other commenters argue that because broadband providers are part of a larger online eco-system that includes edge providers, they should not be subject to a different set of regulations. These arguments ignore the particular role of network providers and the context of the consumer/BIAS provider relationship...
- We disagree with commenters that argue that BIAS providers' insight into customer online activity is no greater than large edge providers because customers' Internet activity is "fractured" between devices, multiple Wi-Fi hotspots, and different providers at home and at work. As commenters have explained, "customers who hop between ISPs on a daily basis often connect to the same networks routinely," and as such, over time, "each ISP can see a substantial amount of that user's Internet traffic."
- ...users have much more control over tracking by web third parties than over tracking by BIAS providers. A range of browser extensions are largely effective at blocking prominent third parties, "but these tools do nothing to stop data collection on the wire."
- Web browsing and application usage history, and their functional equivalents are also sensitive within the particular context of the relationship between the customer and the BIAS provider, in which the BIAS provider is the on-ramp to the Internet for the subscriber and thus sees all domains and IP addresses the subscriber visits or apps he or she uses while using BIAS. This is a different role than even the large online ad networks occupy
- ...the record reflects that BIAS providers are not, in fact, the same as edge providers in all relevant respects. In addition to having access to all unencrypted traffic that passes between the user and edge services while on the network, customers' relationships with their broadband provider is different from those with various edge providers, and their expectations concomitantly differ.
- While the knowledge of any one fact from a customer's online history (the use of an online app) may be known to several parties (including the BIAS provider, the app itself, the server of an in-app advertisement),

---

[1] 81 FR 87274
https://www.federalregister.gov/documents/2016/12/02/2016-28006/protecting-the-privacy-of-customers-of-broadband-and-other-telecommunications-services

the BIAS provider has the technical ability to access the most complete and most unavoidable picture of that history.

- In addition, consumers have a choice in deciding each time whether to use—and thus reveal information—to an edge provider, such as a social network or a search engine, whereas that is not an option with respect to their BIAS provider when using the service.
- ...as stated in the 2016 Broadband Progress Report, approximately 51 percent of Americans still have only one option for a provider of fixed broadband at speeds of 25 Mbps download/3 Mbps upload.
- "Based on our review of the record, we reaffirm our earlier finding that a broadband provider "sits at a privileged place in the network, the bottleneck between the customer and the rest of the Internet"—a position that we have referred to as a gatekeeper. As such, BIAS providers can collect "an unprecedented breadth" of electronic personal information."
- We find that because broadband providers are able to view vast swathes of customer data, customers must be empowered to decide how broadband providers may use and share their data.

Sensitive Data:

General categories of sensitive data:

- For purposes of the sensitivity-based customer choice framework we adopt today, we find that sensitive customer PI includes financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, application usage history, and the functional equivalents of web browsing history or application usage history.
- "The 2016 Pew study, noted by a number of commenters in the record, found that large majorities of Americans considered Social Security numbers, health information, communications content (including phone conversations, email, and texts), physical locations over time, phone numbers called or texted, and web history to be sensitive. Each of these categories has a clear and well attested case in the record and in federal law for being considered sensitive."

Personally Identifiable Information:

- We define personally identifiable information, or PII, as any information that is linked or reasonably linkable to an individual or device. Information is linked or reasonably linkable to an individual or device if it can reasonably be used on its own, in context, or in combination to identify an individual or device, or to logically associate with other information about a specific individual or device.

Browsing history

- "Browsing history can easily lead to divulging other sensitive information, such as when and with what entities she maintains financial or medical accounts, her political beliefs, or attributes like gender, age, race, income range, and employment status. More detailed analysis of browsing history can more precisely determine detailed information, including a customer's financial status, familial status, race, religion, political leanings, age, and location.
- The wealth of information revealed by a customer's browsing history indicates that it, even apart from communications content, deserves the fullest privacy protection.
- By treating all web browsing data as sensitive, we give broadband customers the right to opt in to the use and sharing of that information, while relieving providers of the obligation to evaluate the sensitivity and be the arbiter of any given piece of information.

FCC findings- ISP (BIAS) privacy order 2016

Precise Geolocation:

- Real-time and historical tracking of precise geo-location is both sensitive and valuable for marketing purposes due to the granular detail it can reveal about an individual. Such data can expose "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." In some cases, a BIAS provider can even pinpoint in which part of a store a customer is browsing. The FTC has found that precise geo-location data "includ[es] but [is] not limited to GPSbased, WiFi-based, or cell-based location information."

Communications:

- Like financial and health information, Congress recognized communications as being so critical that their content, information about them, and even the fact that they have occurred, are all worthy of privacy protections. This finding is strongly supported by the record, and consistent with FTC guidance

Applications use:

- A customer's web browsing and application usage history frequently reveal the contents of her communications, but also constitute sensitive information on their own— particularly considering the comprehensiveness of collection that a BIAS provider can enjoy and the particular context of the BIAS provider's relationship with the subscriber.
- A customer using ride-hailing applications, dating applications, and even games will reveal information about his personal life merely through the fact that he uses those apps, even before the information they contain (his location, his profile, his lifestyle) is viewed.

Devices:

- We agree with the FTC staff that "[a]s consumer devices become more personal and associated with individual users, the distinction between a device and its user continues to blur." The Digital Advertising Alliance likewise recognizes the connection between individuals and devices, stating in its guidance that information "connected to or associated with a particular computer or device" is identifiable.
- As the Supreme Court has observed, "[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context."

Why IP addresses must be included:

- ..."a customer's IP address and MAC address each identify a discrete customer and/or customer device by routing communications to a specific endpoint linked to the customer. Information does not need to reveal an individual's name to be linked or reasonably linkable to that person. A unique number designating a discrete individual—such as a Social Security number or persistent identifier—is at least as specific as a name. In many cases, a unique numerical identifier will be more specific than the person's actual name....MAC addresses, IP addresses, and other examples of PII do not need to be able to identify an individual in a vacuum to be linked or reasonably linkable. BIAS providers can combine this information with other information to identify an individual"
- We agree with those commenters that argue that the IP addresses a customer uses and those with which she exchanges packets constitute CPNI because both source and destination IP addresses relate to the destination of use of a telecommunications service; one links to the destination for inbound traffic while the other links to the destination for outbound traffic. IP addresses are also frequently used in geo-location.
- ...the domain names and IP addresses may contain potentially detailed information about the type, form, and content of a communication between a user and a Web site. In some cases, this can be extremely

revealing: For instance, query strings within a URL may include the contents of a user's search query, the contents of a web form, or other information.

Encryption:

- "...even with encryption, by virtue of providing BIAS, BIAS providers maintain access to a significant amount of private information about their customers' online activity, including what Websites a customer has visited, how long and during what hours of the day the customer visited various Web sites, the customer's location, and what mobile device the customer used to access those Web sites. Moreover, research shows that encrypted web traffic can be used to infer the pages within an encrypted site that a customer visits, and that the amount of data transmitted over encrypted connections can also be used to infer the pages a customer visits."
- BIAS providers' inability to access encrypted content is irrelevant; what matters is the information the BIAS providers can access. Moreover, even when traffic is encrypted, some content may remain visible or inferable to the provider.
- We recognize that sophisticated monitoring techniques have blurred the line between content and metadata, with metadata increasingly being used to make valuable determinations about users previously only possible with content.
- While the record indicates that BIAS providers have a less granular view of encrypted web traffic than unencrypted, it does not change the breadth of the carrier's view or the fact that it acquires this information by virtue of its privileged position as the customer's conduit to the internet. Nor does it change the fact that this still constitutes a record of the customer's online behavior, which, as noted above, can reveal details of a customer's life even at the domain level

Opt-in/Opt-out protections:

- The record demonstrates that customers expect that their sensitive information will not be shared without their affirmative consent, and sensitive information, being more likely to lead to more serious customer harm, requires additional protection. For instance, the FTC recognizes that consumer expectations drive increased protections for sensitive information. We find that requiring opt-in approval for the use and sharing of sensitive customer PI reasonably balances burdens between carriers and their customers.
- If a carrier's uses or sharing of customers' sensitive personal information benefits those customers, the customer has every incentive to make that choice, and the carrier has every incentive to make the benefits of that choice clear to the customer.
- The opt-in requirements we adopt today provide telecommunications customers control over how their sensitive customer PI can be used for purposes besides those essential to the delivery of service.
- ...we conclude that opt-out directly and materially advances the government's interest that a customer be given an opportunity to approve (or disapprove) uses of his non-sensitive customer PI by mandating that carriers provide prior notice to customers along with an opportunity to decline the carriers' requested use.
- We find that requiring opt-in approval for the use and sharing of sensitive customer PI is a narrowly-tailored means of advancing the Commission's interests in protecting the privacy of sensitive customer PI, and in enabling customers meaningful choice on the use and sharing of such sensitive customer PI.
- ...we conclude that an opt-out regime for use and sharing of sensitive customer PI would not materially and directly advance the government's interest in protecting customer privacy because it would not

adequately address customers' expectations that their sensitive customer PI is not used without their affirmative consent.

Non-discrimination:

- ..."take-it-or-leave-it" practices offer no choice to consumers. The record supports our finding that such practices will harm consumers, particularly lower-income customers
- Until recently, for example, to participate in AT&T's GigaPower Premium Offer (i.e., to receive the fixed broadband service GigaPower at a lower cost), customers had to opt in to AT&T Internet Preferences. Under AT&T's Internet Preferences, "you agree to share with us your individual browsing, like the search terms you enter and the Web pages you visit, so we can tailor ads and offers to your interests." AT&T explained that "AT&T Internet Preferences works independently of your browser's privacy settings regarding cookies, do-not-track and private browsing" and that "[i]f you optin to AT&T Internet Preferences, AT&T will still be able to collect and use your Web browsing information independent of those settings."

Disclosure:

- Recognizing the fundamental importance of transparency to enable consumers to make informed purchasing decisions, we require carriers to provide privacy notices that clearly and accurately inform customers about what confidential information the carriers collect, how they use it, under what circumstances they share it, and the categories of entities with which they will share it.

- Customer notification is also among the least intrusive and most effective measures at our disposal for giving consumers tools to make informed privacy decisions. In fact, it is only possible for customers to give informed consent to the use of their confidential information if telecommunications carriers give their customers easy access to clear and conspicuous, comprehensible, and not misleading information about what customer data the carriers collect; how they use it; who it is shared with and for what purposes; and how customers can exercise their privacy choices.

- Customers must have access to information about the personal data that a BIAS provider or other telecommunications carrier collects, uses, and shares, in order to make decisions about whether to do business with that provider, and in order to exercise their own privacy decisions.

- Absent such notice, the broad range of data that a provider is capable of gathering by virtue of providing service could leave customers with only a vague concept of how their privacy is affected by their service provider. We also agree with the FTC that disclosing this information "provides an important accountability function," as disclosure of this information "constitute[s] public commitments regarding companies' data practices." To enable customers to exercise informed choice, and to reduce the potential for confusion, misunderstanding, and carrier abuse, we find that a carrier's privacy notices must accurately describe the carrier's privacy policies with regard to its collection, use, and sharing of its customers' data.

- "Requirements to include purely factual and uncontroversial information in commercial speech are constitutional so long as they are reasonably related to the government's substantial interest in protecting consumers. The notice requirements we adopt here, just like the notice requirements in the CPNI rules before them and like numerous notice and labeling requirements before, require only that companies provide factual and uncontroversial information to consumers."

Preemption:

- "We agree with the Pennsylvania Attorney General that it is important that we not "undermine or override state law providing greater privacy protections than federal law," or impede the critical privacy protections states continue to implement."
- See also *Mozilla v FCC*[2] (2019) in which the DC dist. court vacated an attempt by the FCC under current leadership to preempt state broadband regulation:
    - "Not only is the Commission lacking in its own statutory authority to preempt, but its effort to kick the States out of intrastate broadband regulation also overlooks the Communications Act's vision of dual federal-state authority and cooperation in this area specifically. See, e.g., 47 U.S.C. § 1301(4) ("The Federal Government should also recognize and encourage complementary State efforts to improve the quality and usefulness of broadband data."); id. § 1302(a) (referring to "[t]he Commission and each State Commission with regulatory jurisdiction" in a chapter titled "Broadband"); id. § 1304 ("[e]ncouraging State initiatives to improve broadband"); cf. id. § 253(b) ("Nothing in this section shall affect the ability of a State to impose ...requirements necessary to... protect the public safety and welfare,...and safeguard the rights of consumers."
    - "The Commission could choose to enact heavier or lighter regulation under Title II by exercising less or more of its Title II forbearance authority, with symmetrical "preemption implications," id. It just cannot completely disavow Title II with one hand while still clinging to Title II forbearance authority with the other."[3]

Free Speech claims:

Attesting to the state interest in privacy protection:

- "Privacy rights are fundamental because they protect important personal interests—freedom from identity theft, financial loss, or other economic harms, as well as concerns that intimate, personal details could become the grist for the mills of public embarrassment or harassment or the basis for opaque, but harmful judgments, including discrimination."
- We find that requiring customer approval for use and disclosure of customer PI prevents information uniquely collected and collated by telecommunications carriers from being used or disclosed against a customer's wishes, consistent with customer expectations, and as such directly and materially advances the government's substantial government interest in protecting customers' privacy.
- The failure to adequately protect customer PI can have myriad negative consequences for customers and society at large. Revelations of private facts have been recognized as harms since at least the time of Justices Warren and Brandeis. Failure to protect the privacy of consumer information can, of course create a risk of financial harm, identity theft and physical threat. The Commission has also found that emotional and dignitary harms are privacy harms, in other contexts.
- We therefore conclude that the government's interest in protecting customer privacy is a substantial one— a fact recognized widely by consumers, the courts, and the Communications Act.

Relating to disclosure:

---

[2] https://www.cadc.uscourts.gov/internet/opinions.nsf/FA43C305E2B9A35485258486004F6D0F/$file/18-1051-1808766.pdf

[3] The FCC, now headed by a former employee of Verizon, recently abandoned the previous administrations application of title II "common carrier" status to broadband providers.

FCC findings- ISP (BIAS) privacy order 2016

- "Requirements to include purely factual and uncontroversial information in commercial speech are constitutional so long as they are reasonably related to the government's substantial interest in protecting consumers. The notice requirements we adopt here, just like the notice requirements in the CPNI rules before them and like numerous notice and labeling requirements before, require only that companies provide factual and uncontroversial information to consumers.

Additional comments:

- ...the rules adopted here do not disfavor any particular activity. While a large number of commenters are particularly concerned with the limitations that the rules may place upon marketing, customers' privacy interests reach far beyond targeted marketing, to include for instance risk of identity theft or other fraud, stalking, and revelations of private communications, as well as the harms inherent in lacking control over the uses of their proprietary information

- "...if laws impacting expression were considered content-based for not being universal, nearly every privacy and intellectual property law would need to pass strict scrutiny. However, Sorrell stands for no such thing, itself citing HIPAA—limited to covering certain specific entities and types of information—as an example of a constitutionally sound privacy protection."
- Some commenters argue that the Commission can only demonstrate an interest in addressing the disclosure of customer PI and not in how carriers' use customer PI. We disagree. The Supreme Court has recognized that an important part of privacy is the right to know and have an effective voice in how one's information is being used, holding that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.

- While we recognize that adopting these rules cannot protect customers from privacy violations that originate from entities that are not telecommunications providers, the fact that the rules do not create universal privacy protection does not mean that customers' privacy interests are not advanced. Customers have an important interest in ensuring that their personal information is not used by their BIAS providers or other telecommunications carrier without their prior approval in a way that the customers do not or cannot reasonably expect.

Effect on innovation:

- By bolstering customer confidence in broadband providers' treatment of confidential customer information, we also promote the virtuous cycle of innovation in which new uses of the network lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses, business growth, and innovation.

(1)

Rep. Indruk, Hills. 34
February 7, 2020
2020-0560h
05/04

Amendment to HB 1680-FN

Amend the title of the bill by replacing it with the following:

AN ACT regulating the collection of personal information by broadband Internet access service providers and establishing a committee to study establishing broad data privacy rights in the state.

Amend the bill by replacing all after the enacting clause with the following:

1 New Chapter; Collection of Personal Information by Broadband Internet Access Service Providers. Amend RSA by inserting after chapter 359-Q the following new chapter:

CHAPTER 359-R

COLLECTION OF PERSONAL INFORMATION

BY BROADBAND INTERNET ACCESS SERVICE PROVIDERS

359-R:1 Definitions. In this chapter:

I. "Broadband Internet access service" means a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the service, excluding dial-up Internet access service.

II. "Customer" means an applicant for or a current or former subscriber of broadband Internet access service.

III. "Customer personal information" means:

(a) Personally identifying information about a customer, including but not limited to the customer's name, billing information, social security number, billing address and demographic data; and

(b) Information from a customer's use of broadband Internet access service, including but not limited to:

(1) The customer's web browsing history;

(2) The customer's application usage history;

(3) The customer's precise geolocation information;

(4) The customer's financial information;

(5) The customer's health information;

(6) Information pertaining to the customer's children;

(7) The customer's device identifier, such as a media access control address, international mobile equipment identity or Internet protocol address;

(8) The content of the customer's communications; and

(9) The origin and destination Internet protocol addresses.

IV. "Provider" means a person who provides broadband Internet access service.

359-R:2 Privacy of Customer Personal Information. A provider shall not use, disclose, sell, or permit access to customer personal information, except as provided in RSA 359-R:3, RSA 359-R:4, and 18 United States Code Section 2703.

359-R:3 Customer Consent Exception. Consent of a customer is governed by this section.

I. A provider may use, disclose, sell, or permit access to a customer's customer personal information if the customer gives the provider express, affirmative consent to such use, disclosure, sale, or access. A customer may revoke the customer's consent under this paragraph at any time.

II. A provider shall not:

(a) Refuse to serve a customer who does not provide consent under paragraph I; or

(b) Charge a customer a penalty or offer a customer a discount based on the customer's decision to provide or not provide consent under paragraph I.

III. A provider may use, disclose, sell, or permit access to information the provider collects pertaining to a customer that is not customer personal information, except upon written notice from the customer notifying the provider that the customer does not permit the provider to use, disclose, sell, or permit access to that information.

359-R:4 Other Exceptions. Notwithstanding RSA 359-R:2 and RSA 359-R:3, a provider may collect, retain, use, disclose, sell, and permit access to customer personal information without customer approval:

I. For the purpose of providing the service from which such information is derived or for the services necessary to the provision of such service;

II. To advertise or market the provider's communications-related services to the customer;

III. To comply with a lawful court order;

IV. To initiate, render, bill for, and collect payment for broadband Internet access service.

V. To protect users of the provider's or other providers' services from fraudulent, abusive, or unlawful use of or subscription to such services; and

VI. To provide geolocation information concerning the customer:

(a) For the purpose of responding to a customer's call for emergency services, to a public safety answering point; a provider of emergency medical or emergency dispatch services; a public safety, fire service or law enforcement official; or a hospital emergency or trauma care facility; or

(b) To a provider of information or database management services solely for the purpose of assisting in the delivery of emergency services in response to an emergency.

359-R:5 Security of Customer Personal Information. A provider shall take reasonable measures to protect customer personal information from unauthorized use, disclosure, or access.

I. In implementing security measures required by this section, a provider shall take into account each of the following factors:

(a) The nature and scope of the provider's activities;

(b) The sensitivity of the data the provider collects;

(c) The size of the provider; and

(d) The technical feasibility of the security measures.

