LEGISLATIVE COMMITTEE MINUTES

HB1282

Bill as Introduced

HB 1282 - AS INTRODUCED

2022 SESSION

22-2790
12/04

HOUSE BILL *1282*

AN ACT relative to the records of communication common carriers.

SPONSORS: Rep. Yokela, Rock. 33

COMMITTEE: Criminal Justice and Public Safety

ANALYSIS

This bill prohibits a communications common carrier from releasing customer information to a government entity unless requested pursuant to a valid search warrant or an exception to the warrant requirement.

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Matter which is either (a) all new or (b) repealed and reenacted appears in regular type.

HB 1282 - AS INTRODUCED

22-2790
12/04

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Twenty Two

AN ACT relative to the records of communication common carriers.

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

1 Certain Records of Communications Common Carriers; Warrant Requirement. RSA 7:6-b is repealed and reenacted to read as follows:

7:6-b Records of Communications Common Carriers.

I. Every communications common carrier, as defined in RSA 570-A:1, IX, shall require a valid search warrant before providing a government entity with any information related to its customers, unless the request falls under the exceptions listed in RSA 644-A:3. Such information includes, but is not limited to:

(a) The names and addresses of persons to whom stated listed or unlisted telephone numbers are assigned.

(b) The names and addresses of persons to whom any stated or identified services are provided.

(c) Any local and long distance billing records for any subscriber to, or customer of telephone service or wireless telephone service as defined in RSA 638:21, XI.

(d) The length of service provided to a subscriber or customer by the communications common carrier.

(e) The types of services provided to the subscriber or customer by the communications common carrier.

(f) The telephone number or other subscriber number or identity.

II. No such communications common carrier nor any agent, servant, or employee thereof, shall be civilly or criminally responsible or liable for furnishing or delivering any records or information in compliance with a valid search warrant, or if the request falls under the exceptions to the warrant requirement listed in RSA 644-A:3.

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

Committee Minutes

SENATE CALENDAR NOTICE
Commerce

Sen Harold French, Chair
Sen Bill Gannon, Vice Chair
Sen Jeb Bradley, Member
Sen Donna Soucy, Member
Sen Kevin Cavanaugh, Member

Date: March 29, 2022

HEARINGS

Tuesday	04/05/2022
(Day)	(Date)

Commerce	State House 100	9:00 a.m.
(Name of Committee)	(Place)	(Time)

9:00 a.m.	**HB 314**	relative to homestead food operation licensure.
9:10 a.m.	**HB 1048**	relative to minimum nonforfeiture amounts under the standard nonforfeiture law for individual deferred annuities.
9:20 a.m.	**HB 1249**	relative to weights and measures.
9:30 a.m.	**HB 1282**	relative to the records of communication common carriers.
9:40 a.m.	**HB 1089**	relative to the unenforceability of noncompete agreements upon termination of an employee for noncompliance with a medical intervention mandate.

EXECUTIVE SESSION MAY FOLLOW

Sponsors:

HB 314

Rep. Nunez	Rep. Burt	Rep. Verville	Rep. Ankarberg
Rep. Binford	Rep. Abramson	Rep. A. Lekas	Rep. Baxter
Rep. Roy			

HB 1048

Rep. Potucek

HB 1249

Rep. Hunt

HB 1282

Rep. Yokela

HB 1089

Rep. Kofalt	Rep. Comtois	Rep. Spillane	Rep. Bernardy
Rep. Hough	Rep. Johnson	Rep. Ulery	Rep. A. Lekas

Aaron Jones 271-4063

Harold F. French
Chairman

Senate Commerce Committee

Aaron Jones 271-4063

HB 1282, relative to the records of communication common carriers.

Hearing Date: April 5, 2022

Time Opened: 9:30 a.m. **Time Closed:** 10:12 a.m.

Members of the Committee Present: Senators French, Gannon, Soucy and Cavanaugh

Members of the Committee Absent : Senator Bradley

Bill Analysis: This bill prohibits a communications common carrier from releasing customer information to a government entity unless requested pursuant to a valid search warrant or an exception to the warrant requirement.

Sponsors:
Rep. Yokela

Who supports the bill: Representative Josh Yokela, Representative Dennis Acton, Representative Tony Lekas, Representative Alicia Lekas, Representative John Potucek, Curtis Howland, Jesse Medeiros

Who opposes the bill: Maura Weston (NECTA & AT&T), Amanda Noonan (Department of Energy), Lieutenant Eric Kinsman, Teresa Rosenberger (CASA & NHTA)

Who is neutral on the bill: Keen Meng Wong (NH Department of Revenue), John Williams (NH Department of Health & Human Services), Geoff Ward (NH Attorney General's Office)

Summary of testimony presented in support:

Representative Josh Yokela

- Anyone that facilities communication between people, such as Facebook or Google, are regulated as communications common carriers.
- Upon demand from the Attorney General's (AG's) Office, carriers must provide data to the Department.
    - This information could include names, addresses, phone numbers, billing records, subscriptions, and the length of subscription services. However, some subpoenas have asked for more than what is listed in existing statute.

- Representative Yokela submitted written testimony to the Committee.
    - A subpoena given to Facebook, for example, asked for "[a]ny other subscriber number/identification or identity information for the subscriber including email address and IP address." This type of information, according to Representative Yokela, is not listed in existing statute as something that could be asked for.
    - In another example, Apple and Facebook admitted that they had given out private information to non-state actors that had forged requests.
- Representative Yokela said Article 2-b of the State Constitution guarantees an individual's right to live free from government intrusion in private or personal information.
- Representative Yokela was concerned that the Fourth Amendment rights of businesses to own their data had been violated; therefore, he believed that a search warrant should be required to access data belonging to both people and companies.
- Representative Yokela said he spoke to a former Chief Justice of the State Supreme Court who agreed that it is possible that the existing law did not allow for a company to refuse a subpoena. Consequently, he believed the law could be challenged because it violated the Fourth Amendment.
- Representative Yokela said this bill would ensure that no one could reach around the Fourth Amendment to get information about people without a subpoena or a search warrant. If there is enough information that a crime has been committed, then a search warrant could be issued.
- Referring to an example subpoena provided to the Committee, **Senator Soucy** said it stated, "[h]aving been so authorized, and having reasonable grounds to believe that the communications common carrier service has been, is being, or may be used for an unlawful purpose...". She wondered how these situations could be balanced with others, such as child pornography or a child facing imminent physical danger, and if law enforcement had an obligation to at least request information to try to protect people.
    - **Representative Yokela** said that was correct. In existing statute, only suspicion that a crime has a been committed is necessary. For a search warrant, however, they need to have probable cause that a crime has been committed. He agreed that that it could be possible that a law enforcement agency could say information is needed; however, he wondered if a company had a right to refuse until a search warrant had been obtained. Currently, he believed companies did not have that right, which he felt was a breach of the Fourth Amendment. Representative Yokela said as soon as a company has been furnished a written demand, they shall furnish the information to the AG's Office. He said this is not an ask question; instead, it is a force question. There are instances where a company has been made aware of violations or crimes on their platform, which they turn over to the authorities. If a company knows a crime has

been committed, then Representative Yokela said harboring that crime is a problem. However, if they have no knowledge of a crime being committed, then some companies may disagree their platform was used to commit it.

- **Senator Cavanaugh** asked what former Chief Justice of the State Supreme Court reviewed this bill.
    - **Representative Yokela** said it was Representative Bob Lynn.
- **Senator French** asked if this would prevent a carrier from reporting, without inquiry from the AG's Office, anything they thought might be unlawful.
    - **Representative Yokela** did not believe that is how this bill should be read. In RSA 644-A:3, there are exceptions to a search warrant, such as in emergency situations; if a device has been taken by a third-party; if an owner of a device or parent has consented; if there is an emergency that could result in immediate danger, death, or physical injury; or any other legally recognized exceptions.
- Lines 4 through 7 state that "[e]very communications common carrier, as defined in RSA 570-A:1, IX, shall require a valid search warrant before providing a government entity with any information related to its customers..." **Senator French** asked if Facebook would have to wait for a search warrant in order to bring to the attention of the government something they found, such as child abuse.
    - **Representative Yokela** said they are talking about records related to subscriber information, names, addresses, and phone numbers. This bill is unrelated to what is posted on a platform. Presently, a search warrant is needed for posts unless a crime has been committed. If a crime has been committed, Representative Yokela said there are no Fourth Amendment protections. He concluded that carriers are within their rights and they are obligated to share information with authorities.