II. A provider may employ any lawful measure that allows the provider to comply with the requirements of this section.

359-R:6 Notice Required. A provider shall provide to each of the provider's customers a clear, conspicuous, and nondeceptive notice at the point of sale and on the provider's publicly accessible website of the provider's obligations and a customer's rights under this chapter.

359-R:7 Applicability. The requirements of this chapter apply to providers operating within the state when providing broadband Internet access service to customers that are physically located and billed for service received in the state.

359-R:8 Enforcement and Remedies.

I. Any customer whose personal information has been used, disclosed, sold, or accessed in violation of this chapter may institute proceedings in any court of competent jurisdiction against the provider and shall be entitled to recover actual damages, $1,000 in total damages, or $100 for each violation, whichever is greater, as well as non-pecuniary damages.

II. A court shall award costs and reasonable attorneys' fees to a plaintiff who is the prevailing party in an action brought under paragraph I.

III. Any provider that violates this chapter shall be liable for a civil penalty of up to $1,000 per violation, or up to $7,500 per intentional violation, in a civil action brought by the attorney general.

2 Committee Established. There is established a committee to study establishing broad data privacy rights in the state.

3 Membership and Compensation.

I. The members of the committee shall be as follows:

(a) Three members of the house of representatives, one of whom shall be from the commerce and consumer affairs committee, and one of whom shall be from the science and technology committee, appointed by the speaker of the house of representatives.

(b) One member of the senate, appointed by the president of the senate.

II. Members of the committee shall receive mileage at the legislative rate when attending to the duties of the committee.

4 Duties.

I. The committee shall study:

(a) The ways in which the personal information of New Hampshire residents is digitally collected, stored, disclosed, or used for commercial purposes, and by which commercial entities.

(b) Existing protections, or the lack thereof, in New Hampshire law that require consumer consent before personal information can be digitally collected, stored, disclosed, or shared by commercial entities.

(c) How other states provide greater consumer privacy protection than New Hampshire, including restrictions on what digital information can be shared with third parties and when.

(d) How New Hampshire could strengthen consumer data privacy, including consent requirements and requirements that certain data be deleted.

II. The committee may solicit information from any person or entity the committee deems relevant to its study.

5 Chairperson; Quorum. The members of the study committee shall elect a chairperson from among the members. The first meeting of the committee shall be called by the first-named house member. The first meeting of the committee shall be held within 45 days of the effective date of this section. Three members of the committee shall constitute a quorum.

6 Report. The committee shall report its findings and any recommendations for proposed legislation to the speaker of the house of representatives, the president of the senate, the house clerk, the senate clerk, the governor, and the state library on or before November 1, 2020.

7 Effective Date.

I. Section 1 of this act shall take effect July 1, 2021.

II. The remainder of this act shall take effect upon its passage.

2020-0560h

AMENDED ANALYSIS

This bill:

I. Prohibits a provider of broadband Internet access service from using, disclosing, selling or permitting access to customer personal information unless the customer expressly consents to that use, disclosure, sale, or access.

II. Provides other exceptions under which a provider may use, disclose, sell, or permit access to customer personal information.

III. Prohibits a provider from refusing to serve a customer, charging a customer a penalty or offering a customer a discount if the customer does or does not consent to the use, disclosure, sale, or access.

IV. Requires providers to take reasonable measures to protect customer personal information from unauthorized use, disclosure, sale, or access.

V. Establishes a legislative committee to study establishing broad data privacy rights in New Hampshire.

(1)

02/21/20- Indruk
HB 1680 - Amendment

Broadband internet access is a critical component of modern life. The internet is increasingly where we do our banking, shopping, healthcare research, get our news and conduct our social lives, including dating, sharing family photos and making connections of all sorts. Most of us understand that many of the individual websites we visit collect and monetize our personal information, but we may not understand that the "on ramp" to these services, our internet service provider (ISP), may be doing the same thing across an even broader swath of our internet activities.

ISPs occupy a privileged position in the digital data economy- they have a wide view of our activities across different platforms- they are not just one website or app, they are the gateway to every activity. As the FCC wrote in 2016, these providers "...have access to vast amounts of information about their customers including when we are online, where we are physically located when we are online, how long we stay online, what devices we use to access the Internet, what websites we visit, and what applications we use."

Unfortunately the rules the FCC adopted in 2016 to secure our choice of privacy preferences in this market were overwritten by congress and then further eroded in 2018 by the FCC under new leadership.

Make no mistake about it, the action by congress and the FCC to overturn ISP privacy protections has left NH customers vulnerable. This is an untenable situation and the state must step in, as Maine has, to protect NH broadband subscribers from unanticipated and unwanted data surveillance and dissemination. This is why we have introduced an amendment to HB1680 specifically targeting this glaring vulnerability.

Our amendment seeks simply to reestablish the FCC's most critical 2016 privacy protections by establishing them in state law. Customers would be given an opt-in right for the sale or use of particular categories of sensitive information and ISPs would need to provide clear disclosure of their data policies. In other words, just as in any other property transaction, the one giving up the property, the ISP customer, would need to give permission for the transaction, data use or sale, to take place. These simple steps are necessary to ensure NH residents have agency over how their data is used. As the FCC put it in its' 2016 rules:

> *The privacy framework we adopt today focuses on transparency, choice, and data security, and provides heightened protection for sensitive customer information, consistent with customer expectations. In adopting these rules we honor customer's privacy rights and implement the statutory requirement that carriers protect the confidentiality of customer proprietary information. These rules do not prohibit broadband providers from using or sharing customer information, but rather are designed to protect consumer choice while giving broadband providers the flexibility they need to continue to innovate. By bolstering customer confidence in broadband providers' treatment of confidential customer information, we also promote the virtuous cycle of innovation in which new uses of the network lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses, business growth, and innovation.*

Despite the clear reasonableness of our amendment, ISPs have vociferously objected. At least one ISP has claimed it does not sell customer data. Yet they fight tooth and claw to retain the right to do so.

Of course, "selling" data can take many forms. For instance, your web surfing habits can be used to sell targeted advertising services and analytics all while also charging you for your internet service. That is to say, ISPs can charge you a monthly fee for access to the internet and then profit again by offering services to third parties who want to target you, our your family, with specific ads.

It should also be noted that any data that is collected on ISP customers may be susceptible to hacking and released into the world. Every site you've visited, your location data, your demographic information and other sensitive data could be made available for the world to see. As we have seen with events like the 2017 Equifax breach, such disclosures can be far reaching and irreversibly damaging.

And this doesn't even begin to touch on the real concerns of how data is used in conjunction with AI to profile consumers and to make inferences, sometimes in error, and sometimes with spooky accuracy, about our future behavior, exploitable psychological vulnerabilities and inner thoughts. Nor does this even begin to contemplate how such data might be used 10 or 20 years in the future; data does not have an expiration date and technology will surely continue to expand the universe of what is possible beyond our wildest imaginations.

In the wake of debacles like Verizon's super cookie tracking scheme, which ended in a settlement with the FCC, ISPs should be looking to rebuild trust in the internet access they provide instead of working to undermine our faith in such a critical service. The relationship with our ISPs should start with the presumption of protection for our sensitive data; this is why we, following on the heels of the FCC's 2016 privacy rule and Maine's newly enacted ISP privacy law, have adopted an opt-in standard as the basis of data use and sale. The customer should be in the driver's seat; data use and sale should be inline with consumer expectations. If ISPs are not stretching uses beyond these expectations, they should get behind these valuable trust-building protections.

Please join us in supporting HB 1680 and securing choice and transparency in how ISPs collect, use and sell our data. It is past time we start protecting the right to privacy in this state. This is not the only step that will be needed in this long journey, but it is a crucial one.

INDRUK
ARS TECHNICA (1)

How ISPs can sell your Web history—and how to stop them

How the Senate's vote to kill privacy rules affects you.

Enlarge
Getty Images | KrulUA

The US Senate yesterday voted to eliminate privacy rules that would have forced ISPs to get your consent before selling Web browsing history and app usage history to advertisers. Within a week, the House of Representatives could follow suit, and the rules approved by the Federal Communications Commission last year would be eliminated by Congress.

So what has changed for Internet users? In one sense, nothing changed this week, because the requirement to obtain customer consent before sharing or selling data is not scheduled to take effect until at least December 4, 2017. ISPs didn't have to follow the rules yesterday or the day before, and they won't ever have to follow them if the rules are eliminated.

But the Senate vote is nonetheless one big step toward a major victory for ISPs, one that would give them legal certainty if they continue to make aggressive moves into the advertising market. The Senate vote invoked the Congressional Review Act, which lets Congress eliminate regulations it doesn't like and prevent the agency from issuing similar regulations in the future. For ISPs, this is better than the FCC undoing its own rules, because it means a future FCC won't be able to reinstate them.

Unless the House or President Donald Trump oppose the Senate's action, ISPs will not have to worry about any strong privacy rules getting in the way of using your browsing history for profit. There won't be any specific rules requiring them to get opt-in consent before sharing browsing history, even if that data is related to just one customer instead of being aggregated with other customers' data in order to anonymize it.

Senate Democrats warned before yesterday's vote that ISPs will be able to "draw a map" of where families shop and go to school, detect health information by seeing which illnesses they use the Internet to gather information on, and build profiles of customers' listening and viewing history.

The Senate vote was 50-48, with every Republican senator voting to kill privacy rules and every Democratic senator voting to preserve them.

ISPs can't see encrypted traffic, so if you visit an HTTPS site, ISPs will see only the domain (like https://arstechnica.com) rather than each page you visit. But that's still plenty, said Dallas Harris, an attorney who specializes in broadband privacy and is a policy fellow at consumer advocacy group Public Knowledge.

ISPs might be able to figure out where you bank, your political views, and your sexual orientation based on what sites you visit, Harris told Ars.

"You don't need to see the contents of every communication" to develop efficient ad tracking mechanisms, she said. "The fact that you're looking at a website can reveal when you're home, when you're not home."

An ISP might notice that a particular tablet often visits children's websites. From that, "they can infer that this tablet then belongs to a child" and deliver advertising targeted to kids. "The level of information that they can figure out is beyond what even most customers expect," Harris said.

How the rules have changed

The legal changes all stem from the FCC's decision in February 2015 to reclassify home and mobile ISPs as common carriers. The reclassification had numerous effects: it allowed the FCC to impose net neutrality rules, but it also stripped the Federal Trade Commission of its authority over ISPs because the FTC's charter from Congress prohibits the agency from regulating common carriers.

Before the February 2015 reclassification, ISPs could have been punished by the FTC for violating customers' privacy. But following the FTC rules wasn't too onerous—the FTC recommends opt-in consent before selling or sharing the most sensitive information, such as Social Security numbers, the content of communications, financial and health information, information about children, and precise geo-location data. But ISPs could use an opt-out system for everything else, including Web browsing and app usage history.

ISPs "want to be the advertising powerhouse."

The FCC's reclassification of ISPs removed FTC authority but imposed privacy requirements from Title II, Section 222 of the Communications Act. The problem is that Section 222 was written in 1996 for telephone service, so the FCC said it would write new broadband-specific rules explaining exactly how Section 222 would be enforced on ISPs. Those rules, including the opt-in requirements, were finalized in October 2016.

Theoretically, Congress and the FCC could return jurisdiction to the FTC by eliminating the privacy rules *and* eliminating the ISPs' common carrier classification. But even that might not work, because a federal appeals court ruling in August 2016 said that any company with a common carrier business cannot be regulated by the FTC at all, even when they're offering non-common carrier services. The common carrier designation is also used for landline phone and mobile voice service; that means ISPs like AT&T, Verizon, T-Mobile, and Sprint could be entirely exempt from FTC oversight. Comcast and other cable companies are only common carriers for Internet service because their VoIP phones are regulated differently, so they could more easily go back under FTC oversight.

But even if the FTC regains jurisdiction, its guidelines are weaker than the FCC's privacy rules. Thus, yesterday's Senate vote could leave us with no rules preventing ISPs from selling your Web browsing histories to advertisers and data brokers without obtaining opt-in consent.

When AT&T charged extra for privacy

The most prominent example of an ISP monetizing customers' browsing history comes from AT&T. Starting in 2013, AT&T charged fiber Internet customers at least $29 extra each month unless they opted in to a system that scanned customers' Internet traffic in order to deliver personalized ads.

AT&T killed this "Internet Preferences" program shortly before the FCC finalized its privacy rules. But that doesn't mean ISPs are giving up on advertising.

ISPs "want to be the advertising powerhouse, which is why they fought so hard against these rules," Harris said. "They want to compete with Google and Facebook and other edge providers in the advertising space. This is going to be their new frontier, a new way for them to increase their profits."

ISP lobby groups have argued that privacy rules would prevent them from showing Internet users more relevant advertising via "data-driven services" and would prevent ISPs from competing in the online advertising market. They've argued that Web browsing and app usage history should not be classified as "sensitive" information.

Advertising lobby groups, knowing that they could end up working more closely with ISPs, recently thanked Republican lawmakers for taking steps to kill the privacy rules.

AT&T sells advertising via its AdWorks division, which boasts of "more targeted" ads to "more screens," via TV set-top boxes and online video. Comcast sells online advertising that can appear on xfinity.com and NBC sites. Verizon boosted its online advertising technology when it purchased AOL and is trying to finalize a purchase of Yahoo.

Because these ISPs operate their own advertising networks, they don't need to share individuals' browsing history with third parties in order to serve targeted ads. But they can use customers' browsing history to sell targeted ads. Businesses would pay the ISPs to have their advertising reach people

who are more likely to buy their products, but only the ISPs would know exactly who those customers are.

"They've already begun marketing [to advertisers], explaining how they have the ability to track you on four devices," Harris said. "Because they're also your cable [TV] providers, they can combine what you're watching on TV with what you're doing on the Internet and looking at on your phones and your tablets. They're heavily invested in this idea that they have a lot of data that can be valuable to advertisers and want to build up that part of their business."

For ISPs that don't operate their own ad networks, getting into the targeted advertising business could involve sharing customers' browsing with third parties. The FCC privacy rules would have prevented both the internal use and sharing of such information without opt-in consent.

I Gave a Bounty Hunter $300. Then He Located Our Phone

Image: Shutterstock. Remix: Jason Koebler

Nervously, I gave a bounty hunter a phone number. He had offered to geolocate a phone for me, using a shady, overlooked service intended not for the cops, but for private individuals and businesses. Armed with just the number and a few hundred dollars, he said he could find the current location of most phones in the United States.

The bounty hunter sent the number to his own contact, who would track the phone. The contact responded with a screenshot of Google Maps, containing a blue circle indicating the phone's current location, approximate to a few hundred metres.

Queens, New York. More specifically, the screenshot showed a location in a particular neighborhood—just a couple of blocks from where the target was. The hunter had found the phone (the target gave their consent to Motherboard to be tracked via their T-Mobile phone.)

The bounty hunter did this all without deploying a hacking tool or having any previous knowledge of the phone's whereabouts. Instead, the tracking tool relies on real-time location data sold to bounty hunters that ultimately originated from the telcos themselves, including T-Mobile, AT&T, and Sprint, a Motherboard investigation has found. These surveillance capabilities are sometimes sold through word-of-mouth networks.

Whereas it's common knowledge that law enforcement agencies can track phones with a warrant to service providers, IMSI catchers, or until recently via other companies that sell location data such as one called Securus, at least one company, called Microbilt, is selling phone geolocation services with little oversight to a spread of different private industries, ranging from car salesmen and property managers to bail bondsmen and bounty hunters, according to sources familiar with the company's products and company documents obtained by Motherboard. Compounding that already highly questionable business practice, this spying capability is also being resold to others on the black market who are not licensed by the company to use it, including me, seemingly without Microbilt's knowledge.

Motherboard's investigation shows just how exposed mobile networks and the data they generate are, leaving them open to surveillance by ordinary citizens, stalkers, and criminals, and comes as media and policy makers are paying more attention than ever to how location and other sensitive data is collected and sold. The investigation also shows that a wide variety of companies can access cell phone location data, and that the information trickles down from cell phone providers to a wide array of smaller players, who don't necessarily have the correct safeguards in place to protect that data.

"People are reselling to the wrong people," the bail industry source who flagged the company to Motherboard said. Motherboard granted the source and others in this story anonymity to talk more candidly about a controversial surveillance capability.

Got a tip? You can contact Joseph Cox securely on Signal on +44 20 8133 5190, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.

Your mobile phone is constantly communicating with nearby cell phone towers, so your telecom provider knows where to route calls and texts. From this, telecom companies also work out the phone's approximate location based on its proximity to those towers.

Although many users may be unaware of the practice, telecom companies in the United States sell access to their customers' location data to other companies, called location aggregators, who then sell it to specific clients and industries. Last year, one location aggregator called LocationSmart faced harsh criticism for selling data that ultimately ended up in the hands of Securus, a company which provided phone tracking to low level enforcement without requiring a warrant. LocationSmart also exposed the very data it was selling through a buggy website panel, meaning anyone could geolocate nearly any phone in the United States at a click of a mouse.

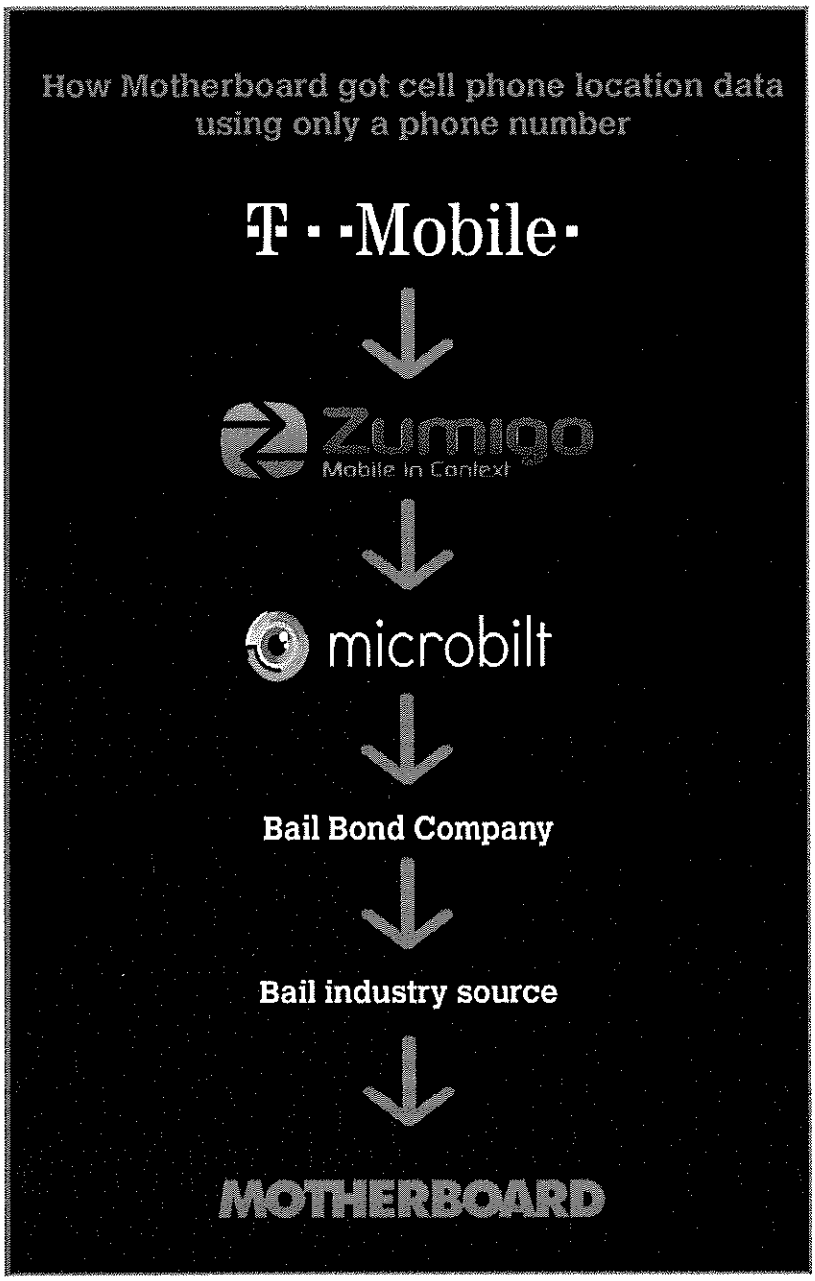
[Subscribe to CYBER on Apple Podcasts or any podcast app.]