Summary of testimony presented in opposition:

Amanda Noonan, Director of the Consumer Services Division, Department of Energy

- The Department is concerned about potential unintended consequences caused by this bill.
- In addition, they are concerned about its impact on the work done by the Department, the Public Utilities Commission (PUC), and other federal regulatory agencies with jurisdiction over telecommunication service providers.
- The Department requested the Committee add language that would allow telecommunication providers to provide customer information, without first having to obtain a search warrant, to the Department, the PUC, or any federal agency with regulatory jurisdiction.

- Without this language, Director Noonan said the ability of the Department and other agencies to work with and assist customers of telecommunication providers, or to investigate any other matters, would be significantly impacted to the detriment of consumers.
- Customer-related information obtained by the Department is confidential and it is not subject to Right-To-Know requests.
- The Department would remain neutral on the remainder of the bill if the following language were added to Section 1: "... or unless the information is requested by the New Hampshire Public Utilities Commission, the New Hampshire Department of Energy, or a federal regulatory agency with jurisdiction over the communications common carrier."

Eric Kinsman, Lieutenant, Portsmouth Police Department, & Commander for the NH Internet Crimes Against Children Task Force

- Lieutenant Kinsman said the possibility of a search warrant for information they can currently obtain legally through the administrative process would have dire consequences and an impact on child victims.
- Nationally, Internet Crimes Against Children (ICAC) Task Forces receive a majority of their cyber tips from the National Center for Missing and Exploited Children (NCMEC). Cyber tips are sent to Task Forces based on the geolocation of the IP address of the suspect.
- Cyber tips are generated from internet service providers (ISPs), such as Facebook or Instagram. These providers are federally mandated to report child sexual abuse material on their platforms.
- In 2019, 16 million individual cyber tips were reported by NCMEC. Those numbers rose to 21 million in 2020 and 29 million in 2021. Lieutenant Kinsman clarified that each report had at least one child victim.
    - In the past 3 years, cybers tips in NH have increased. In 2018, they fielded 35 to 50 cyber tips a month. In 2019, they fielded 90 to 100 per month. By 2022, they were fielding 150 per month.
- As a result of limited resources and the large number of tips, most are not received until 2 months past an incident.
- The NH ICAC Task Force provides assets and training to local law enforcement to help investigate cases of exploitation.
- Lieutenant Kinsman said a search warrant is obtained when they would like to acquire content information from a person's account. He said to require an additional search warrant to gain subscriber information would be detrimental to their ability to investigate in a timely manner. Currently, they are able to obtain subscriber information through an administrative process.
- When an IP address is received from NCMEC, they do not have the information to match the IP address to a specific person. Often times, an IP address may be associated with a person who is simply paying the bill and the suspect is a different resident within the home.

- **Senator French** asked if cyber tips would stop coming in if this bill were passed.
    - **Lieutenant Kinsman** replied that ISPs are federally mandated to report any child abuse sexual material they come across. Since NCMEC is not a law enforcement entity, they are limited to the information provided by ISPs. While they may have an IP address or e-mail, they cannot undertake investigative processes to identify suspects like law enforcement can. Typically, a PDF report is generated with the material that is believed to contain the abuse along with who sent it and who received it. These reports range from 7 pages to 40 or more pages.

Neutral Information Presented:

Keen Meng Wong, NH Department of Revenue

- The Department did not have a position on the bill; however, they believed it would cause problems for communication services tax (CST) audits.
- The communication services tax is imposed on communication services and it is calculated based on the users of the services. The tax is collected by retailers and it is remitted to the Department.
- During audits, records are requested from carriers, which include phone numbers, names, and addresses of their customers. Mr. Meng Wong said this information is collected only for test checks of specific months.
- Except for limited circumstances, existing statutes prohibit the disclosure of taxpayer information outside of the Department.
- For fiscal year 2021, CST revenue was $41 million to the state. In addition, tax notice revenue was $600,000.
- Mr. Meng Wong said this bill would expand RSA 7:6-b to be applicable to all government agencies. Consequently, the Department was unsure how an extra standard of probable cause would affect CST audits. Without information from carriers, the Department has no way to conduct an audit.

John Williams, Director of Legislative Affairs, Department of Health & Human Services

- The Department did not have a position on the bill.
- Director Williams said NH and its agencies respect privacy rights, but they need to be balanced with protecting children.
- This bill would be applicable to all state agencies, which could lead to unintended consequences.
- Despite the amendment offered by the Department of Energy, Director Williams felt it did not work for every agency, particularly those concerned with protecting children.

- This bill does not include Paragraph 3 of RSA 7:6-b, which delegated authority to county attorney's offices to proceed with investigations as well as receive information.
- Director Williams said this bill would take away the authority to use subpoenas to obtain baseline information so that investigations can be conducted.

Geoff Ward, Senior Assistant Attorney General & Chief of the Criminal Justice Bureau, NH Attorney General's Office

- Attorney Ward emphasized that RSA 7:6-b requires reasonable suspicion that criminal activity has taken place and only limited information can be received under those circumstances.
- Typically, cyber tips received by NCMEC come with an image that may be child pornography and the IP address it is associated with. While this may not be suitable for a search warrant, it could be used for a subpoena to gain additional limited information about who may be subscribing to the service and where to find that person.
- While federal law impacts federal cyber tips, Attorney Ward felt this bill would cause issues because the language in Paragraph 1 was broad.
    - Cyber tips would fall under any information a communications common carrier has because they could contain information related to a customer of an ISP and an image from an ISP.
    - The language would severely limit the ability of communications carriers to provide information to law enforcement.
    - Often times, grand juries issue subpoenas for information from communications common carriers. The broad language, however, would prohibit companies from complying with subpoenas.
- Attorney Ward clarified that an individual does not lose their Fourth Amendment rights when they have committed a crime.
- The exceptions found in RSA 644-A:3 are only applicable to emergency circumstances and location data. In other words, pings from a cellphone could be used to find someone who is missing or lost. Attorney Ward felt these exceptions were not as broad as presented by Representative Yokela and they did not address issues that had been raised.
- Attorney Ward concluded that this bill posed significant unintended consequences that would hamper law enforcement and impact key initial investigative stages, especially in child sexual abuse crimes.
- **Senator French** asked if there were any ongoing abuses that required this bill.
    - **Attorney Ward** responded no because requests are done in very limited fashion. In addition to the AG's Office, county attorney's offices are trained and authorized to do them. In his 10 years, he said he had only done them a handful of times because they are limited to (a) through (f) in the statute. Typically, the focus has been on drug crimes; however, it can be related to internet crimes against children and sexual abuse crimes.

- **Senator French** asked how many times Attorney Ward has done one of these.
    - **Attorney Ward** replied that the AG's Office can authorize them, but they have to receive a written request from law enforcement for this type of subpoena. They go through a checklist with law enforcement regarding the type of information they are asking for. They have to be provided with reasonable grounds or suspicion in a written form, which is normally in the form of a preliminary police report, as the basis for requesting a subpoena. Subpoena requests are spread around to at least 15 to 20 people who are authorized to provide them. In his 10 years in the AG's Office, Attorney Ward reiterated that he has only done a handful of them.

AJ
Date Hearing Report completed: April 8, 2022

Speakers

Senate Commerce Committee
SIGN-IN SHEET

Date: 04/5/2022 **Time:** 9:30 a.m.

HB 1282 An ACT relative to the records of communication common carriers.

Name/Representing ***(please print neatly)***

Name/Representing	Support	Oppose	Speaking? Yes	Speaking? No
Dennis Acton / Rock 10	☑	☐	☐	☑
Josh Yokela / Rock 33	☑	☐	☑	☐
Tony Lekas / Hills 37	☒	☐	☐	☐
Alicia Lekas / Hills 37	☒	☐	☐	☐
Rep John Potucek Rock 6	☒	☐	☐	☒
Keen Meng Wong / NHDRA	☐	☐	☑	☐
Maura Weston, NECTA	☐	☑	☐	☑
Maura Weston, AT&T	☐	☑	☐	☑
Amanda Noonan Department of Energy	☐	☑	☑	☐
Eric Kinsman	☐	☒	☒	☐
John Williams DHHS	☐	☐	☑	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐

Senate Commerce Committee
SIGN-IN SHEET

Date: 04/5/2022 **Time:** 9:30 a.m.