There's a complex supply chain that shares some of American cell phone users' most sensitive data, with the telcos potentially being unaware of how the data is being used by the eventual end user, or even whose hands it lands in. Financial companies use phone location data to detect fraud; roadside assistance firms use it to locate stuck customers. But AT&T, for example, told Motherboard the use of its customers' data by bounty hunters goes explicitly against the company's policies, raising questions about how AT&T allowed the sale for this purpose in the first place.

"The allegation here would violate our contract and Privacy Policy," an AT&T spokesperson told Motherboard in an email.

In the case of the phone we tracked, six different entities had potential access to the phone's data. T-Mobile shares location data with an aggregator called Zumigo, which shares information with Microbilt. Microbilt shared that data with a customer using its mobile phone tracking product. The bounty hunter then shared this information with a bail industry source, who shared it with Motherboard.

The CTIA, a telecom industry trade group of which AT&T, Sprint, and T-Mobile are members, has official guidelines for the use of so-called "location-based services" that "rely on two fundamental principles: user notice and consent," the group wrote in those guidelines. Telecom companies and data aggregators that Motherboard spoke to said that they require their clients to get consent from the people they want to track, but it's clear that this is not always happening.



A second source who has tracked the geolocation industry told Motherboard, while talking about the industry generally, "If there is money to be made they will keep selling the data."

"Those third-level companies sell their services. That is where you see the issues with going to shady folks [and] for shady reasons," the source added.

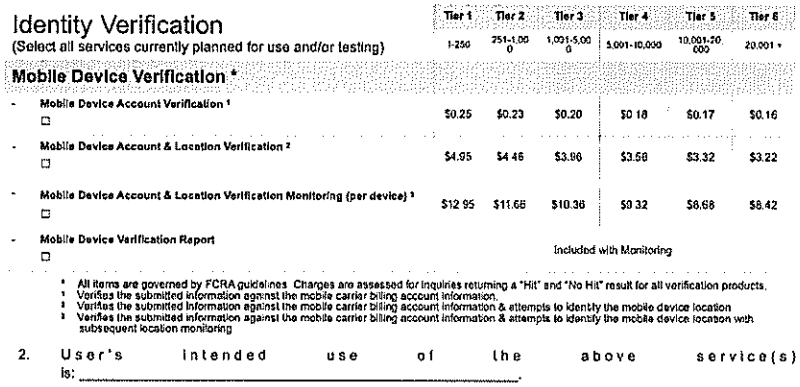
Frederike Kaltheuner, data exploitation programme lead at campaign group Privacy International, told Motherboard in a phone call that "it's part of a bigger problem; the US has a completely unregulated data ecosystem."

Microbilt buys access to location data from an aggregator called Zumigo and then sells it to a dizzying number of sectors, including landlords to scope out potential renters; motor vehicle salesmen, and others who are conducting credit checks. Armed with just a phone number, Microbilt's "Mobile Device Verify" product can return a target's full name and address, geolocate a phone in an individual instance, or operate as a continuous tracking service.

"You can set up monitoring with control over the weeks, days and even hours that location on a device is checked as well as the start and end dates of monitoring," a company brochure Motherboard found online reads.

Posing as a potential customer, Motherboard explicitly asked a Microbilt customer support staffer whether the company offered phone geolocation for bail bondsmen. Shortly after, another staffer emailed with a price list—locating a phone can cost as little as $4.95 each if searching for a low number of devices. That price gets even cheaper as the customer buys the capability to track more phones. Getting real-time updates on a phone's location can cost around $12.95.

"Dirt cheap when you think about the data you can get," the source familiar with the industry added.



Identity Verification
(Select all services currently planned for use and/or testing)

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5	Tier 6
	1-250	251-1,000	1,001-5,000	5,001-10,000	10,001-20,000	20,001 +
Mobile Device Verification *						
- Mobile Device Account Verification [1] ☐	$0.25	$0.23	$0.20	$0.18	$0.17	$0.16
- Mobile Device Account & Location Verification [2] ☐	$4.95	$4.46	$3.96	$3.58	$3.32	$3.22
- Mobile Device Account & Location Verification Monitoring (per device) [3] ☐	$12.95	$11.66	$10.36	$9.32	$8.68	$8.42
- Mobile Device Verification Report ☐	Included with Monitoring					

* All items are governed by FCRA guidelines. Charges are assessed for inquiries returning a "Hit" and "No Hit" result for all verification products.
1 Verifies the submitted information against the mobile carrier billing account information.
2 Verifies the submitted information against the mobile carrier billing account information & attempts to identify the mobile device location
3 Verifies the submitted information against the mobile carrier billing account information & attempts to identify the mobile device location with subsequent location monitoring

2. User's intended use of the above service(s) is: _____.

It's bad enough that access to highly sensitive phone geolocation data is already being sold to a wide range of industries and businesses. But there is also an underground market that Motherboard used to geolocate a phone—one where Microbilt customers resell their access at a profit, and with minimal oversight.

"Blade Runner, the iconic sci-fi movie, is set in 2019. And here we are: there's an unregulated black market where bounty-hunters can buy information about where we are, in real time, over time, and come after us. You don't need to be a replicant to be scared of the consequences," Thomas Rid, professor of strategic studies at Johns Hopkins University, told Motherboard in an online chat.

The bail industry source said his middleman used Microbilt to find the phone. This middleman charged $300, a sizeable markup on the usual Microbilt price. The Google Maps screenshot provided to Motherboard of the target phone's location also included its approximate longitude and latitude coordinates, and a range of how accurate the phone geolocation is: 0.3 miles, or just under 500 metres. It may not necessarily be enough to geolocate someone to a specific building in a populated area, but it can certainly pinpoint a particular borough, city, or neighborhood.

In other cases of phone geolocation it is typically done with the consent of the target, perhaps by sending a text message the user has to deliberately reply to, signalling they accept their location being tracked. This may be done in the earlier roadside assistance example or when a company monitors its fleet of trucks. But when Motherboard tested the geolocation service, the target phone received no warning it was being tracked.

The bail source who originally alerted Microbilt to Motherboard said that bounty hunters have used phone geolocation services for non-work purposes, such as tracking their girlfriends. Motherboard was unable to identify a specific instance of this happening, but domestic stalkers have repeatedly used technology, such as mobile phone malware, to track spouses.

As Motherboard was reporting this story, Microbilt removed documents related to its mobile phone location product from its website.

A Microbilt spokesperson told Motherboard in a statement that the company requires anyone using its mobile device verification services for fraud prevention must first obtain consent of the consumer. Microbilt also confirmed it found an instance of abuse on its platform—our phone ping.

"The request came through a licensed state agency that writes in approximately $100 million in bonds per year and passed all up front credentialing under the pretense that location was being verified to mitigate financial exposure related to a bond loan being considered for the submitted consumer," Microbilt said in an emailed statement. In this case, "licensed state agency" is referring to a private bail bond company, Motherboard confirmed.

"As a result, MicroBilt was unaware that its terms of use were being violated by the rogue individual that submitted the request under false pretenses, does not approve of such use cases, and has a clear policy that such violations will result in loss of access to all MicroBilt services and termination of the requesting party's end-user agreement," Microbilt added. "Upon investigating the alleged abuse and learning of the violation of our contract, we terminated the customer's access to our products and they will not be eligible for reinstatement based on this violation."

Zumigo confirmed it was the company that provided the phone location to Microbilt and defended its practices. In a statement, Zumigo did not seem to take issue with the practice of providing data that ultimately ended up with licensed bounty hunters, but wrote, "illegal access to data is an unfortunate occurrence across virtually every industry that deals in consumer or employee data, and it is impossible to detect a fraudster, or rogue customer, who requests location data of his or her own mobile devices when the required consent is provided. However, Zumigo takes steps to protect privacy by providing a measure of distance (approx. 0.5-1.0 mile) from an actual address." Zumigo told Motherboard it has cut Microbilt's data access.

"People are reselling to the wrong people."

In Motherboard's case, the successfully geolocated phone was on T-Mobile.

"We take the privacy and security of our customers' information very seriously and will not tolerate any misuse of our customers' data," A T-Mobile spokesperson told Motherboard in an emailed statement. "While T-Mobile does not have a direct relationship with Microbilt, our vendor Zumigo was working with them and has confirmed with us that they have already shut down all transmission of T-Mobile data. T-Mobile has also blocked access to device location data for any request submitted by Zumigo on behalf of Microbilt as an additional precaution."

Microbilt's product documentation suggests the phone location service works on all mobile networks, however the middleman was unable or unwilling to conduct a search for a Verizon device. Verizon did not respond to a request for comment.

AT&T told Motherboard it has cut access to Microbilt as the company investigates.

"We only permit the sharing of location when a customer gives permission for cases like fraud prevention or emergency roadside assistance, or when required by law," the AT&T spokesperson said.

Sprint told Motherboard in a statement that "protecting our customers' privacy and security is a top priority, and we are transparent about that in our Privacy Policy [...] Sprint does not have a direct relationship with MicroBilt. If we determine that any of our customers do and have violated the terms of our contract, we will take appropriate action based on those findings." Sprint would not clarify the contours of its relationship with Microbilt.

These statements sound very familiar. When *The New York Times* and Senator Ron Wyden published details of Securus last year, the firm that was offering geolocation to low level law enforcement without a warrant, the telcos said they were taking extra measures to make sure their customers' data would not be abused again. Verizon

announced it was going to limit data access to companies not using it for legitimate purposes. T-Mobile, Sprint, and AT&T followed suit shortly after with similar promises.

After Wyden's pressure, T-Mobile's CEO John Legere tweeted in June last year "I've personally evaluated this issue & have pledged that @tmobile will not sell customer location data to shady middlemen."

"It appears these promises were little more than worthless spam in their customers' inboxes."

Months after the telcos said they were going to combat this problem, in the face of an arguably even worse case of abuse and data trading, they are saying much the same thing. Last year, Motherboard reported on a company that previously offered phone geolocation to bounty hunters; here Microbilt is operating even after a wave of outrage from policy makers. In its statement to Motherboard on Monday, T-Mobile said it has nearly finished the process of terminating its agreements with location aggregators.

"It would be bad if this was the first time we learned about it. It's not. Every major wireless carrier pledged to end this kind of data sharing after I exposed this practice last year. Now it appears these promises were little more than worthless spam in their customers' inboxes," Wyden told Motherboard in a statement. Wyden is proposing legislation to safeguard personal data.

Due to the ongoing government shutdown, the Federal Communications Commission (FCC) was unable to provide a statement.

"Wireless carriers' continued sale of location data is a nightmare for national security and the personal safety of anyone with a phone," Wyden added. "When stalkers, spies, and predators know when a woman is alone, or when a home is empty, or where a White House official stops after work, the possibilities for abuse are endless."

POLICY —

NebuAd, ISPs sued over DPI snooping, ad-targeting program

NebuAd and a number of ISPs find themselves on the wrong end of a class-action ...

JACQUI CHENG - 11/11/2008, 10:50 PM

NebuAd, the company behind the highly-controversial behavioral-targeting ad platform, has been targeted itself—by a class-action lawsuit, that is. A suit has been filed in the US District Court of Northern California against the company, as well as a number of ISPs that tested NebuAd's technology, alleging numerous privacy violations, fraud, and unjust enrichment.

NebuAd made news earlier this year when it made a deal to test its deep-packet inspection technology with US cable operator Charter Communications. The idea behind the tech was that the companies would carefully monitor each user's Internet use in order to use that information to show highly-targeted advertising. Needless to say, there was an immediate and extreme outcry over the technology, with some going so far as referring to it as a "man-in-the-middle attack." Users could opt out—if they learned about the trial—but the tracking defaulted to automatic opt-in.

Questions arose as to whether NebuAd's system was even legal in the first place, as a number of advocacy groups criticized the service as an invasion of privacy and said it could even be violating federal wiretap laws. NebuAd, on the other hand, insisted to Congress that everything was on the up-and-up and that the system was collecting no personally-identifying information. Still, skeptics said

that, identifying information or not, collecting data the way NebuAd does was in violation of state and federal laws.

The lawsuit accuses NebuAd, Bresnan Communications, Cable One, CenturyTel, Embarq, Knology, and WOW! of all being involved in the interception, copying, transmission, collection, storage, usage, and altering of private data from users. NebuAd "exploits normal browser platform security behaviors by forging IP packets, allowing their own JavaScript code to be written into source code trusted by the web browser," reads the complaint. "NebuAd and ISPs together cooperate in this attack against the intentions of the consumers, the designers of their software, and the owners of the servers they visit."

All of the involved parties are alleged to have violated the Electronic Communications Privacy Act of 1986, California's Computer Crime Law, the federal Computer Fraud and Abuse Act, and the California Invasion of Privacy Act. Several of the ISPs are accused of aiding and abetting violations of the above laws and are even accused of civil conspiracy. All defendants are being charged with unjust enrichment for benefiting from the communications they intercepted.

The lawsuit asks for injunctive relief prohibiting NebuAd and the ISPs from engaging in deep packet inspection and requiring them to "disgorge all of their ill-gotten gains" to the class. The suit also asks that the defendants delete all of their collected data and offer a way for class members to permanently opt out of any future data collection activities. Of course, NebuAd has already lost its CEO and announced plans in September to scale back its tracking in order to "broaden its focus" on traditional advertising, but that probably won't stop the case from moving forward.

Further reading:

- Found via ZDNet: NebuAd, ISPs, named in class action lawsuit

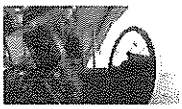
READER COMMENTS

SHARE THIS STORY

JACQUI CHENG

Jacqui is an Editor at Large at Ars Technica, where she has spent the last eight years writing about Apple culture, gadgets, social networking, privacy, and more.

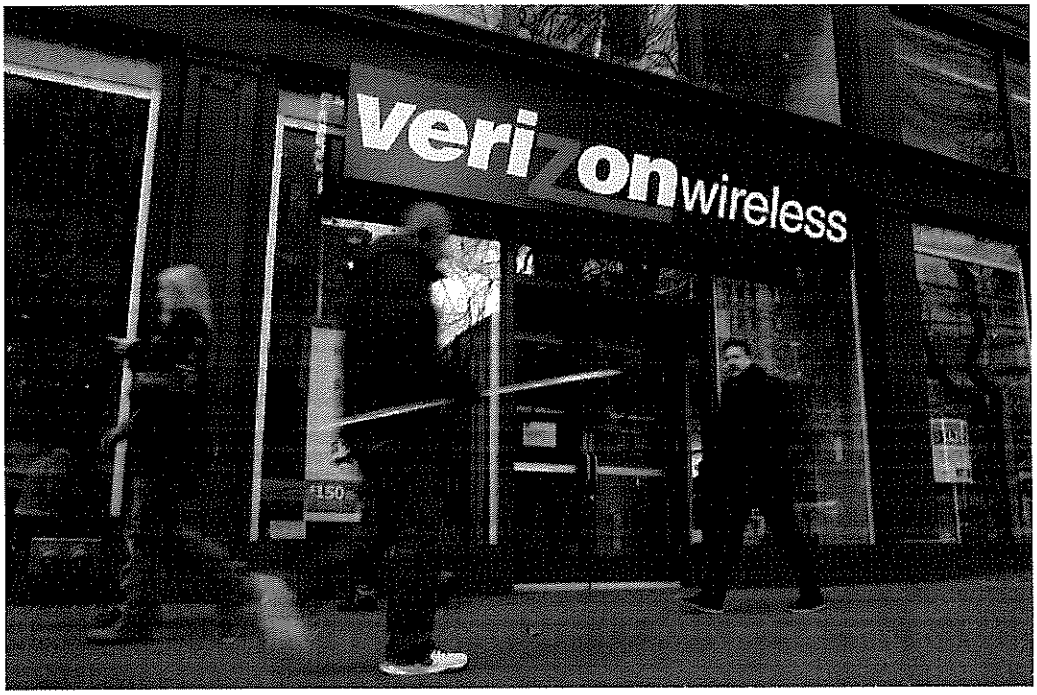
EMAIL jacqui@arstechnica.com // **TWITTER** @ejacqui



SITREP: DOD Resets Ballistic Missile

(1)

ShareAll sharing options for:FCC fines Verizon $1.35 million over 'supercookie' tracking



Justin Sullivan/Getty Images

Verizon is settling with the FCC over its use of an ad targeting technology known as a "supercookie," which tracks the websites visited by phones on its network. Supercookies allow websites to better target ads to visitors with Verizon cellphone service; but those visitors — for a period of time — weren't informed of the tracking or given the option to opt out. Because of that, Verizon will pay a fine of $1.35 million and will now have to receive customer permission before sharing tracking data with other companies or even within its organization, including with sites owned by AOL.

""[Consumers] should have a say in how their personal information is used.""

After an initial backlash, Verizon allowed customers to opt out of its supercookie tracking program about a year ago. Today's settlement pushes the options Verizon offers customers even further, allowing those who don't opt out of the program to limit who gets to see their information. That's an important change, as a major concern with supercookies from the

start was that websites might be able to permanently track someone, since it was impossible for a person on Verizon's network to disassociate themself from the supercookie. As the EFF put it, "It allows third-party advertisers and websites to assemble a deep, permanent profile of visitors' web browsing habits without their consent."

In addition to requiring that consumers opt in to having their data shared, Verizon will also have to inform customers about its ad-targeting practices in the first place. Verizon says that it's already been working on this. "Verizon gives customers choices about how we use their data, and we work hard to provide customers with clear, complete information to help them make decisions about our services," Rich Young, Verizon's regulatory spokesperson, says in a statement. "Over the past year, we have made several changes to our advertising programs that have provided consumers with even more options. Today's settlement with the FCC recognizes that. We will continue to give customers the information they need to decide what programs and services are right for them."

The FCC says that this settlement represents a defense of its Open Internet Transparency Rule; its second enforcement action to date following a fine against AT&T over unlimited data plans. The Transparency Rule is an extension of its net neutrality rules meant to require clear and accurate communication to consumers. It's possible that we'll see stricter rules around ad tracking developed as the commission begins determining how Title II applies to carriers. For now, the FCC seems to suggest that there's some degree of tracking — albeit with clarity and the option to opt out — that's acceptable. "Consumers care about privacy and should have a say in how their personal information is used, especially when it comes to who knows what they're doing online," Travis LeBlanc, chief of the FCC's Enforcement Bureau, says in a statement. He continues, "Privacy and innovation are not incompatible. This agreement shows that companies can offer meaningful transparency and consumer choice while at the same time continuing to innovate."

US008763101B2

(12) **United States Patent**
Counterman

(10) **Patent No.: US 8,763,101 B2**
(45) **Date of Patent: Jun. 24, 2014**

(54) **MULTI-FACTOR AUTHENTICATION USING A UNIQUE IDENTIFICATION HEADER (UIDH)**

(75) Inventor: **Raymond C. Counterman**, Canton, MA (US)

(73) Assignee: **Verizon Patent and Licensing Inc.**, Basking Ridge, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 66 days.

(21) Appl. No.: **13/477,578**

(22) Filed: **May 22, 2012**

(65) **Prior Publication Data**

US 2013/0318581 A1 Nov. 28, 2013

(51) **Int. Cl.**

G06F 17/30	(2006.01)
H04L 9/32	(2006.01)
H04L 29/06	(2006.01)
H04W 12/06	(2009.01)
H04W 84/12	(2009.01)

(52) **U.S. Cl.**

CPC ***H04L 63/08*** (2013.01); ***H04W 12/06*** (2013.01); ***H04W 84/12*** (2013.01); *H04L 2209/80* (2013.01)

USPC **726/7**; 726/3; 726/5; 713/168

(58) **Field of Classification Search**

CPC . H04L 63/08; H04L 2209/56; H04L 63/0823; H04L 2209/80; H04W 12/06; H04W 88/08; H04W 84/12; G06Q 20/04; G06Q 20/32; G06F 21/31

USPC 726/1–7, 26–29; 713/168, 170, 182, 713/183, 189

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,606,918	B2 *	10/2009	Holzman et al.	709/229
8,151,328	B1 *	4/2012	Lundy et al.	726/5
8,195,956	B2 *	6/2012	Bilodi	713/189
2006/0075230	A1 *	4/2006	Baird et al.	713/168
2007/0050303	A1 *	3/2007	Schroeder et al.	705/67
2007/0136573	A1 *	6/2007	Steinberg	713/155
2007/0220594	A1 *	9/2007	Tulsyan	726/5
2007/0240202	A1 *	10/2007	Sullivan et al.	726/4
2008/0189772	A1 *	8/2008	Sims et al.	726/5
2009/0037995	A1 *	2/2009	Zapata et al.	726/9
2009/0260064	A1 *	10/2009	McDowell et al.	726/4
2010/0011212	A1 *	1/2010	Anemikos et al.	713/171
2010/0138297	A1 *	6/2010	Fitzgerald et al.	705/14.53
2010/0250937	A1 *	9/2010	Blomquist et al.	713/170
2010/0250957	A1 *	9/2010	Cuppett	713/186
2010/0274913	A1 *	10/2010	Ando	709/229
2011/0246235	A1 *	10/2011	Powell et al.	705/3
2011/0258120	A1 *	10/2011	Weiss	705/44
2011/0275348	A1 *	11/2011	Clark et al.	455/411

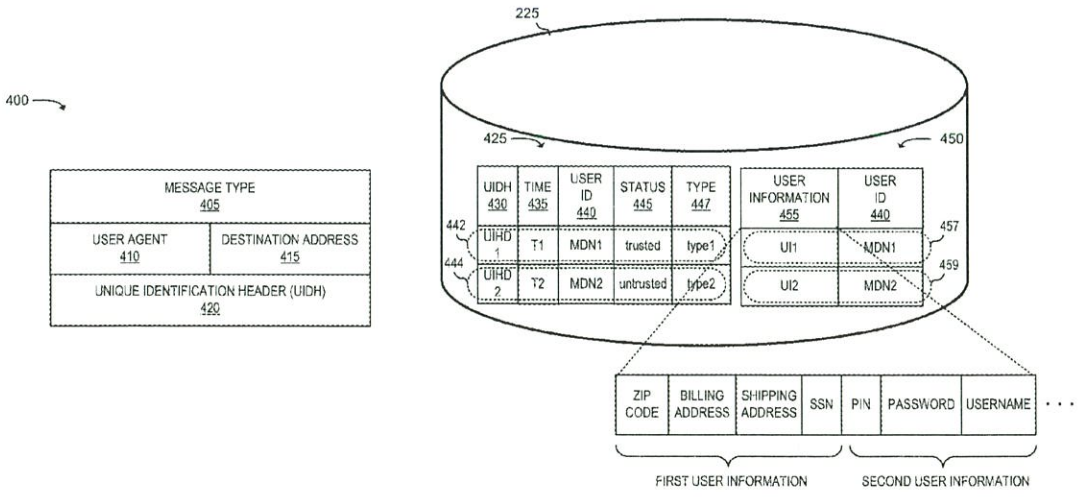
(Continued)

Primary Examiner — Catherine Thiaw

(57) **ABSTRACT**

A system is configured to receive, from a user device, information associated with a request to receive a service from a server device, the information including a unique identifier, an identifier, associated with a user of the user device, being encoded with a key to obtain the unique identifier. The system may also be configured to extract the unique identifier from the information; retrieve, from a memory, the identifier, associated with the user, that corresponds to the unique identifier; obtain an indication whether the identifier, associated with the user, is trusted; perform one or more additional authentication operations on the user when the identifier, associated with the user, is trusted; and transmit, to the server device, a notification that indicates that the user is authenticated when the one or more additional authentication operations indicate that the user device is authenticated.

20 Claims, 13 Drawing Sheets



US006339761B1

(12) **United States Patent**
Cottingham

(10) **Patent No.: US 6,339,761 B1**
(45) **Date of Patent: Jan. 15, 2002**

(54) **INTERNET SERVICE PROVIDER ADVERTISING SYSTEM**

(76) Inventor: **Hugh V. Cottingham**, 49 Mountain Ave., Caldwell, NJ (US) 07006

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/312,072**

(22) Filed: **May 13, 1999**

(51) **Int. Cl.**[7] **G06F 17/60**

(52) **U.S. Cl.** **705/14**

(58) **Field of Search** 705/10, 14, 16; 709/217, 219

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,029,045	A *	2/2000	Picco et al.	725/34
6,134,532	A *	10/2000	Lazarus et al.	705/14
6,226,648	B1 *	5/2001	Appleman et al.	707/102

FOREIGN PATENT DOCUMENTS

WO	WO 98/34189	*	8/1998	705/14

OTHER PUBLICATIONS

Press Release: "NetZero Launches New Advertising–driven, Free Internet Access Sevice; Startup to Combine Complimentary Access with Targeted, Personalized Ads", http://www.netzero.net/company/19981019nzlaunch.html 10/98.

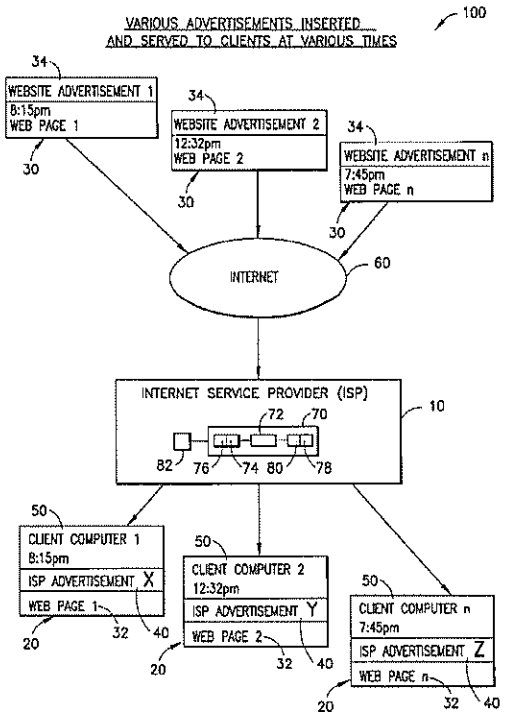
* cited by examiner

Primary Examiner—Stephen Gravini
(74) *Attorney, Agent, or Firm*—Stroock & Stroock & Lavan LLP

(57) **ABSTRACT**

The present invention advantageously provides to Internet Service Providers (ISP) precise control over who receives an advertisement. Thus, in accordance with the present invention, an ISP provider may now offer advertisers precision advertising. An ISP provider has access to precise demographic data on each of the ISP's customers. The ISP provider also has access to data on the periods of usage, including the type of customers accessing the Internet during such periods of usage. With this information, which is available only to the ISP provider, a profile may be compiled by the ISP provider that provides precise information on the ISP customers (e.g., demographic data) and the periods of heaviest Internet access by the various different ISP customer groups (e.g., 20–35 year old males, retired persons, children, etc.).

15 Claims, 4 Drawing Sheets



US007376714B1

(12) **United States Patent**
Gerken

(10) **Patent No.: US 7,376,714 B1**
(45) **Date of Patent: May 20, 2008**

(54) **SYSTEM AND METHOD FOR SELECTIVELY ACQUIRING AND TARGETING ONLINE ADVERTISING BASED ON USER IP ADDRESS**

(76) Inventor: **David A. Gerken**, 13955 W. Tahiti Way, #368, Marina Del Rey, CA (US) 90292

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 853 days.

(21) Appl. No.: **10/817,593**

(22) Filed: **Apr. 1, 2004**

Related U.S. Application Data

(60) Provisional application No. 60/459,923, filed on Apr. 2, 2003.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/219**

(58) **Field of Classification Search** 709/219, 709/223, 227; 705/14
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,948,061	A *	9/1999	Merriman et al.	709/219
6,151,631	A	11/2000	Ansell et al.	
6,182,050	B1 *	1/2001	Ballard	705/14
6,339,761	B1 *	1/2002	Cottingham	705/14
6,487,538	B1 *	11/2002	Gupta et al.	705/14
6,665,715	B1 *	12/2003	Houri	709/223
2001/0039210	A1	11/2001	ST-Denis	
2002/0010626	A1	1/2002	Agmoni	
2002/0016831	A1	2/2002	Peled et al.	
2002/0120629	A1	8/2002	Leonard	
2003/0036949	A1	2/2003	Kaddeche et al.	

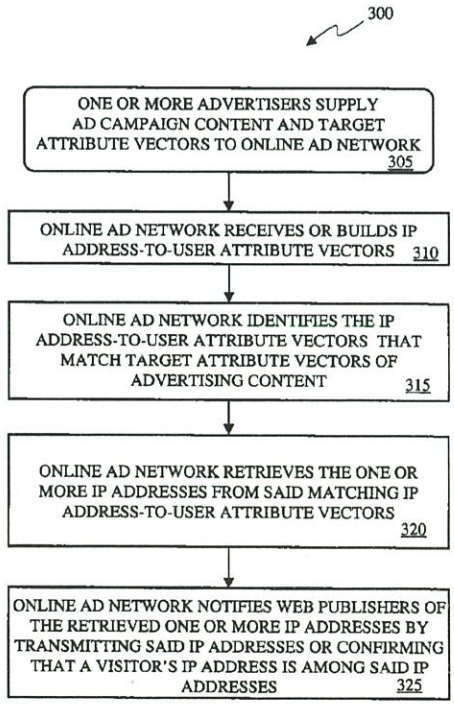
* cited by examiner

Primary Examiner—David Y. Eng
(74) *Attorney, Agent, or Firm*—Michael Blaine Brooks, P.C.; Michael B. Brooks

(57) **ABSTRACT**

The present invention provides a system and method for selectively acquiring and targeting online advertising inventory based on users' Internet Protocol (IP) addresses. In one aspect of the invention, Web publishers are made aware of IP addresses of interest, determined by matching attributes of current Internet users for whom IP addresses are known and targeting attributes of ad campaigns. Then, for each site visitor from one of said IP addresses, publishers choose whether to supply ad inventory to fulfill the immediate demand. Another aspect of the invention provides for targeting of online ads based on updated user IP addresses and some associated personal data provided by ISPs. An embodiment of the invention provides for a localized online advertising network in which ad inventory is selectively acquired from web sites, as required to fulfill immediate advertiser demand, and targeted by user zip code, as registered with users' ISPs.

25 Claims, 4 Drawing Sheets



BUSINESS BizPhilly

Comcast Funds Civil Rights Groups That Rallied Against New FCC Rules

Congress voted to repeal the internet privacy rules last week.

by FABIOLA CINEAS • *4/3/2017, 2:17 p.m.*

Comcast Center | Jeff Fusco

Last week the U.S. House of Representatives followed the Senate and voted to overturn new FCC rules that would have required Internet service providers like **Comcast** to get customers' permission before selling their online browsing data.

Supporters of the repeal have stated that regulators failed to listen to objections from the "Internet community" when the new rules were created under the Obama administration. But a report from *The Intercept* reveals that many of the objections in the Internet community are coming from civil-rights groups with "extensive financial ties" to telecomm companies like Comcast. And their objections to the FCC rules seem absurd and unrelated to their core missions, *The Intercept* points out.

Two such civil rights groups funded by Comcast are the League of United Latin American Citizens (LULAC) and the non-profit OCA – Asian Pacific American Advocates. The two organizations wrote a letter to the FCC, urging then-commissioner Tom Wheeler to reconsider the new rules. One reason provided in the letter is that the rules would deprive consumers of access to "new, innovative, and convenient products, services, and features" that they get through advertising. They also wrote that "Many consumers, especially those households with limited incomes, appreciate receiving relevant advertising that is keyed to their interests and provides them with discounts on the products and services they use."

But the FCC regulations would have actually allowed ISPs to sell their customers' browsing data for such target advertising if users gave them explicit permission. They would also be notified of how their browsing data was being used. The letter states that the FCC's umbrella of "sensitive

data" should be limited only to information about location, children's data, social security numbers, and other information about health and finances. All other information is fair game.

Comcast and Verizon are listed as business advisory council members to the OCA and sponsored the organization's gala in 2016. Comcast along with other ISPs like AT&T, Charter, and Verizon are a part of the League of United Latin American Citizens' "corporate alliance," which provides advice and assistance according to the group. *The New York Times* reported that Comcast gave the organization $260,000 between 2004 and 2012.

The Intercept says neither OCA nor LULAC immediately responded when asked if contributions from ISPs influenced their decision to engage on the privacy rule. Comcast did not respond to request for comment on the FCC regulations from *Philadelphia* magazine.

"It is terrifying that our elected representatives just gave Comcast, Verizon, and other major ISPs a windfall – at massive cost to their own constituents. Here in the poorest big city in the United States, the revocation of these rules means all bets are off," said **Hannah Jane Sassaman** of Philly's Media Mobilizing Project, which has rallied in opposition to the bill. "It means that poor people's identities, dreams, and organizing can be mined for profit for the highest bidding advertiser."

Others have recognized that Comcast and other broadband providers have also ramped up their lobbying efforts against the FCC rules and are in a position to benefit from further deregulation.

Moving forward, President Trump is expected to sign the bill into law.

Follow @fabiolacineas on Twitter.

Read More About:

Comcast Internet Privacy Internet Providers

Fabiola Cineas

Senior Editor

@fabiolacineas

fcineas@phillymag.com

5.

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

STATE PRIVACY AND SECURITY COALITION

February 21, 2020

Rep. Edward Butler
House Committee on Commerce and Consumer Affairs
New Hampshire State Legislature
33 North Street
Concord, NH 03301

Re: HB 1680- amendment relating to Maine ISP privacy

Dear Chair Butler and members of the Committee:

On behalf of the hundreds of the nation's leading technology and innovation companies our organizations represent, the associations listed below write to express our opposition to a proposed amendment, which would change the bill to language very similar to the Maine ISP privacy bill that was passed by the Legislature last year. While we appreciate the desire to address consumer privacy protections, Maine's law should not serve as a model to be passed in other states; over half the states in the country have considered and rejected this type of legislation. New Hampshire would be best served to determine the problems it seeks to solve and carefully examine solutions, rather than rushing to pass a law that would make it an outlier from the other states.

Consumer's benefit most from being protected by a predictable, consistent regulatory framework that has a history of successfully governing how their online data is handled and protected. Maine's law may very well harm the consumers it purports to protect. By prohibiting the "use" of data, it will impede product and service improvements and other innovations. Nor does it contain flexibility for companies to protect consumers from the broad array of cybersecurity risks that exist in today's world. It could also very well disrupt the user experience, e-commerce, and throw sand in the gears of the Internet experience most consumers expect.

Additionally, federal law already protects the online privacy of New Hampshire residents. There is no gap in federal law that would permit ISPs to violate their customers' privacy. The Federal Trade Commission (FTC) currently has oversight and enforcement authority over ISP consumer privacy practices. The FTC is the established expert agency and a strong enforcer of consumer privacy interests, and has brought over 500 cases protecting the privacy and security of consumer information, and also has a staff of 40+ privacy experts who police internet and data privacy. In developing its privacy framework, the FTC engaged in a thoughtful, multi-year

process that solicited and took into account input from many stakeholders and was praised by privacy and consumer groups.

Additionally, our member companies do not sell their customer's personal information and they take their consumer's privacy concerns very seriously. ISP customers are already protected from the sale or any surprising use of their data, such as their personal web browsing history. All major ISPs have designed their privacy practices based on the FTC's robust privacy framework, which includes guidance on transparency and choice and requires opt-in consent for use or disclosure of sensitive categories of data.

As mentioned above, no other state has passed language similar to that contained in Maine's bill. Because broadband service is critical to e-commerce, particularly in a rural state, creating new and different standards in New Hampshire risks disrupting a significant portion of the state's innovation economy and would have major unintended consequences for consumers and businesses as ISPs are forced to adjust their investment and technology deployment plans based on a singular set of rules for the state. Additionally, adding new state requirements will only confuse consumers who should have the ability to rely on clear, national uniform privacy protections across the Internet. Consumer's benefit by keeping a single, uniform set of privacy obligations governing broadband data, which is based on the FTC's time-tested framework.

In conclusion, given the ever-evolving nature of the Internet, online privacy is a complex issue we continue to ask the Committee to hold off on enacting privacy legislation this session and instead carefully determine the problems it seeks to solve. We thank you in advance for your consideration. Please do not hesitate to reach out with any questions.

Sincerely,

Christina Fisher
Executive Director, Northeast
TechNet
cfisher@technet.org
508-397-4358

Andrew Kingman
General Counsel, State Privacy & Security Coalition
Senior Managing Attorney, DLA Piper
Andrew.Kingman@dlapiper.com
(774) 313-9543

6

Testimony of Russell Hanser

On Behalf of the New England Cable & Telecommunications Association (NECTA)

on

New Hampshire HB 1680 and Proposed Amendment 2020-0560H

February 21, 2020

EXECUTIVE SUMMARY

- **HB 1680 and proposed amendment 2020-0560 are unnecessary.**
  - ***Enforceable ISP Commitments.*** ISPs have made substantial commitments regarding their privacy practices, which the FTC and the New Hampshire Attorney General can enforce.
  - ***Preexisting Legal Requirements.*** ISPs already are subject to a web of federal and state requirements. The FTC alone brought more than 100 privacy cases within the last decade (only one of which involved an ISP). Recent actions against Facebook and Google/YouTube resulted in fines of $5 billion and $170 million, respectively.
  - ***Promise of Federal Legislation.*** Congress is working actively on federal privacy legislation. Three pending bills, reflecting broad agreement on key principles, each would provide what consumers really need – a coherent and unified national framework.
  - ***No Unique ISP-Related Risks.*** Suggestions that ISPs pose unique risks to consumer privacy are wrong. Multiple laws govern privacy practices broadly and the specific privacy issues posed by particular types of sensitive data. Further, the rise of encryption and the fact that most consumers access the Internet using multiple devices mean that – contrary to some claims – ISPs cannot monitor users' traffic, whereas large edge providers can.
- **HB 1680 and proposed amendment 2020-0560H would harm consumers.**
  - ***Ambiguous Application.*** Customers are unlikely to realize that the law imposes no limits on search engines, social networks, and other edge providers, which could lead them to the sharing of information that they did not want disclosed.
- **HB 1680 and proposed amendment 2020-0560H conflict with the bipartisan, generally applicable, and broadly agreed-upon framework that has been in place since the Obama Administration's 2012 Privacy Report.**
  - ***Generally Applicable Approach.*** Whereas HB 1680 and proposed amendment 2020-0560H single out ISPs, privacy policymakers and enforcers have long recognized – on a bipartisan basis – that data should be treated alike irrespective of the identity of the entity that possess the data. A generally applicable framework of this type could allow for action against a Cambridge Analytica or another entity that unlawfully obtained user data, while HB 1680 and proposed amendment 2020-0560H could not.
  - ***Role of Sensitivity and Context in Obama Approach.*** The Obama-era Privacy Report ensured that companies could use data for legitimate business activities by applying substantial restrictions only on the use or disclosure of *sensitive* personal information and establishing tiers of consumer choice depending on the specific context. HB 1680 and proposed amendment 2020-0560H apply severe restrictions with respect to *all* data in *all* circumstances.