HB 1282 An ACT relative to the records of communication common carriers.

Name/Representing ***(please print neatly)***

Name/Representing	Support	Oppose	Speaking?	Yes	No
Teresa Rosenberger – NHTA	☐	☒	Speaking?	☐	☒
Geoff Ward NH Atty General's	☐	☐	Speaking?	☑	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐
	☐	☐	Speaking?	☐	☐

Senate Remote Testify

Commerce Committee Testify List for Bill HB1282 on 2022-04-05

Support: 2 Oppose: 1

Name	Title	Representing	Position
Howland, Curtis	A Member of the Public	Myself	Support
Medeiros, Jesse	A Member of the Public	Myself	Support
Rosenberger, Teresa	A Lobbyist	CASA	Oppose

Testimony

I. Every communications common carrier, as defined in RSA 570-A:1, IX, shall require a valid search warrant before providing a government entity with any information related to its customers, unless the request falls under the exceptions listed in RSA 644-A:3, ***or unless the information is requested by the New Hampshire Public Utilities Commission, the New Hampshire Department of Energy, or a federal regulatory agency with jurisdiction over the communications common carrier.*** Such information includes, but is not limited to:

ATTORNEY GENERAL
DEPARTMENT OF JUSTICE
33 CAPITOL STREET
CONCORD, NEW HAMPSHIRE 03301-6397

GORDON J. MACDONALD
ATTORNEY GENERAL

ANN M. RICE
DEPUTY ATTORNEY GENERAL

May 14, 2018

VIA INTERNET PORTAL (https://www.facebook.com/records)

Facebook, Inc.
Attention: Facebook Security LE Response Team
1601 Willow Road
Menio Park, CA 94124

RE: [redacted]

ADMINISTRATIVE SUBPOENA

To Whom It May Concern:

Pursuant to New Hampshire Revised Statutes Annotated (RSA) 7:6-b, III, the New Hampshire Attorney General has authorized me to issue written demands to communications common carriers for certain information pertaining to services furnished to a person or a location, as provided in N.H. RSA 7:6-b, I & II. Having been so authorized, and having reasonable grounds to believe that the communications common carrier service has been, is being, or may be used for an unlawful purpose, I make this written demand as follows:

Please provide the following information for the following **URL:**

- [redacted] which was used for as unlawful purpose between [redacted] and [redacted]

1. The names and addresses of persons to whom any stated or identified services are provided;

2. The length and types of service provided to the subscriber or customer; and

3. Any other subscriber number/identification or identity information for the subscriber including email address and IP address.

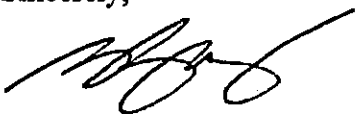
RTK-000005

You are not to disclose the existence of this request, as any such disclosure could impede the investigation being conducted and thereby interfere with the enforcement of the law.

Pursuant to N.H. RSA 7:6-b, III, this demand shall constitute an administrative subpoena for purposes of determining compliance with federal law.

All records should be sent to:
Chief Paul Roberts
Plainfield Police Department
P.O. Box 380, 110 Main Street
Plainfield, NH 03770
Phone: (603) 469-3344
Fax: (603) 469-3343
Email: chief@plainfieldnh.org

Sincerely,



Geoffrey W.R. Ward
Senior Assistant Attorney General
Criminal Justice Bureau
Phone: (603) 271-3671
Fax: (603) 271-2110
geoffrey.ward@doj.nh.gov

ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

33 CAPITOL STREET
CONCORD, NEW HAMPSHIRE 03301-6397

GORDON J. MACDONALD
ATTORNEY GENERAL

JANE E. YOUNG
DEPUTY ATTORNEY GENERAL

March 4, 2019

Best Buy
Subpoena Compliance
Fax: (612) 291-9200

By Fax Submission

Administrative Subpoena

To Whom It May Concern:

Pursuant to his authority under New Hampshire Revised Status Annotated (RSA) 7:6-b, III, New Hampshire Attorney General Gordon J. MacDonald has authorized me to issue written demands to communications common carriers for certain information pertaining to services furnished to a person or a location, as provided in RSA 7:6-b, I & II. Having been so authorized, and having reasonable grounds to believe that the communications common carrier services has been, is being, or may be used for an unlawful purpose, I make this written demand as follows:

Please provide the following information for a Verizon account (opened and serviced through Best Buy), with telephone number [redacted]

- The names and addresses of persons to whom stated listed or unlisted telephone numbers are assigned;
- Any local and long distance billing records for any subscriber to, or customer of telephone service; and
- Any and all subscriber and/or identifying information, including any Internet Protocol (IP) address history since [redacted];

Please also provide the following information for a Verizon account (opened and serviced through Best Buy), with the name [redacted]

- The types of services provided to the subscriber or customer; and
- The telephone number or *any* other subscriber information, to include any subscriber numbers or information. This includes any e-mail address, and IP address information.

Please also provide the following information for a Verizon account (opened and serviced through Best Buy), with an account associated with e-mail address

Telephone 603-271-3658 • FAX 603-271-2110 • TDD Access: Relay NH 1-800-735-2964

[redacted] and physical address [redacted] Bridgeport, CT 06604:

- IP address information obtained;
- Subscriber and billing information; and
- Account login session information, such as IP address information.

You are **not** to disclose the existence of this request, as any such disclosure could impede the investigation being conducted and thereby interfere with the enforcement of the law. Pursuant to RSA 7:6-b, III, this demand shall constitute an administrative subpoena for purpose of determining compliance with federal law.

All Records should be sent by regular mail or e-mail to:

Master Patrolman James Kear
Epsom Police Department
980 Suncook Valley Highway
Epsom, NH 03234
Jkearepsompd@metrocast.net

Sincerely,

Bryan J. Townsend, II
Assistant Attorney General
Medicaid Fraud Control Unit
(603) 271-7094
Fax: (603) 271-2110
Bryan.Townsend@doj.nh.gov

BJT/

ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

33 CAPITOL STREET
CONCORD, NEW HAMPSHIRE 03301-6397

GORDON J. MACDONALD
ATTORNEY GENERAL

JANE E. YOUNG
DEPUTY ATTORNEY GENERAL

March 23, 2020

VIA INTERNET PORTAL (https://www.facebook.com/records)

Facebook, Inc.
Attn: Facebook Security LE Response Team
1601 Willow Road
Menlo Park, CA 94025

RE: Facebook accounts and information for [redacted] & [redacted]

TO: Whom it May Concern:

Pursuant to New Hampshire Revised Statutes Annotated (RSA) 7:6-b, III, the New Hampshire Attorney General has authorized me to issue written demands to communications common carriers for certain information pertaining to services furnished to a person or location, as provided in N.H. RSA 7:6-b, I & II. Having been so authorized, and having reasonable grounds to believe that the communications common carrier service has been, is being, or may be used for an unlawful purpose, I make this written demand as follows:

Please provide the following information: the user ID numbers, email addresses, profile names and URL's associated with the phone number [redacted] **including any deactivated accounts,** and for any accounts provided to:

[redacted]
Fall River, MA 02720
[redacted]
Profile name [redacted]

Which have been used for an unlawful purpose. Please also provide the following for those accounts:

1. The names and addresses of persons to whom any stated or identified services are provided;

RTK-000041

2. The length and types of service provided to the subscriber or customer; and

3. Any other subscriber number/identification or identity information for the subscriber including email address and IP addresses.

You are not to disclose the existence of this request, as any such disclosure could impede the investigation being conducted and thereby interfere with the enforcement of the law.

Pursuant to N.H. RSA 7:6-b, III, this demand shall constitute an administrative subpoena for purposes of determining compliance with federal law.