- **HB 1680 and proposed amendment 2020-0560H are overbroad in many respects.**

  - ***Overbreadth.*** The amended bill is overly broad in a host of ways. For example, it applies the same limits to use of sensitive and non-sensitive information, covers even anonymized data and other data not linked to a particular customer, allows customers to guard even information that is outside of the already overbroad customer information category, and applies to every customer located in New Hampshire, irrespective of whether the customer is a resident of the state.

- **HB 1680 and proposed amendment 2020-0560H's private right of action will undermine, not promote, consumer privacy.**

  - ***Shift Toward Protracted Court Battles With Little Upside for Consumers.*** The bill would redirect enforcement efforts from regulatory bodies and state attorneys general, who are well-positioned for such activities, to class-action suits, which often are protracted and fail to provide any benefit to the individuals alleging harm.

- **HB 1680 and proposed amendment 2020-0560H violate the First Amendment**

  - ***Speaker-Based Speech Limitations.*** Because it limits the expression of ISPs but not other speakers, HB 1680 and proposed amendment 2020-0560H violate the First Amendment. For this reason, the identical Maine law is currently subject to constitutional challenge.

- **HB 1680 and proposed amendment 2020-0560H are preempted by federal law.**

  - The bill conflicts with the decision by Congress and the President to reject an ISP-specific privacy framework.

  - The bill also conflicts with the FCC's determination that broadband customers are best protected by a regime focused on FTC and state enforcement of broadly applicable consumer protection mandates.

Chairman Butler, Vice Chairman Williams, and distinguished Members of the Committee:

Thank you for the opportunity to submit this testimony regarding legislation introduced before this committee, HB 1680 and proposed amendment 2020-0560H.

My name is Russell Hanser. I am a partner at the law firm Wilkinson Barker Knauer, LLP, where I focus on privacy, communications, artificial intelligence, and cybersecurity issues. For more than 14 years, I have advised and represented wireless, wireline, and cable broadband providers in privacy proceedings before the Federal Communications Commission (FCC) and in the courts. In all, I have practiced communications law for nearly two decades. Prior to joining Wilkinson Barker Knauer in 2005, I served as Legal Advisor to a Commissioner at the FCC, as Special Counsel to the FCC's General Counsel, and as Special Counsel to the Chief of the Competition Policy Division in the FCC's Wireline Competition Bureau. My involvement with these issues thus stretches back to the origins of the broadband Internet. I have taught Communications Law and Policy at the University of New Hampshire Law School. From 1999-2000, I was a law clerk to Judge Normal Stahl of the United States Court of Appeals for the First Circuit, here in Concord New Hampshire. I hold a B.A. from Amherst College, a J.D. from Harvard Law School, and an M.A. from Johns Hopkins University.

I am here today on behalf of NECTA, the regional trade association that represents private cable companies in New Hampshire and several other states in New England. NECTA commends the Committee for its attention to this very important issue. The challenges facing consumers' privacy are real, and we support efforts to address them. We are concerned about HB 1680 and proposed amendment 2020-0560H, however, because it diverges from the bipartisan, widely adopted, and well-established approach reflected by the approach that the Federal Trade Commission ("FTC") developed during the Obama Administration to respond to these challenges.

Other states, and other privacy regulators, have adopted this sensible, generally applicable framework. While protecting consumer privacy is a well-intentioned and laudable goal, HB 1680 and proposed amendment 2020-0560H's divergent approach would have serious consequences, failing to meaningfully protect—and even frustrating—New Hampshire consumers.

I. HB 1680 AND PROPOSED AMENDMENT 2020-0560H ARE UNNECESSARY.

As an initial matter, the bill before you is unnecessary, because (1) all major ISPs have made public commitments to protect their consumers' privacy, and these commitments are enforceable by both the FTC (which has been an active enforcer in this area, having brought over 500 privacy and data security cases) and the New Hampshire Attorney General, (2) even apart from their commitments, ISPs are subject to a number of federal and state requirements governing their practices with respect to consumer data, (3) federal legislators are working actively to establish a nationwide framework that would apply to all entities that obtain user information, and (4) allegations of ISP-specific risks to privacy are unfounded and contrary to marketplace facts.

First, ISPs have made substantial and publicly available commitments to protect their consumers' privacy – and these commitments are enforceable under federal and state law. In 2017, all major ISPs publicly committed to common transparency, consumer choice, data security, and data breach notification principles in connection with consumer data practices.[1] Some ISPs have made more detailed commitments. Comcast, for example, has told customers that "we do not track the websites you visit or apps you use through your broadband connection," do not use such information "to build a profile about you," and that the company "ha[s] never sold that information to anyone. Comcast further commits to customers that "[w]e don't sell, and

[1] These principles are available at https://prodnet.www.neca.org/publicationsdocs/wwpdf/12717ctia.pdf.

have never sold, your location data when you use our Xfinity Mobile service."[2] Similarly, other providers commit not to provide user information to third parties except when the consumer has expressly consented to such sharing and the recipient will use the information solely to fulfill a narrow set of functions, including authentication of the customer's identity, fraud protection, and protecting the user's financial accounts.[3]

In the event an ISP in New Hampshire were to violate its commitments, the New Hampshire Attorney General is empowered to take enforcement action under the New Hampshire Consumer Protection Act, which bars "any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state"[4] – terms well understood to bar practices that diverge from promises a provider has made to consumers. These enforceable commitments obviate any need for an ISP-specific privacy law.

Second, even apart from their commitments, ISPs are subject to a web of federal and state requirements governing their practices with respect to consumer data. The FCC has repealed its 2015 *Open Internet Order*, which reclassified ISPs as common carriers. As a result, ISPs are once again under the FTC's jurisdiction.[5] FTC Chairman Simons has stated that the FTC stands ready to "challenge deceptive and unfair privacy and security practices by ISPs,"[6] and the agency's actions have confirmed its willingness to take action. Last year, the FTC issued orders to seven major ISPs "seeking information the agency will use to examine how broadband

---

[2] Comcast's commitments are available at https://corporate.comcast.com/privacy.

[3] See, for example, AT&T's privacy policy, which is available at https://about.att.com/csr/home/privacy/full_privacy_policy.html.

[4] RSA 358-A.

[5] Section 5 of the FTC Act bars "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce," but excludes common carriers from its scope. 15 U.S.C. § 45(a).

[6] Remarks of Federal Trade Commission Chairman Joseph Simons, Free State Foundation Speech at Eleventh Annual Telecom Policy Conference (Mar. 26, 2019) available at https://www.ftc.gov/system/files/documents/public_statements/1508991/free_state_foundation_speech_march_26.pdf

companies collect, retain, use, and disclose information about consumers and their devices."[7] One need only review the FTC's track record to see that its aggressive privacy enforcement has revealed virtually no problems arising from the practices of ISPs. In a January 2019 report, the Government Accountability Office identified 101 privacy-related enforcement actions by the FTC in the past decade, *only one* of which involved an ISP. The others involved social media and search engine providers, software developers, and brick-and-mortar manufacturers also conducting business online, among others.[8] Recently, the FTC has taken action involving privacy harms by Facebook and Google/YouTube, resulting in fines of $5 billion and $170 million, respectively.[9]

Moreover, the New Hampshire Attorney General and New Hampshire consumers already have the ability to hold broadband providers accountable for unfair and deceptive acts or practices. If an ISP fails to adhere to representations it has made about its privacy practices to its customers, or if it neglects its duty to maintain reasonable data security safeguards, there are existing avenues of recourse under the New Hampshire Consumer Protection Act.

In addition to these federal and state consumer-protection laws, there already exist numerous laws protecting (for example) the privacy of medical information, of information regarding or obtained from children, and of financial information.[10] Laws such as these diminish

---

[7] Federal Trade Commission, Press Release, *FTC Seeks to Examine the Privacy Practices of Broadband Providers* (Mar. 26, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers.

[8] *See* Government Accountability Office, Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility (Jan. 2019) at 21, available at https://www.gao.gov/assets/700/696437.pdf.

[9] *See* https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions; https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[10] *See generally* Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506; Gramm-Leach-Bliley Act 15 U.S.C. § 6801 et seq.; Fair Credit Reporting Act, 15 U.S.C. § 1681.

substantially any sense of urgency as the committee considers this extremely complicated set of issues, and should dispel any suggestion that ISPs are currently free to share and use sensitive customer information at will.

Third, Congress is working actively on federal privacy legislation that would apply to all entities – not merely ISPs – and would establish a uniform nationwide framework. Three bills have emerged in Congress (one bipartisan bill in the House, two bills by the leading Republican and leading Democrat on the Senate Commerce Committee). The bills are similar: All of them provide a coherent framework that would apply broadly and uniformly to all entities subject to the FTC Act, and all of them provide consumers with extensive rights to control their personal data and limit companies' use and disclosure of personal data. Unlike HB 1160-FN, all of them distinguish between sensitive personal information such as medical, financial, or children's data (which is subject to opt-in consent) and non-sensitive information such as IP addresses (which is subject to opt-out consent). Unlike HB 1160-FN, all of them carve out de-identified data, allowing sharing of information that is not connected to any individual's identity and thus cannot harm that individual. They each provide consumers the right to access, correct, and delete their information, prohibit covered entities from maintaining and/or processing or transferring more information than reasonably necessary to carry out the purposes for which it was collected, and require covered entities to implement and maintain reasonable data security policies and practices. These are serious legislative efforts, founded on bipartisan consensus concerning core issues – and they eliminate any need for state-specific laws.

The likelihood of federal legislation in the near future is especially important because the regulation of online privacy is quintessentially a federal issue. Indeed, compliance with conflicting state privacy rules would not only be impossible for companies in the Internet

ecosystem, but would also create inconsistent privacy protections for consumers based upon where they live, work, or happen to access online services. This is why NECTA's members strongly support – and are encouraged by bipartisan progress in Congress to develop – robust federal legislation that would apply uniformly to all entities throughout the United States and would provide for enforcement by State attorneys general.

Fourth, suggestions that ISPs pose unique risks with respect to consumer privacy are flatly untrue. Recent technological developments have drastically limited ISPs' access to consumers' data when transmitted over their Internet connection. Widespread encryption is "pervasively limiting the ability of ISPs to see Internet activity."[11] The widely adopted HTTPS encryption standard, for example, prevents ISPs from seeing both the full URL[12] and the content of websites their customers visit.[13] To illustrate, if a customer conducts a Google search for "best bookstores in Concord," her ISP can "see" only that she contacted google.com; it *cannot* see what she asked Google to search for. For these and other reasons, "other companies often have access to more information and a wider range of user information than ISPs [and] ISPs have neither comprehensive nor unique access to information about users' online activity. Rather, the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts."[14] In addition, consumers today increasingly

---

[11] Peter Swire, et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* 25, Working Paper of The Institute for Information Security & Privacy at Georgia Tech (Feb. 29, 2016), https://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf ("Swire Study"); *see also* Cam Cullen, *Global Internet Phenomena Preview: Encrypted Traffic Dominates the Internet*, Sandwire (2018) (estimating that 75 to 90 percent of Internet traffic is encrypted), https://bit.ly/2O8fzri.

[12] A "URL" or Uniform Resource Locator is the text that represents information accessible over the Internet. For example, http://www.med.uscourts.gov is the URL for the Court's home page, while http://www.med.uscourts.gov/office-hours is the full URL that provides direct access to the page listing the clerk's offices' telephone numbers and hours of operations.

[13] *See* Swire Study at 26.

[14] *Id.* at 3.

access the Internet through multiple devices and, as a result, they typically use the services of more than one ISP.[15] In using several devices, many of which are mobile, consumers "constantly shift from one ISP to another, not just for home and work, but among many WiFi hotspots and other locations from which they connect to the internet," providing ISPs mere "episodic glimpses" of a customer's Internet usage.[16] These developments have *not*, however, affected the ability of *edge providers* and *software developers* – entities not covered by HB 1160-FN – to access Internet-usage information.[17] To the contrary, edge providers are obtaining ever more comprehensive and detailed customer information by tracking customers across devices.[18]

II. HB 1680-FN AND PROPOSED AMENDMENT 2020-0560H WILL HARM CONSUMERS.

ISP-only privacy laws like HB 1680 and proposed amendment 2020-0560H not only ineffective, they are also bad for consumers. Applying one set of laws to data-handling by ISPs and another set of laws to handling of the exact same data by an edge provider is a recipe for consumer confusion and could, in fact, lead consumers to exercise less care over their data disclosures. If New Hampshire adopts a privacy law that regulates the practices of ISPs alone, many consumers will not understand that the state's internet privacy law does not comprehensively protect their privacy on the internet. And those consumers who mistakenly believe that the law protects them across the ecosystem may be less careful with their data online. In this way, the law would harm consumer privacy.

Moreover, even consumers who generally understand the asymmetric nature of the law are unlikely to understand exactly which entities they interact with online are subject to which

---

[15] *See* Cisco, *Cisco Visual Networking Index (VNI), Complete Forecast Update, 2017–2022*, at 22 (Dec. 2018).

[16] Swire Study at 25.

[17] *See* Swire Study at 11-14.

[18] *See id.* at 116-18.

restrictions, under what circumstances. These consumers are likely to experience surprise and frustration when data that they thought was protected is bought and sold by, or subject to a data breach from, an edge provider.

Finally, consumers who fully appreciate the limited scope of the bill are likely to be frustrated by the enactment of a privacy law that does not address their primary concerns about control over their data across the entire internet ecosystem.

III. HB 1680 AND PROPOSED AMENDMENT 2020-0560H CONFLICT WITH THE GENERALLY APPLICABLE AND BROADLY AGREED-UPON FRAMEWORK ESTABLISHED BY THE OBAMA ADMINISTRATION IN 2012.

Consumers expect and benefit from a consistent privacy regime that protects their personal information regardless of who is collecting it.[19] The FTC's technology-neutral approach to privacy regulation[20] and the framework adopted in the Obama Administration's 2012 Privacy Report ("Obama Privacy Report")[21] do just that. The FTC spent months examining companies' practices, even holding a public workshop examining the practices of broadband providers, and it concluded that there was no need to single out broadband providers for heightened restrictions.[22]

---

[19] *See* Memorandum from Public Opinion Strategies and Peter D. Hart to the Progressive Policy Institute, Key Findings from Recent National Survey of Internet Users (May 26, 2016) (showing that 94 percent of consumers favor such a consistent and technology-neutral privacy regime, i.e., they overwhelmingly want the same privacy protections to apply to their personal information *regardless* of the entity that collects such information) available at https://www.progressivepolicy.org/wpcontent/ uploads/2016/05/Internet-User-National-Survey-May-23-25-Key-Findings-Memo.pdf.

[20] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012) ("FTC Report") at 15 (stating that the framework applies to "all commercial entities that collet or use consumer data"), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[21] Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012) ("Obama Privacy Report") at 10 (stating that the framework applies to all "commercial uses of personal data"), available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

[22] FTC, *The Big Picture: Comprehensive Online Data Collection* (2012), available at https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection.

The European Union's General Data Protection Regulation ("GDPR"), which is widely regarded as the most rigorous privacy regime in the world, similarly applies to all commercial entities doing business in Europe that collect, use, and share personal information. All of these regimes reflect the reality of the 21st century Internet economy by regulating the same data consistently across the digital ecosystem, regardless of the nature of the entity involved.

HB 1680 and proposed amendment 2020-0560H take a starkly different approach. They heavily regulate a single group of companies in the online data services ecosystem—providers of "broadband Internet access service," which have had a strong track record in protecting consumer privacy—but leaves edge providers—including search engines, social networks, mobile apps, other large platform providers, and data brokers whose principal business model is to sell and monetize consumer data —outside the scope of the law. By narrowly focusing on ISPs, HB 1680 and proposed amendment 2020-0560H fail to protect consumers in the areas where their privacy is most at risk.

Nor does the bill explain how consumers will be protected if their personal information is disclosed to third parties (with the required opt-in consent) who mishandle their information, as was the case, for example, in the Cambridge Analytica situation that spawned much concern about these issues.[23] Indeed, many of the data privacy and security incidents reported over the last year have been caused by such third parties. The bill's failure to even address this set of issues illustrates that this legislation does not fully protect consumers.

In addition to covering *all* entities and addressing the obligations of third parties, the Obama Administration and FTC privacy frameworks ensured that companies were permitted to

---

[23] Kathleen Chaykowski, *Lawmakers Grill Facebook on Privacy Practices, Pitfalls of Ad-Fueled Business,* Forbes (Apr. 10, 2018), available at https://www.forbes.com/sites/kathleenchaykowski/2018/04/10/lawmakers-grill-facebook-on-privacy-practices-pitfalls-of-ad-fueled-business/#21ee1a433705.

use data to engage in legitimate business activities, innovate, and adapt to ever-changing technology. They achieve this important balance by focusing on actual privacy harms to consumers and subjecting *sensitive* personal information to heightened protection through opt-in consent, while allowing greater flexibility to use and share *non-sensitive* information and enabling entities to use and disclose data when consistent with the context of the relationship between the consumer and the company and within consumers' expectations.[24]

Drawing on these principles, the FTC established tiers of consumer choice that allow companies to infer consent for practices that are consistent with the context of the consumer's relationship to the company.[25] The Obama Administration took the same context-driven approach, recognizing that consent could be inferred for certain uses and disclosures of data. The Obama Privacy Report explained, for instance, that companies could "infer consent to use and disclose personal data to achieve objectives that consumers have specifically requested, as long as there is a common understanding of the service," to "conduct marketing in the context of most first-party relationships, given the familiarity of this activity," and to use personal data for purposes that are "common," such as "analyzing how consumers use a service in order to improve it, … complying with … legal obligations, and protecting intellectual property."[26]

HB 1680 and proposed amendment 2020-0560H, on the other hand, would require ISPs (and only ISPs) to obtain opt-in consent from consumers, subject to overly narrow exceptions, before companies use, disclose, or make available to any person a broad range of information. As written, the bill would not even allow a broadband provider to use information about customers'

---

[24] FTC Report at 36-44; 47-48

[25] *Id.*

[26] Obama Privacy Report at 17.

use of broadband services for well-recognized internal business purposes, such as improving the services or developing new products and services, unless the consumer provided *opt-in* consent by affirmatively telling the broadband provider that such use was permissible. And it would not allow a broadband provider to use such information to protect its networks and provide a secure online environment for its customers – something customers not only expect, but demand from their providers. These results are even more bizarre when one considers that every other entity on the Internet will be able to use the same information for these same purposes without opt-in consent.

Moreover, HB 1680 and proposed amendment 2020-0560H's advertising and marketing exception allows broadband providers to market only their own "communications-related services" – a term that the bill does not define. This restriction, too, departs from the FTC's approach, which allows companies to infer consent for most first-party marketing, recommends that companies provide consumers with an *opt-out* mechanism when the context of marketing does not allow consent to be inferred, and recommends *opt-in* consent only in limited circumstances, such as when companies deliberately collect and market using sensitive data.[27] HB 1680 and proposed amendment 2020-0560H, in contrast, would prevent broadband providers from continuing to rely on this privacy framework, while allowing other online entities to continue doing so. More specifically, under the law, an ISP can send its customers information about discounted offers for a package of broadband and phone services but ***not*** a discounted package of broadband and non-communications-related products and services. This approach does not serve any privacy goal. It only harms consumers by depriving them of commonplace cost-saving benefits. The bill also goes far beyond not only the FTC's framework, but even the

[27] FTC Report at 40-41; 57-60.

2016 Federal Communications Commission ("FCC") broadband privacy order, which allowed ISPs to engage in all first-party marketing based on non-sensitive personal information subject to more flexible *opt-out* consent.

IV. HB 1680 AND PROPOSED AMENDMENT 2020-0560H ARE TERMINALLY OVERBROAD.

Complicating matters further, the bill is overbroad in numerous respects. For example, it defines "customer personal information" without distinguishing between sensitive data (e.g., social security numbers; health, financial, or children's information; or precise geolocation data) and non-sensitive data (e.g., names, addresses, demographic data, and device identifiers). Yet, not all data, even if misused or wrongfully disclosed, has the same potential to harm consumers. For that reason, the FTC carved out five categories of data that it deemed particularly sensitive and in need of heightened protection such as opt-in consent.[28] The GDPR and the California Privacy Protection Act also distinguish between these two types of personal information and apply more restrictions to sensitive data.

Moreover, HB 1680 and proposed amendment 2020-0560H's definition of "customer personal information" is overbroad and lacks any limiting principle. It includes two categories: (1) "personally identifying information about a customer, including but not limited to the customer's name, billing information" and so forth, and (2) "information from a customer's use of broadband Internet access service, including but not limited to" web browsing history, app usage history, device identifiers, as well as other listed and unlisted information.[29] The bill does not require information in category (1) to be paired with information from category (2), or for

[28] The FTC identified the following categories of data as sensitive: children's information, financial information, health-related data, social security numbers, and precise geolocation information. FTC Report at 59.

[29] HB 1680-FN, § III.

information in category (2) to be linked or linkable to an identified individual, in order for use or disclosure to be permissible, as is typically the case in privacy laws. Thus any "information from a customer's use of broadband Internet access service"—regardless of whether it is connected to an *identifiable* or even a *specific* or *particular* individual—would be subject to the bill's prohibitions. The bill would potentially capture virtually all data that broadband subscribers generate when they use broadband services, regardless of whether it has been de-identified, anonymized, or aggregated, prohibiting broadband providers from using, disclosing or making such information available unless the provider obtains the customer's prior consent or can satisfy the narrow requirements of the bill's limited exceptions. This sweeping definition may impede providers' ability to conduct business and network operations and substantially degrade the Internet experiences of customers in New Hampshire, without providing any meaningful benefit to consumers because every other company on the Internet already has access to, collects, and/or uses this information.

These technical infirmities also make other features of HB 1680 and proposed amendment 2020-0560H unworkable. For example, the bill prohibits broadband providers from making consent to the disclosure of personal information a condition of "serv[ing]" the customer. The bill does not indicate whether it prohibits such conditions only in connection with providing broadband Internet access service or in connection with providing *any* service that a provider may offer. Either way, it will not be possible for providers to function if they have to provide certain services to consumers who refuse to consent to the disclosure of their personal information necessary to facilitate such services in the first place.

HB 1680 and proposed amendment 2020-0560H also prohibit offering customers a discount for agreeing to provide consent. This goes far beyond, and will cause more harm than,

the similar controversial provision in the California Privacy Protection Act. The bill would prohibit – without exception – companies from providing discounted services, loyalty programs, and other financial incentives, such as access to content in exchange for receiving targeted advertising. Provided that the terms of the exchange are clear, there is no privacy benefit to be gained by prohibiting this exchange, and it will only serve to diminish consumers' online experience and access to price discounts and other benefits. Even the GDPR provides consumers greater choice by allowing companies to offer ad-supported content in exchange for consumers' consent to receive online ads.[30]

In addition, the bill allows consumers to prohibit providers' use of information that is *not* "customer personal information." It is not clear what such information would be, but in any event, this provision serves no consumer protection purpose and would interfere with a host of operations online that consumers expect to be executed quickly and without service interruption. For instance, this provision could affect providers' ability to share information necessary to enable the transmission of data across networks. No other privacy law – except the Maine law being challenged in court – permits customers to prohibit use of any type of information while simultaneously requiring the ISP to provide service. Because ISPs rely on certain information to operate their networks, the two concepts are simply not compatible.

In addition, the bill applies not to citizens or residents of New Hampshire, but to the personal information of *any* customers who happen to be "located" in New Hampshire while using broadband service on a mobile device and are billed for that service in the state, even if the individual resides in another state. In many circumstances, it will not be possible for a provider to

---

[30] Regulation (EU) 2016/697 of the European Parliament and of the Council, Art. 7 (Apr. 27, 2016), *available at* http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

know where a customer is located without collecting additional information about the precise geolocation of every individual with which it interacts. As such, the extraterritorial application of the bill would undermine the key goal of *protecting* consumers' privacy by forcing broadband providers to track the movements and locations of all customers at every moment in time. And yet, the bill requires providers to obtain express affirmative consent from customers before using precise geolocation information for any purpose other than those listed in the exceptions, which do not include determining a customer's location for purposes of compliance with the bill. Surely, that cannot be the intent of the bill, yet that is how it currently reads. And if such precise location information cannot be obtained by the business, compliance will be impossible.

V. HB 1680 AND PROPOSED AMENDMENT 2020-0560H'S PRIVATE RIGHT OF ACTION WILL UNDERMINE, NOT PROMOTE, CONSUMER PRIVACY.

In addition to the above, HB 1680 and proposed amendment 2020-0560H go far beyond the current federal framework and other state privacy laws by including a broad private right of action with statutory damages for a breach of *any* personal information, including information that, if disclosed, would present no privacy or security risk to consumers whatsoever. This would allow plaintiffs (or, more accurately, their attorneys) to potentially recover damages of between $10 million and $75 million from a company that inadvertently disclosed the IP addresses and browser types of 100,000 consumers who visited the company's website, even though the disclosure of such information would not harm consumers (and might not involve the disclosure of any user's identity at all). This broad private right of action with uncapped statutory damages and no requirement that consumers show even a threat of harm will do nothing to protect the privacy and security of consumers. To the contrary, it would actually *reduce* effective privacy protection by diverting resources and management attention from privacy-by-design and proactive compliance, toward defensive action to avoid lawsuits and pay damages, and it could

even put smaller companies out of business altogether. Moreover, a review of recent class actions shows that the likely winners would be class action lawyers, not consumers:

- Recent class action settlements with large technology companies alleged to have violated privacy laws have resulted in windfalls for the attorneys while class members were left empty-handed – in one case, class attorneys received $3.2 million and the 129 million class members received nothing; in another, attorneys and the class representatives received $3 million while the class members, again, received no compensation whatsoever.
- Courts that approved these and similar settlements did not impose any injunctive requirements on the defendants, leaving companies uncertain about how best to comply in the future and without incentive to modify their conduct.
- In a regime focused on private actions, plaintiffs are forced to wait years while cases wind through the courts, whereas regulators can act with dispatch and provide coherent administration of the law.

The most effective way to regulate privacy and protect consumers is through enforcement actions brought by the state, not through a private right of action.

VI. HB 1680 AND PROPOSED AMENDMENT 2020-0560H VIOLATE THE FIST AMENDMENT.

Even more problematically, the bill as amended would violate the First Amendment of the U.S. Constitution. It is well established that the First Amendment protects companies' ability to communicate with existing and potential customers, and rules that single out and restrict one class of speakers – such as ISPs – are subject to heightened scrutiny. HB 1680 and proposed amendment 2020-0560H do precisely that. They impose unique, discriminatory restrictions on ISPs' ability to engage in commercial speech while leaving other entities that use the exact same

information in the same medium for the same purposes free to continue to engage in such speech. The U.S. Supreme Court held in *Sorrell v. IMS Health Inc.*, that such discriminatory speaker-based restrictions violate the First Amendment.[31] The bill imposes speaker-based restraints because it is "aimed at" and burdens just one category of speaker — ISPs and ISPs alone. It leaves other speakers (including edge providers, data brokers, and offline retailers) free to use the same or even greater quantities of customer personal information, regardless of how sensitive it may be, for any purpose whatsoever. The bill thus "has the effect of preventing [ISPs] — and only [ISPs] — from communicating . . . in an effective and informative manner."[32] As leading Constitutional Law scholar Lawrence Tribe has observed, an ISP-specific privacy framework cannot withstand First Amendment scrutiny.[33] Likewise, in a recent op-ed, Harvard Law School professor Richard Fallon concludes that the Maine law that HB 1680 and proposed amendment 2020-0560H mimic, which constrains "only internet-service providers' privacy practices and not those of edge providers," renders the law "more vulnerable to constitutional challenge than a nondiscriminatory privacy-protection statute would be."[34] In the Supreme Court's words: "[G]overnment regulation may not favor one speaker over another."[35] It is for this reason, among others, that groups representing wireless, cable, and wireline ISPs have challenged the Maine legislation on which HB 1680 and proposed amendment 2020-0560H is based in federal court.[36] While this bill is not good policy under any circumstances, it would be prudent for this body to, at

---

[31] 564 U.S. 552, 567 (2011).

[32] *Id.* at 564.

[33] *See* Lawrence H. Tribe & Jonathan Massey, The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment (May 26, 2016), *available at* https://ecfsapi.fcc.gov/file/60002077291.pdf.

[34] *See* Richard H. Fallon, Jr., Maine can do more to regulate internet privacy, BANGOR DAILY NEWS (Jan. 22, 2020), available at https://bangordailynews.com/2020/01/22/opinion/contributors/maine-can-do-more-to-regulate-internet-privacy/.

[35] *Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 828 (2000).

[36] *See ACA Connects et al. v. Frey et al.*, Case 1:20-cv-00055-LEW (D. Me.).

the very least, forbear from adopting this bill until the courts have spoken on the constitutionality of the Maine law, which is virtually identical.

VII. HB 1680 AND PROPOSED AMENDMENT 2020-0560H ARE PREEMPTED BY FEDERAL LAW.

Finally, HB 1680 and proposed amendment 2020-0560H are preempted by federal law because they directly conflict with and deliberately thwart federal determinations about the proper way to protect consumer privacy. The United States Constitution's Supremacy Clause "nullifies state laws that interfere with, or are contrary to, federal laws,"[37] including where a state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[38] HB 1680 and proposed amendment 2020-0560H would do just this.

In April 2017, Congress passed, and the President signed, a Joint Resolution repealing Federal Communications Commission rules applying privacy requirements to ISPs but not to other entities. The Joint Resolution reflected Congress's judgment that imposing privacy rules only on ISPs and not any other actor in the Internet ecosystem would undermine the public interest by creating a false sense of privacy, sowing confusion for both consumers and businesses, stifling competition, and impeding innovation in the Internet marketplace. Congress also made clear that a uniform, technology-neutral approach, rather than a patchwork of burdensome regulation, was necessary to give consumers consistent privacy protection. As members of Congress explained, the Joint Resolution advanced the goal of "restoring regulatory balance to the internet ecosystem" by establishing "a single, uniform set of privacy rules" administered by the FTC.[39] HB 1680 and proposed amendment 2020-0560H would effectively undo this act of

---

[37] *Bower v. Egyptair Airlines Co.*, 731 F.3d 85, 92 (1st Cir. 2013).
[38] *Crosby v. National Foreign Trade Council*, 530 U.S. 363, 373 (2000).
[39] 163 Cong. Rec. at S1928 (statement of Sen. Thune); *see also* 163 Cong. Rec. at H2495 (statement of Rep. Lance) (Congress sought to "provide American consumers with a consistent set of privacy rules").

Congress by reinstating privacy regulations only on ISPs and not any other companies. Indeed, the bill would not only reinstate many of the FCC rules that Congress vacated, but would enact a more stringent regime that that omitted the exceptions for non-sensitive information that the FCC had adopted. As a result, HB 1680 and proposed amendment 2020-0560H would conflict with the Joint Resolution's repeal of the FCC's broadband privacy rules and undermine the federal objectives that Congress sought to promote through this repeal.

The bill also would conflict with the FCC's *Restoring Internet Freedom Order*.[40] Acting pursuant to congressionally delegated authority in the *RIF Order*, the FCC determined that the best way to protect consumers' privacy interests "without imposing costly burdens on ISPs" is to pair mandatory privacy disclosures,[41] with FTC enforcement of those disclosures.[42] That approach applied the FTC's technology-neutral privacy framework to ISPs and non-ISPs alike, instead of imposing restrictions only on ISPs and not any other companies regarding the use of consumer data.[43] In upholding the *Restoring Internet Freedom Order* in relevant part, the United States Court of Appeals for the D.C. Circuit specified that, to the extent a state requirement conflicted with that decision, it would be subject to conflict preemption.[44] HB 1680 and proposed amendment 2020-0560H conflict with and would frustrate the FCC's determination about the best way to protect consumers' privacy interests. For this reason, too, it is preempted.

* * *

Privacy is a complicated issue that transcends industries, business models, and state borders. NECTA members believe strongly in protecting their customers' privacy, and believe

---

[40] Declaratory Ruling, Report and Order, and Order, *Restoring Internet Freedom*, 33 FCC Rcd 311, *petitions for review denied in pertinent part, Mozilla Corp. v. FCC*, 940 F.3d 1 (D.C. Cir. 2019).
[41] *Id.* ¶ 223.
[42] *Id.* ¶ 244.
[43] *Id.* ¶¶ 181-183, 244-245.
[44] *Mozilla*, 940 F.3d at 85.

that those customers will benefit most from a regime that applies equally to *all* entities that have access to their data. For that reason, NECTA and its members are strong supporters of a national, generally applicable privacy framework. Indeed, we are working with federal legislators to help them develop robust federal privacy legislation, and are pleased that a robust and dynamic process is underway as Congress evaluates how such legislation should be framed. We therefore respectfully urge the Committee to not move this bill forward and to continue to work with industry and other stakeholders to review and further consider this important topic.

Thank you again for the opportunity to appear before you today.

Testimony of
Professor Daniel Lyons
Boston College Law School

Before the New Hampshire House Commerce and Consumer Affairs Committee
Hearing on House Bill 1680, An Act Regulating the Collection of Personal Information by Broadband Internet Access Service Providers (as amended)

February 21, 2020

Chairman Butler, Vice Chairman Williams, and members of the Committee:

I'd like to thank the committee for allowing me to comment today. My name is Daniel Lyons, and I am a professor at Boston College Law School, where I teach and research in the areas of telecommunications, Internet law, and federalism.

I would like to address two issues today. First, given the competitive dynamics of the Internet ecosystem, it makes very little sense to single out Internet service providers to bear a greater privacy burden than other companies. Second, when leveling the playing field, an opt-out privacy model is preferable to an opt-in model.

First: It is a mistake to create a new, more stringent privacy regime that applies to ISPs but not Internet-based companies such as Google, Amazon, and Facebook. This creates an unlevel playing field in the market for digital advertising dollars. These Internet-based companies are subject to rules by the Federal Trade Commission, which generally requires them to notify consumers regarding what information is collected and how it is used, and to allow consumers to "opt out" of such collection efforts. But HB1680 reverses this presumption for ISPs: they cannot collect such data unless the consumers affirmatively "opts in." This distinction is fairly trivial for consumers, but it distorts the competitive dynamics of the Internet ecosystem by putting ISPs at a disadvantage in the market for digital advertising dollars.

I imagine that some supporters justify this unlevel playing field by highlighting the allegedly "privileged place" that ISPs occupy in the network. One could argue that because ISPs control the wires that carry information to and from the consumer's home, the ISP is in a unique position so track the consumer's activities online. But this is misleading. First, my home broadband provider can only gather, at most, information about my online activity while I am at home. By comparison, Google can capture all my activity while logged into my Google account whether at home, at work, or on mobile networks, if, like me, you use a phone powered by Google's Android operating system. My ISP has no way of knowing that I'm here today, for example, unless I tell them. But Google knew the moment I punched it into my map app. Second, as Professor Christopher Yoo notes, companies like Google can capture the content that we view online, while ISPs can only see metadata and traffic flow information (unless they engage in

deep packet inspection, which would raise concerns under the Electronic Communications Privacy Act).

Putting ISPs at a competitive disadvantage in the digital advertising market is especially problematic because ISPs were late to the digital advertising game. Think about the amount of free content you consume online each day—content that is largely paid for by advertising. News, blogs, games, social media. The vast majority is paid for by converting data into advertising. Now, appreciate this: As much as 2 out of every 3 dollars spent on digital advertising goes to only two companies: Google and Facebook. HB1680 not only distorts competition, it distorts competition in favor of the existing duopoly by making it harder for ISPs to break into this market. That's bad for competition and innovation online.

Second, independent of the issue of an unlevel playing field is the question of whether to favor an opt-out or opt-in model for privacy. HB1680 makes the same mistake that regulators in Europe and California made, one that is, unfortunately, common to many policy discussions in this area: it focuses on privacy in a vacuum, without considering the role that consumer data plays as the lifeblood of the Internet ecosystem. Online companies have perfected the old television-age adage that "if you're not paying, you're the product." It is the monetization of customer data that allows Google, Facebook, and countless other companies offer the "free" services that we all take for granted as the modern internet experience—and may someday bring broadband prices down as ISPs cover more of their fixed costs with advertising rather than subscription dollars. By changing the default rule governing data collection, HB1680 would shrink the pool of information available for monetization. At a minimum, this reduces revenues available for research and innovation and can cause companies to reduce the quality of their products to compensate. At worst, an opt out regime means those companies might start charging for services that they currently provide for free and higher prices for goods that could otherwise be subsidized through advertising—thus widening the digital divide by stratifying available services between the haves and have-nots. This is in part why the Federal Trade Commission has long endorsed opt-out rules as the proper balance between consumer protection and the benefits of digital advertising.

Importantly, both regimes give consumers ultimate control over their personal data by allowing them to choose what to share. The difference is that in an opt-out system, companies can cross-subsidize their operations by monetizing the data of those consumers who are indifferent about its use.

Thank you for your time and consideration.

8

Testimony of
BENJAMIN ARON
CTIA

In Opposition to New Hampshire House Bill 1680 as amended

Before the
New Hampshire House Commerce and Consumer Affairs Committee

February 21, 2020

Chair, Vice-Chair, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I am here in opposition to House Bill 1680 as amended. This bill would impose unworkable restrictions on how internet service providers (ISPs) manage customer-related information. If enacted into law, these restrictions would create serious unintended consequences that would harm New Hampshire businesses and consumers.