All records should be sent to:

Detective Elizabeth Turner
Rochester Police Department
23 Wakefield Street
Rochester, NH 03867
Elizabeth.turner@rochesternh.net
603-330-7103
Fax: 603-330-7159
Police case # [redacted]

Sincerely,

Susan G. Morrell by
Elizabeth C Wardwell, AAG

Susan G. Morrell
Senior Assistant Attorney General
Susan.morrell@doj.nh.gov

Copy to: Lawyers Incorporating Service
10 Ferry Street, suite 313
Concord, NH 03301

Technology

Cybersecurity

Apple and Meta Gave User Data to Hackers Who Used Forged Legal Requests

- Hackers compromised the emails of law enforcement agencies
- Data was used to enable harassment, may aid financial fraud

Apple, Meta Gave Customer Information to Hackers

By William Turton

March 30, 2022, 1:59 PM EDT *Updated on March 30, 2022, 3:30 PM EDT*

Apple Inc. and Meta Platforms Inc., the parent company of Facebook, provided customer data to hackers who masqueraded as law enforcement officials, according to three people with knowledge of the matter.

Apple and Meta provided basic subscriber details, such as a customer's address, phone number and IP address, in mid-2021 in response to the forged "emergency data requests." Normally, such requests are only provided with a search warrant or subpoena signed by a judge, according to the people. However, the emergency requests don't require a court order.

Snap Inc. received a forged legal request from the same hackers, but it isn't known whether the company provided data in response. It's also not clear how many times the companies provided data prompted by forged legal requests.

Cybersecurity researchers suspect that some of the hackers sending the forged requests are minors located in the U.K. and the U.S. One of the minors is also believed to be the mastermind behind the cybercrime group Lapsus$, which hacked Microsoft Corp., Samsung Electronics Co. and Nvidia Corp., among others, the people said. City of London Police recently arrested seven people in connection with an investigation into the Lapsus$ hacking group; the probe is ongoing.

An Apple representative referred Bloomberg News to a section of its law enforcement guidelines.

The guidelines referenced by Apple say that a supervisor for the government or law enforcement agent who submitted the request "may be contacted and asked to confirm to Apple that the emergency request was legitimate," the Apple guideline states.

"We review every data request for legal sufficiency and use advanced systems and processes to validate law enforcement requests and detect abuse," Meta spokesman Andy Stone said in a statement. "We block known compromised accounts from making requests and work with law enforcement to respond to incidents involving suspected fraudulent requests, as we have done in this case."

Snap had no immediate comment on the case, but a spokesperson said the company has safeguards in place to detect fraudulent requests from law enforcement.

Law enforcement around the world routinely asks social media platforms for information about users as part of criminal investigations. In the U.S., such requests usually include a signed order from a judge. The emergency requests are intended to be used in cases of imminent danger and don't require a judge to sign off on it.

Hackers affiliated with a cybercrime group known as "Recursion Team" are believed to be behind some of the forged legal requests, which were sent to companies throughout 2021, according to the three people who are involved in the investigation.

Recursion Team is no longer active, but many of its members continue to carry out hacks under different names, including as part of Lapsus$, the people said.

The information obtained by the hackers using the forged legal requests has been used to enable harassment campaigns, according to one of the people familiar with the inquiry. The three people said it may be primarily used to facilitate financial fraud schemes. By knowing the victim's information, the hackers could use it to assist in attempting to bypass account security.

Bloomberg is omitting some specific details of the events in order to protect the identities of those targeted.

The fraudulent legal requests are part of a months-long campaign that targeted many technology companies and began as early as January 2021, according to two of the people. The forged legal requests are believed to be sent via hacked email domains belonging to law enforcement agencies in multiple countries, according to the three people and an additional person investigating the matter.

The forged requests were made to appear legitimate. In some instances, the documents included the forged signatures of real or fictional law enforcement officers, according to two of the people. By compromising law enforcement email systems, the hackers may have found legitimate legal requests and used them as a template to create forgeries, according to one of the people.

"In every instance where these companies messed up, at the core of it there was a person trying to do the right thing," said Allison Nixon, chief research officer at the cyber firm Unit 221B. "I can't tell you how many times trust and safety teams have quietly saved lives because employees had the legal flexibility to rapidly respond to a tragic situation unfolding for a user."

On Tuesday, Krebs on Security reported that hackers had forged an emergency data request to obtain information from the social media platform Discord. In a statement to Bloomberg, Discord confirmed that it had also fulfilled a forged legal request.