With the Federal Communications Commission's *Restoring Internet Freedom Order* in effect, the Federal Trade Commission (FTC) once again has authority over ISP consumer privacy practices. For over 20 years, the FTC has developed and enforced an effective privacy framework that applies to all players in the internet ecosystem. The FTC is an active consumer privacy enforcer. It has brought over 500 enforcement actions protecting consumer privacy. Through these enforcement actions, as well as through extensive policy guidance, the FTC has articulated a consumer privacy framework in which more sensitive personal information (e.g., biometric or genetic information, children's information, and health information) is generally subject to heightened protections, while there is greater flexibility to collect, use, and disclose non-sensitive information. The FTC is currently in the process of collecting extensive, detailed information from multiple ISPs for an industry-wide study into ISP privacy practices, ensuring the

FTC remains a well-educated and well-equipped consumer privacy enforcer.[1] In addition, the New Hampshire Attorney General already has the authority to address unfair or deceptive acts or practices relating to consumer privacy under state consumer protection laws. Because of these existing federal and state measures, and other privacy laws, there is no gap in ISP customers' privacy protections that New Hampshire needs to fill.

HB 1680 as amended would create two sets of rules that are different for various entities within the internet ecosystem. This would lead to widespread consumer confusion about which rules apply to their data and work to create an uneven playing field. Internet users overwhelmingly prefer a single national standard. Survey results submitted to the FCC showed that 94 percent of internet users believe all companies touching their online data should follow the same privacy rules.[2] These findings indicate that state legislation, like HB 1680 as amended, targeting ISPs would in fact be inconsistent with what consumers actually want.

In addition, ISPs do not have unique access to consumer data. A study by noted privacy expert Peter Swire found that ISP access to consumer data is not comprehensive, that technological developments place substantial limits on ISP visibility, and ISP access to user data is not unique – other companies may have access to more information and a wider range of user information.[3] Furthermore, consumers no longer use a single stationary device. Today consumers

---

[1] Federal Trade Commission, "FTC Revises List of Companies Subject to Broadband Privacy Study," https://www.ftc.gov/news-events/press-releases/2019/08/ftc-revises-list-companies-subject-broadband-privacy-study, last accessed 2/19/2020; Federal Trade Commission, "FTC Seeks to Examine the Privacy Practices of Broadband Providers," https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers, last accessed 2/19/20.

[2] The Progressive Policy Institute, "Consumers Want One Set of Rules Protecting Their Information," http://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rules-protecting-information/, last accessed 2/6/2020.

[3] "Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others," http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf, Swire, Peter, last accessed 2/6/2020: "ISP access to user data is not comprehensive – technological developments place

use many connected devices serviced by multiple ISPs.

Moreover, research indicates that more than 80 percent of web traffic is encrypted, and that number continues to grow.[4] Google estimates, for example, that 94 percent of traffic across Google is encrypted.[5] When a website is encrypted, an ISP does not know what a user views on that site. Additionally, a growing number of consumers use virtual private networks that block ISPs from even seeing the domain name that a user is visiting. There cannot be comprehensive ISP visibility when ISPs are prevented from seeing user activity.

Uniform federal policies work best. CTIA and its members support efforts to address the growing challenges to consumers' privacy. In particular, CTIA supports federal legislation that establishes uniform, technology-neutral consumer privacy protections. Such legislation is the only way to ensure clearer, more specific, and nationally consistent privacy protections for consumers and certainty for businesses.

HB 1680 as amended would not produce any of the benefits of a uniform federal approach. To the contrary, it would create a highly restrictive technology-specific privacy regime. This legislation would require ISPs (but not other entities) to obtain "express affirmative consent" from consumers to use, disclose, sell or otherwise disseminate consumers' personal information. Such a sweeping and inflexible opt-in requirement is at odds with nearly every other U.S. consumer privacy law and framework. As a result, this bill would change how New Hampshire consumers access information on the internet causing consumer confusion by creating different levels of privacy protections based on the type of entity that handles their personal information,

---

substantial limits on ISPs' visibility. [And] ISP access to user data is not unique – other companies often have access to more information and a wider range of user information than ISPs."

[4] *See* Bond Internet Trends 2019, https://www.bondcap.com/report/itr19/#view/168, last accessed 2/6/2020.

[5] Google Transparency Report: https://transparencyreport.google.com/https/overview?hl=en, last accessed 2/6/2020.

something consumers would not expect.

Maine passed an ISP-only privacy law last year. Last week, CTIA, along with other associations representing broadband providers, filed a lawsuit in the U.S. District Court of Maine. Maine's decision to impose unique burdens on ISPs' speech — while ignoring the online and offline businesses that have and use the very same information and for the same purposes as ISPs — represents discrimination between similarly situated speakers that is impermissible under the First Amendment.

In addition, the Maine law is preempted by federal law because it directly conflicts with federal determinations about the proper way to protect consumer privacy. Among other things, the law conflicts with the FCC's decision that a combination of disclosure, competition, and FTC oversight — not prescriptive ISP-specific rules — best balances the federal policies of promoting broadband and protecting consumer privacy.

In closing, conflicting state rules could hamper the provision of broadband service in New Hampshire, lead to increase compliance costs, and inhibit providing new and innovative products and services – all to the detriment of consumers. Accordingly, CTIA respectfully requests that you not move this legislation as amended. Thank you for your consideration.

Comcast Funds Civil Rights Groups That Rallied Against New FCC Rules

Congress voted to repeal the internet privacy rules last week.

by FABIOLA CINEAS • *4/3/2017, 2:17 p.m.*

Comcast Center | Jeff Fusco

Last week the U.S. House of Representatives followed the Senate and voted to overturn new FCC rules that would have required Internet service providers like **Comcast** to get customers' permission before selling their online browsing data.

Supporters of the repeal have stated that regulators failed to listen to objections from the "Internet community" when the new rules were created under the Obama administration. But a report from *The Intercept* reveals that many of the objections in the Internet community are coming from civil-rights groups with "extensive financial ties" to telecomm companies like Comcast. And their objections to the FCC rules seem absurd and unrelated to their core missions, *The Intercept* points out.

Two such civil rights groups funded by Comcast are the League of United Latin American Citizens (LULAC) and the non-profit OCA – Asian Pacific American Advocates. The two organizations wrote a letter to the FCC, urging then-commissioner Tom Wheeler to reconsider the new rules. One reason provided in the letter is that the rules would deprive consumers of access to "new, innovative, and convenient products, services, and features" that they get through advertising. They also wrote that "Many consumers, especially those households with limited incomes, appreciate receiving relevant advertising that is keyed to their interests and provides them with discounts on the products and services they use."

But the FCC regulations would have actually allowed ISPs to sell their customers' browsing data for such target advertising if users gave them explicit permission. They would also be notified of how their browsing data was being used. The letter states that the FCC's umbrella of "sensitive

data" should be limited only to information about location, children's data, social security numbers, and other information about health and finances. All other information is fair game.

Comcast and Verizon are listed as business advisory council members to the OCA and sponsored the organization's gala in 2016. Comcast along with other ISPs like AT&T, Charter, and Verizon are a part of the League of United Latin American Citizens' "corporate alliance," which provides advice and assistance according to the group. *The New York Times* reported that Comcast gave the organization $260,000 between 2004 and 2012.

The Intercept says neither OCA nor LULAC immediately responded when asked if contributions from ISPs influenced their decision to engage on the privacy rule. Comcast did not respond to request for comment on the FCC regulations from *Philadelphia* magazine.

"It is terrifying that our elected representatives just gave Comcast, Verizon, and other major ISPs a windfall – at massive cost to their own constituents. Here in the poorest big city in the United States, the revocation of these rules means all bets are off," said **Hannah Jane Sassaman** of Philly's Media Mobilizing Project, which has rallied in opposition to the bill. "It means that poor people's identities, dreams, and organizing can be mined for profit for the highest bidding advertiser."

Others have recognized that Comcast and other broadband providers have also ramped up their lobbying efforts against the FCC rules and are in a position to benefit from further deregulation.

Moving forward, President Trump is expected to sign the bill into law.

Follow @fabiolacineas on Twitter.

Read More About:

Comcast Internet Privacy Internet Providers

Fabiola Cineas

Senior Editor

@fabiolacineas

fcineas@phillymag.com

ACLU New Hampshire

Statement by Jeanne Hruska, ACLU-NH Political Director
House Consumer Affairs Committee
House Bill 1680 – Amendment 2020-0560h
February 21, 2020

I submit this testimony on behalf of the American Civil Liberties Union of New Hampshire (ACLU)—a non-partisan, non-profit organization working to protect civil liberties throughout New Hampshire for nearly 50 years. I appreciate the opportunity to testify today in support amendment 2020-0560h, which would modify House Bill 1680 and continue New Hampshire's tradition of prioritizing personal privacy.

This bill is simple – get my permission first.
This amendment is about Granite Staters having the right to tell an internet service provider, or ISP[1], "Before you use my personal information to make money, you have to get my permission." It is not some draconian privacy regime, but a simple premise that ISPs should get your permission before using and profiting from your data.

Unregulated, your ISP will know you better than you know yourself—and they will be able to sell all the detailed sensitive information they collect about you to other companies or the government, which will be able to use it in ways you will never fully understand. Indeed, as artificial intelligence systems become more intelligent and complex, enabling new forms of surveillance, tracking, and data analytics, the stakes for establishing commonsense internet consumer privacy could not be higher.

Information collected by ISPs and sold to the highest bidder can be used to swing elections, alter individual lives, manipulate public discourse, and even populate FBI databases. If state legislatures do not protect internet consumer privacy, people in America will not be able to use the internet without subjecting themselves to increasingly dangerous levels of unregulated corporate and government surveillance.

Opposition to this bill is about one thing: money. ISPs do not want to have to ask for your permission because many people will decline to opt-in and that could cost the ISP money. ISPs can make considerable profits from users' data, whether it is selling the data to third parties or using the data to attract more advertisers with the ability to target certain users. The ways in which ISPs can profit off your data will continue to grow, which is why privacy protections need to be put in place now.

Maine heard the same opposition to its law that the NH legislature is hearing now, and Maine came down on the side of privacy. We are urging you to similarly prioritize the privacy rights of Granite Staters. Your decision to go online should not be tantamount to you giving your ISP permission to use your data as it sees fit without telling you.

ISPs have unique access to your data. This bill focuses specifically on Internet providers doing business in New Hampshire because ISPs are the gatekeepers to the internet. Google and

---

[1] ISPs are also sometimes referred to as broadband internet access services ("BIAS").

Facebook only see what you do on Google and Facebook. Your ISP sees everything you do online because they connect you to the internet. You can choose not to use Google and Facebook – and in the wake of privacy breaches, many people have made that choice. Google and Facebook only see about 25 percent of overall internet traffic. ISPs see 100 percent of internet traffic.

People pay for Google and Facebook with their privacy. People pay for the internet with their money. ISPs oppose legislation like this because they want to be able to sell consumer data *on top* of that. This bill still allows ISPs to sell data *if* they get their customers' consent first.

The FCC believed there should be restrictions on ISPs collection and use of our data. In 2016, the Federal Communications Commission (FCC) implemented long-awaited regulations establishing basic privacy rules pertaining to ISP collection, use, and sale of sensitive customer information. The regulations aimed to protect internet users' private information much in the same way federal regulations have long protected the privacy of landline phone users.

Just as telecommunications regulations bar telephone service providers from gleaning information about us from our phone calls and monetizing that information, the FCC regulations barred ISPs from collecting, using, or monetizing sensitive customer information without opt-in consent from the consumer.

In 2017, Congress used a seldom-used law, the Congressional Review Act, to overturn the FCC regulations. It is worth noting that ISPs lobbied for Congress to take this step and overturn the privacy regulations.

Granite States cannot rely on the FCC or the FTC to protect consumer privacy. Unfortunately for consumers, the Congressional Review Act contains a provision barring regulatory agencies from ever instituting "substantially similar" regulations if the Act is used to eradicate them. It will therefore be difficult—and may require a change to the Congressional Review Act—for the FCC to institute regulations to protect internet users under a future administration. Moreover, since 2017, the FCC has come under new leadership and is now chaired by a former senior employee at Verizon. Not surprising, the FCC's perspective on consumer privacy has shifted.

Nor can the Federal Trade Commission (FTC) act to protect consumer privacy in this area. While the Ninth Circuit has ruled that the FTC retains some jurisdiction of ISPs, the FTC's powers are *remedial* powers. The FTC can only vindicate consumer rights after there has been an unfair and deceptive trade practice. Thus the FTC does not provide adequate protection for two reasons: first, the FTC can only act after the harm has been done, which may provide closure for consumers, but does not undo the harm; second, ISPs can get around the FTC by simply disclosing their practices to consumers, who have no real choice but to take whatever conditions an ISP wants to put on their contract. In addition, the FTC lacks rulemaking authority, and so could not promulgate privacy regulations similar to the now-repealed FCC regulations. Instead, the FTC can only step in to hold ISPs accountable for violating consumer rights *after* those violations have occurred and the damage has been done.

There is no broad federal privacy regime on the horizon, and Granite Staters cannot afford to wait for Godot. There is an argument that piecemeal privacy protections from a variety of different states is confusing and not effective, and instead, we should sit on our hands and wait for the federal government to enact comprehensive and nationwide privacy protections. This is effectively an argument to do nothing. As discussed above, the prospect of comprehensive federal privacy protections has significantly diminished over the past few years. There is no indication that the federal government intends to enact privacy protections, or if it did, that such legislation would be comprehensive and eliminate the need for state-level privacy protections.

The distant future possibility of federal legislation is simply not a valid reason for states to avoid taking action now. New Hampshire has always been a leader on privacy, apart from whatever is happening at the federal level. We are unique in that our case precedent applies a right to privacy to our trash, wherein other states do not. Additionally, more than 81 percent of Granite State voters adopted a constitutional amendment in 2018 that provides an explicit right to privacy for personal and private information. We have always understood that any federal privacy law is the floor, leaving room for states to step in and provide greater protections. Maine did exactly that, and New Hampshire should follow suit.

Amendment 2020-0560h would protect Granite Staters' privacy in several ways. It is a strong step towards regaining what Granite State consumers lost when Congress eliminated the FCC privacy regulations. Among the key elements in the amendment are:

- Definitions of "customer personal information." Any legislation that aims to provide Granite Staters with FCC regulation-equivalent protections must clearly stipulate what information is protected by the law. Crucially, amendment 2020-050h identifies location information, communications content, web browsing information, application usage history, and health and financial information as "personal" and therefore subject to opt-in requirements.

- A ban on the use, disclosure or sale of customer personal information absent the granting of customer opt-in approval, with few exceptions. The exceptions in the amendment are comprehensive, and allow for the provision of internet service, billing, customer-requested service assistance, and emergencies.

- A requirement that the opt-in process and language be "clear and conspicuous." In other words, it is important that ISPs not hide the truth about what they want to do with our information in fine, legalistic print that many people will not read or understand. Amendment 2020-0560h stipulates that information about the opt-in process be written and presented in ways that will provide maximum benefit to the public.

- A ban on "Pay-for-Privacy" and other incentives for customer opt-ins, and a prohibition from providing different qualities of internet service to customers based on their opt-in status. This is essential to prevent companies from undermining the intent of the law. Some companies, including AT&T, have already experimented with Pay-for-Privacy schemes, charging substantially less money to people who allow the company to sell their

sensitive information.[2] It is not fair to grant privacy rights only to those who can afford them. Nor is it acceptable for companies to provide privacy-conscious customers with lesser quality service.

Amendment 2020-0560h is not preempted by federal law. Federal privacy protections are considered a floor, not a ceiling. States have passed a wide variety of privacy legislation on different issues without running into federal preemption.

While only a court could definitively rule on preemption, we do not believe that amendment 2020-0560h would be preempted by federal law. Under the Supremacy Clause, federal laws and regulations may, in some circumstances, preempt state laws and regulations. There are three general types of preemption: (1) express preemption; (2) field preemption; and (3) conflict preemption. Express preemption applies where a federal law or regulation explicitly states that it preempts state law. *See Cipollone v. Liggett Group, Inc.*, 505 U.S. 504, 516 (1992). Field preemption applies where a federal law wholly occupies a given area of law, to the exclusion of all state law. *Id.* Conflict preemption applies where federal law and state impose conflicting obligations such that compliance with both is impossible ("impossibility preemption"), or where state law poses an obstacle to the accomplishment and execution of a federal law's purposes and objectives ("obstacle preemption"). *See Fidelity Federal Sav. & Loan Ass'n v. de la Cuesta*, 458 U.S. 141, 153 (1982). There is a "presumption against preemption," but this presumption does not apply in areas of law that have traditionally been subject to federal regulation. *See Buckman Co. v. Plaintiffs' Legal Comm.*, 531 U.S. 341, 347 (2001).

Nor does express preemption apply here, because the relevant federal statute regulating privacy of telecommunications customer information, Section 222 of the Communications Act, is silent with respect to preemption. *See* 47 U.S.C. § 222. Field preemption also does not apply here, because the FCC has consistently ruled that Section 222 does not preempt all state laws governing customer proprietary network information (CPNI). Rather, the FCC has said that it will determine whether its regulations preempt state laws on a case-by-case basis, depending primarily on whether those laws impose irreconcilably conflict with its regulations, without imposing any presumption that more stringent state privacy protections are preempted by federal law or FCC regulations.[3] Because the bill's provisions are based on the FCC's repealed broadband privacy order, and the federal law in this area has not changed since 2017, amendment 2020-0560h's provisions are fully consistent with existing federal law and FCC regulations.

---

[2] Sandra Fulton, "Pay-for-Privacy Schemes Put the Most Vulnerable Americans at Risk," Free Press, May 10, 2016. Available at https://www.freepress.net/blog/2016/05/10/pay-privacy-schemes-put-most-vulnerable-americans-risk.

[3] *See* Federal Communications Commission, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended; 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers, Third Report and Order and Third Further Notice of Proposed Rulemaking*, 17 FCC Rcd 14860, 14891–93 (2002) (2002 CPNI Order); Federal Communications Commission, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking*, 22 FCC Rcd 6927, 6958 (2007) (2007 CPNI Order).

We do not believe that amendment 2020-0560h runs afoul of the Dormant Commerce Clause doctrine, which prohibits states from imposing inappropriate burdens on interstate commerce. First, this amendment does not violate the extraterritoriality doctrine. Under that doctrine, laws that regulate purely out-of-state transactions are invalid. Here, however, amendment 2020 0560h regulates ISP interactions only with respect to their in-state consumers. It is presumably feasible for ISPs to identify these individuals and implement appropriate safeguards for their protected information.

Amendment 2020-0560h does not violate the *Pike* balancing test. Under that test, state laws that impose indirect burdens on interstate commerce are invalid if those burdens are disproportionate to the law's legitimate local benefits. *See, e.g., Brown-Forman Distillers Corp. v. New York State Liquor Auth.*, 476 U.S. 573, 579 (1986). Like many state laws, this amendment may impose some burdens on interstate commerce by regulating the commercial activities of national and international corporations, but these burdens are justified by the significant privacy benefits afforded to Granite Staters.

Finally, amendment 2020-0560h does not threaten to expose ISPs to conflicting duties. *See, e.g., Bibb v. Navajo Freight Lines*, 359 U.S. 520 (1959) (striking down an Illinois law that required trucks to use contoured mudguards while driving on in-state highways, because the law conflicted with other states' mudguard requirements). We have heard arguments that a patchwork of laws across the country will be unworkable for ISPs. However, it seems plausible that ISPs could tailor their practices for consumers in each state to conform to that state's privacy protections. While an ISP might have economic incentives to apply a national policy that conforms with even the most stringent state privacy protections, that alone does not suffice to make out a Dormant Commerce Clause violation. *See, e.g., Nat'l Federation of the Blind v. Target Corp.*, 452 F. Supp. 2d 946, 961 (N.D. Cal. 2006) ("Courts have held that when a defendant chooses to manufacture one product for a nationwide market, rather than target its products to comply with state laws, defendant's choice does not implicate the commerce clause." (collecting cases)).

This law does not violate the First Amendment. The basis for a First Amendment challenge is the concept that you cannot go after a specific speaker because you do not like the content of their speech and what they are trying to communicate. So, if a law passed that said ISPs are not allowed to advertise on behalf of candidates from a certain party, that would be a First Amendment violation.

This bill places no restrictions based on the viewpoint or content of a speaker. Rather, like many privacy laws, it regulates the commercial relationship between a particular industry (ISPs) and its customers. Courts have made clear that laws imposing neutral regulations on business's interactions with consumers do not inherently offend the Constitution. *See, e.g. Ades v. Omni Hotels Mgmt. Corp.*, 46 F. Supp. 3d 999, 1011–16 (C.D. Cal. 2014) (holding that the California Invasion of Privacy Act does not violate the Dormant Commerce Clause); *Elane Photography, LLC v. Willock*, 309 P.3d 53, 66 (N.M. 2013) (holding that application of New Mexico's anti-discrimination ordinance to a photography business did not violate the First Amendment).

The New Hampshire Legislature must act because the market will not provide adequate privacy protections. Most Granite Staters do not have a choice between multiple providers for access to high speed internet. In many parts of the state, there is only one ISP that can deliver high speed internet, making it impossible for Granite Staters to choose a provider with strong privacy policies. While it is true that consumers can take some limited steps to protect their privacy, it is not realistic to expect every Granite Stater to have the tech savvy and financial means to utilize encryption or virtual private networks (VPS).

Moreover, privacy should not be only for those who can afford it or have the sophistication to stay up to date with and utilize the latest privacy technology. Investing in VPNs and other privacy protections is expensive and requires a certain level of computer savvy. Without privacy protections that apply to all consumers, privacy becomes a privilege for those with the skills and/or the financial means to afford it. .

Encryption is not a panacea for privacy protection. Even if every Granite Stater had the skills and means to utilize encryption, ISPs would still be able to access – and sell – certain types of personal information. Many websites and streaming services do not work if a consumer is using a VPN or ad-blocker in an effort to protect their privacy. Moreover, the actual privacy protection that comes from encryption is limited with regards to ISPs. Encryption can prevent an ISP from being able to track what you type into a search engine, but ISPs can still track what website you go to and how long you stay on any given one.

An internet provider sees everywhere you go online because they connect you to the internet. Even if the website you are visiting is encrypted, your ISP can still see the website name, how frequently you visit that website, and how long you stay there, distinguishing a website you glance at from one you are on for hours. This information is revealing. Your ISP knows if you visited an alcoholics anonymous site, a religious website, a website about HIV/AIDs, or other websites that are indicative of personal health, habits, traits, and other information. This is yet another reason why the NH legislature should take action to provide blanket privacy protections when it comes to ISPs using and selling customers' data.

The lawsuit against Maine's law is frivolous and intended to scare other states, like NH. A lawsuit does not automatically have merit simply because it was filed. It is our position that the Maine lawsuit was not filed because it is likely to win. Instead, its purpose is to tie up the Maine privacy law in court and delay its implementation. And, it is intended to scare legislators in other states from passing similar legislation. In essence, it is a bullying tactic.

In sum, the burden of ensuring that Granite Staters' consumer privacy rights are protected falls to this legislature. ISPs have access to considerable data about its users; all this bill does is require that ISPs get users' permission before financially benefiting from the use of their data. For these reasons, we urge the committee to support amendment 2020-0560h and to vote *ought to pass as amended* on HB1680.

Bill as Introduced

2020 SESSION

20-2535
05/04

HOUSE BILL ***1680-FN***

AN ACT relative to the collection of personal information by businesses.

SPONSORS: Rep. Muscatel, Graf. 12; Rep. Indruk, Hills. 34

COMMITTEE: Commerce and Consumer Affairs

ANALYSIS

This bill grants consumers the right to request that a business disclose the type of personal information it collects, the purpose for which it is collected, and the categories of third parties with which it is shared. The bill authorizes consumers to opt out of the sale of their personal information. The bill also establishes a private right of action and provides for further enforcement by the attorney general.

- -

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

20-2535
05/04

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Twenty

AN ACT relative to the collection of personal information by businesses.

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

1 New Chapter; Collection of Personal Information by Businesses. Amend RSA by inserting after chapter 359-Q the following new chapter:

CHAPTER 359-R

COLLECTION OF PERSONAL INFORMATION BY BUSINESSES

359-R:1 Definitions. In this chapter:

I. "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

II. "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

III. "Business" means:

(a) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of New Hampshire, and that satisfies one or more of the following thresholds:

(1) Has annual gross revenues in excess of $25,000,000, as adjusted pursuant to RSA 359-R:13, I(e).

(2) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(3) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(b) Any entity that controls or is controlled by a business, as defined in subparagraph (a), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, service mark, or trademark.

IV. "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(a) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(b) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(c) Debugging to identify and repair errors that impair existing intended functionality.

(d) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(e) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(f) Undertaking internal research for technological development and demonstration.

(g) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

V. "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

VI. "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

VII. "Consumer" means a natural person who is a New Hampshire resident, however identified, including by any unique identifier.

VIII. "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(a) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(b) Has implemented business processes that specifically prohibit reidentification of the information.

(c) Has implemented business processes to prevent inadvertent release of deidentified information.

(d) Makes no attempt to reidentify the information.

IX. "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the attorney general pursuant to RSA 359-R:13.

X. "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

XI. "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

XII. "Homepage" means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by RSA 359-R:10, I, including, but not limited to, before downloading the application.

XIII. "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

XIV. "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

XV.(a) "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(1) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(2) Any of the following categories of personal information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

(3) Characteristics of protected classifications under New Hampshire or federal law.

(4) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(5) Biometric information.

(6) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(7) Geolocation data.

(8) Audio, electronic, visual, thermal, olfactory, or similar information.

(9) Professional or employment-related information.

(10) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99).

(11) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(b) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.

XVI. "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

XVII. "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

XVIII. "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

XIX. "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(a) Compatible with the business purpose for which the personal information was collected.

(b) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(c) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(d) Subject to business processes that specifically prohibit reidentification of the information.

(e) Made subject to business processes to prevent inadvertent release of deidentified information.

(f) Protected from any reidentification attempts.

(g) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(h) Not be used for any commercial purpose.

(i) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

XX.(a) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

(b) For purposes of this chapter, a business does not sell personal information when:

(1) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this chapter. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(2) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(3) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(A) The business has provided notice that information being used or shared in its terms and conditions consistent with RSA 359-R:9.

(B) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(4) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with RSA 359-R:4 and 359-R:5. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with RSA 359-R:6. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate RSA 358-A.

XXI. "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

XXII. "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this chapter, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

XXIII. "Third party" means a person who is not any of the following:

(a) The business that collects personal information from consumers under this chapter.

(b)(1) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(A) Prohibits the person receiving the personal information from:

(i) Selling the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(B) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(2) A person covered by this paragraph that violates any of the restrictions set forth in this chapter shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this chapter if the person receiving the personal information uses it in violation of the restrictions set forth in this chapter, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

XXIV. "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of

this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

XXV. "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the secretary of state, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to rules adopted by the attorney general pursuant to RSA 359-R:13, I(g) to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to RSA 359-R:4 and RSA 359-R:5 if the business cannot verify, pursuant this paragraph and rules adopted by the attorney general that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

359-R:2 Collection of Personal Information; Disclosure to Consumer Required.

I. A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

II. A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

III. A business shall provide the information specified in paragraph I to a consumer only upon receipt of a verifiable consumer request.

IV. A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily usable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

V. This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

359-R:3 Consumer's Right to Request Deletion of Personal Information.

I. A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

II. A business that collects personal information about consumers shall disclose, pursuant to RSA 359-R:8, the consumer's rights to request the deletion of the consumer's personal information.

III. A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

IV. A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(a) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(b) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(c) Debug to identify and repair errors that impair existing intended functionality.

(d) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.

(e) Comply with the Electronic Communications Privacy Act of 1986 or RSA 570-A.

(f) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(g) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(h) Comply with a legal obligation.

(i) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

359-R:4 Collection of Personal Information; Disclosure to Consumer Required.

I. A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(a) The categories of personal information it has collected about that consumer.

(b) The categories of sources from which the personal information is collected.

(c) The business or commercial purpose for collecting or selling personal information.

(d) The categories of third parties with whom the business shares personal information.

(e) The specific pieces of personal information it has collected about that consumer.

II. A business that collects personal information about a consumer shall disclose to the consumer, pursuant to RSA 359-R:8, I(c), the information specified in paragraph I upon receipt of a verifiable consumer request from the consumer.

III. A business that collects personal information about consumers shall disclose, pursuant to RSA 359-R:8, II(e):

(a) The categories of personal information it has collected about that consumer.

(b) The categories of sources from which the personal information is collected.

(c) The business or commercial purpose for collecting or selling personal information.

(d) The categories of third parties with whom the business shares personal information.

(e) The specific pieces of personal information the business has collected about that consumer.

IV. This section does not require a business to do the following:

(a) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(b) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

359-R:5 Sale of Personal Information; Disclosure to Consumer Required.

I. A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(a) The categories of personal information that the business collected about the consumer.

(b) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.

(c) The categories of personal information that the business disclosed about the consumer for a business purpose.

II. A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to RSA 359-R:8, the information specified in paragraph I to the consumer upon receipt of a verifiable consumer request from the consumer.

III. A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to RSA 359-R:8:

(a) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.

(b) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

IV. A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to RSA 359-R:6.

359-R:6 Consumer Right to Opt-out.

I. A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

II. A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to RSA 359-R:9, I, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

III. Notwithstanding paragraph I, a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

IV. A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to RSA 359-R:9, I(d), from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

359-R:7 Discrimination Against Consumer Who Has Exercised Opt-out Prohibited.

I.(a) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this chapter, including, but not limited to, by:

(1) Denying goods or services to the consumer.

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(3) Providing a different level or quality of goods or services to the consumer.

(4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(b) Nothing in this paragraph prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

II.(a) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.

(b) A business that offers any financial incentives pursuant to this paragraph, shall notify consumers of the financial incentives pursuant to RSA 359-R:9.

(c) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to RSA 359-R:9 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(d) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

359-R:8 Methods of Disclosure.

I. In order to comply with RSA 359-R:2 through RSA 359-R:5 and RSA 359-R:7, a business shall, in a form that is reasonably accessible to consumers:

(a) Make available to consumers 2 or more designated methods for submitting requests for information required to be disclosed pursuant to RSA 359-R:4 and 359-R:5, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet website, a website address.

(b) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily usable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

(c) For purposes of RSA 359-R:4, II:

(1) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(2) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in paragraph III that most closely describes the personal information collected.

(d) For purposes of RSA 359-R:5, II:

(1) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(2) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in paragraph III that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in paragraph III that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of paragraph III.

(3) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12months by reference to the enumerated category or categories in paragraph III that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in paragraph III that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (2).

(e) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any New Hampshire-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

(1) A description of a consumer's rights pursuant to RSA 359-R:4, RSA 359-R:5, and RSA 359-R:7 and one or more designated methods for submitting requests.

(2) For purposes of RSA 359-R:4, III, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in paragraph III that most closely describe the personal information collected.

(3) For purposes of RSA 359-R:5, III(a) and (b), 2 separate lists:

(A) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in paragraph III that

most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(B) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in paragraph III that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(f) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this chapter are informed of all requirements in RSA 359-R:4, RSA 359-R:5, RSA 359-R:7, and this section, and how to direct consumers to exercise their rights under those sections.

(g) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification.

II. A business is not obligated to provide the information required by RSA 359-R:4 and RSA 359-R:5 to the same consumer more than twice in a 12-month period.

III. The categories of personal information required to be disclosed pursuant to RSA 359-R:4 and RSA 359-R:5 shall follow the definition of personal information in RSA 359-R:1, XV.

359-R:9 Form of Notice.

I. A business that is required to comply with RSA 359-R:6 shall, in a form that is reasonably accessible to consumers:

(a) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(b) Include a description of a consumer's rights pursuant to RSA 359-R:6, along with a separate link to the "Do Not Sell My Personal Information" Internet webpage in:

(1) Its online privacy policy or policies if the business has an online privacy policy or policies.

(2) Any New Hampshire-specific description of consumers' privacy rights.

(c) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this chapter are informed of all requirements in RSA 359-R:6 and this section and how to direct consumers to exercise their rights under those sections.

(d) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(e) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(f) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

II. Nothing in this chapter shall be construed to require a business to comply with the chapter by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to New Hampshire consumers and that includes the required links and text, and the business takes reasonable steps to ensure that New Hampshire consumers are directed to the homepage for New Hampshire consumers and not the homepage made available to the public generally.

III. A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to rules adopted by the attorney general under RSA 541-A.

359-R:10 Exceptions.

I. The obligations imposed on businesses by this chapter shall not restrict a business's ability to:

(a) Comply with federal, state, or local laws.

(b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(c) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(d) Exercise or defend legal claims.

(e) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(f) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of New Hampshire. For purposes of this chapter, commercial conduct takes place wholly outside of New Hampshire if the business collected that information while the consumer was outside of New Hampshire, no part of the sale of the consumer's personal information occurred in New Hampshire, and no personal information collected while the consumer was in New Hampshire is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in New Hampshire and

then collecting that personal information when the consumer and stored personal information is outside of New Hampshire.

II. The obligations imposed on businesses by RSA 359-R:4 through 359-R:9 shall not apply where compliance by the business with the chapter would violate an evidentiary privilege under New Hampshire law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under New Hampshire law as part of a privileged communication.

III.(a) This chapter shall not apply to any of the following:

(1) Medical information governed by RSA 332-I or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(2) A provider of health care or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (1).

(3) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(b) For purposes of this paragraph, the definitions of "medical information" and "provider of health care" in RSA 332-I shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

IV. This chapter shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.).

V. This chapter shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the New Hampshire Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This paragraph shall not apply to RSA 359-R:11.

VI. This chapter shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Section 2721 et seq.). This paragraph shall not apply to RSA 359-R:11.

VII. Notwithstanding a business's obligations to respond to and honor consumer rights requests pursuant to this chapter:

(a) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(b) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(c) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

VIII. A business that discloses personal information to a service provider shall not be liable under this chapter if the service provider receiving the personal information uses it in violation of the restrictions set forth in the chapter, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this chapter for the obligations of a business for which it provides services as set forth in this chapter.

IX. This chapter shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

X. The rights afforded to consumers and the obligations imposed on the business in this chapter shall not adversely affect the rights and freedoms of other consumers.

XI. The rights afforded to consumers and the obligations imposed on any business under this chapter shall not apply to the extent that they infringe on the noncommercial activities of a person or entity as described in part I, article 22 of the New Hampshire Constitution.

359-R:11 Private Right of Action.

I.(a) Any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the

nature of the information to protect the personal information may institute a civil action for any of the following:

(1) To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.

(2) Injunctive or declaratory relief.

(3) Any other relief the court deems proper.

(b) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

II. Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this chapter the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this chapter. If a business continues to violate this chapter in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the chapter that postdates the written statement.

III. The cause of action established by this section shall apply only to violations as defined in paragraph I and shall not be based on violations of any other section of this chapter. Nothing in this chapter shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or New Hampshire Constitution.

359-R:12 Opinion of the Attorney General.

I. Any business or third party may seek the opinion of the attorney general for guidance on how to comply with the provisions of this chapter.

II. A business shall be in violation of this chapter if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this chapter shall be subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the state of New

Hampshire by the attorney general. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the state of New Hampshire by the attorney general.

III. Any civil penalty assessed for a violation of this chapter, and the proceeds of any settlement of an action brought pursuant to paragraph II, shall be deposited in the general fund and credited to the department of justice to offset any costs incurred by the department in connection with this chapter.

359-R:13 Rulemaking.

I. On or before July 1, 2021, the attorney general shall adopt rules under RSA 541-A to further the purposes of this chapter, including, but not limited to, the following areas:

(a) Updating as needed additional categories of personal information to those enumerated in this chapter in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(b) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to RSA 359-R:8.

(c) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this chapter and as needed thereafter.

(d) Establishing rules and procedures for the following:

(1) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to RSA 359-R:6.

(2) To govern business compliance with a consumer's opt-out request.

(3) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(e) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this chapter are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this chapter and as needed thereafter.

(f) Establishing rules and procedures to further the purposes of RSA 359-R:4 and 359-R:5 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to RSA 359-R:8, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to

govern a business's determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this chapter and as needed thereafter.

II. The attorney general may adopt additional rules as necessary to further the purposes of this chapter.

III. The attorney general shall not bring an enforcement action under this chapter until 6 months after the publication of the final rules issued pursuant to this section or July 1, 2021, whichever is sooner.

359-R:14 Contractual Waiver Prohibited. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

2 Effective Date. This act shall take effect January 1, 2021.

LBAO
20-2535
12/20/19

HB 1680-FN- FISCAL NOTE
AS INTRODUCED

AN ACT relative to the collection of personal information by businesses.

FISCAL IMPACT: [X] State [ ] County [ ] Local [ ] None

	Estimated Increase / (Decrease)			
STATE:	FY 2020	FY 2021	FY 2022	FY 2023
Appropriation	$0	$0	$0	$0
Revenue	$0	$0	$0	$0
Expenditures	$0	Indeterminable	Indeterminable	Indeterminable
Funding Source:	[X] General	[ ] Education	[ ] Highway	[ ] Other

The Judicial Branch was originally contacted on Novermber 25, 2019 for a fical note worksheet, which they have not provided as of December 20, 2019.

METHODOLOGY:

This bill grants consumers the right to request that a business disclose the type of personal information it collects, the purpose for which it is collected, and the categories of third parties with which it is shared. The bill authorizes consumers to opt out of the sale of their personal information. The bill also establishes a private right of action and provides for further enforcement by the attorney general.

The Department of Justice indicates this bill would create several new responsibilities for the Department:

- The bill would allow a business or third party to seek an opinion from the Department of Justice on how to comply with the provisons of the new law.
- , The Department would be required to adopt rules by July 1, 2021.
- The bill would allow the Department to bring an enforcement action against any business that fails to comply with the bills provisons.
- The Department would be authorized to collect civil penalties and use the amounts collected to offset the costs incurred by the Department in connection with the bill.

The Department assumes the there would be an increase in investigations and enforcement actions brought by the Consumer Protection Bureau. The degree of such increase cannot be estimated. In addition, the Department expects the bill will require additional resources to

comply with the rulemaking and advisory requirements. These are new functions not currently assigned to the Department and would likely require additional staff positions. Because the scope and volume of the additional responsibilities is unknown, the impact on State expenditures and revenue cannot be determined.

AGENCIES CONTACTED:

Department of Justice and Judicial Branch