"We verify these requests by checking that they come from a genuine source, and did so in this instance," Discord said in a statement. "While our verification process confirmed that the law enforcement account itself was legitimate, we later learned that it had been compromised by a malicious actor. We have since conducted an investigation into this illegal activity and notified law enforcement about the compromised email account."

Apple and Meta both publish data on their compliance with emergency data requests. From July to December 2020, Apple received 1,162 emergency requests from 29 countries. According to its report,

Apple provided data in response to 93% of those requests.

Meta said it received 21,700 emergency requests from January to June 2021 globally and provided some data in response to 77% of the requests.

"In emergencies, law enforcement may submit requests without legal process," Meta states on its website. "Based on the circumstances, we may voluntarily disclose information to law enforcement where we have a good faith reason to believe that the matter involves imminent risk of serious physical injury or death."

The systems for requesting data from companies is a patchwork of different email addresses and company portals. Fulfilling the legal requests can be complicated because there are tens of thousands of different law enforcement agencies, from small police departments to federal agencies, around the world. Different jurisdictions have varying laws concerning the request and release of user data.

"There's no one system or centralized system for submitting these things," said Jared Der-Yeghiayan, a director at cybersecurity firm Recorded Future Inc. and former cyber program lead at the Department of Homeland Security. "Every single agency handles them differently."

Companies such as Meta and Snap operate their own portals for law enforcement to send legal requests, but still accept requests by email and monitor requests 24 hours a day, Der-Yeghiayan said.

Apple accepts legal requests for user data at an apple.com email address, "provided it is transmitted from the official email address of the requesting agency," according to Apple's legal guidelines.

Compromising the email domains of law enforcement around the world is in some cases relatively simple, as the login information for these accounts is available for sale on online criminal marketplaces.

"Dark web underground shops contain compromised email accounts of law enforcement agencies, which could be sold with the attached cookies and metadata for anywhere from $10 to $50," said Gene Yoo, chief executive officer of the cybersecurity firm Resecurity, Inc.

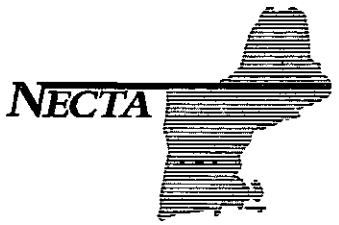
Yoo said multiple law enforcement agencies were targeted last year as a result of previously unknown vulnerabilities in Microsoft Exchange email servers, "leading to further intrusions."

A potential solution to the use of forged legal requests sent from hacked law enforcement email systems will be difficult to find, said Nixon, of Unit 221B.

"The situation is very complex," she said. "Fixing it is not as simple as closing off the flow of data. There are many factors we have to consider beyond solely maximizing privacy."

– With assistance by Sarah Frier

(Updated to include mention of recent arrests in the U.K.)



New England Cable & Telecommunications Association, Inc.

New England Cable & Telecommunications Association, Inc.
53 State Street ● 5th Floor ● Boston, MA 02109
Tel: 781.843.3418

New England Cable & Telecommunications Association, Inc.

Testimony in Opposition to HB 1282, relative to the records of communication common carriers.

Senate Commerce Committee

April 5, 2022

Chairman French, Vice Chairman Gannon and members of the Senate Commerce Committee,

On behalf of the New England Cable and Telecommunications Association (NECTA), I appreciate the opportunity to submit testimony in opposition to **HB 1282, *relative to the records of communications common carriers.*** NECTA's members, including Breezeline (formerly known as Atlantic Broadband), Charter Communications and Comcast, are New Hampshire's leading broadband and communications providers. Together they serve approximately 485,000 customers and offer their services to more than 650,000 locations in more than 184 communities across the state.

We are concerned that the repeal of RSA 7:6-b and reenactment by passage of HB 1282 would create inconsistencies with federal law which would impede the lawful and proactive sharing of information. The lawful sharing of information in certain circumstances offers important public safety benefits and allows providers to protect property rights and employee safety. These are important rights and obligations which the passage of HB 1282 would impede or constrain.

New Hampshire House Bill 1282 (HB 1282) would require communications common carriers[1] to respond to any law enforcement requests for certain types of personal information on its customers or subscribers **only with a warrant**. Specifically, HB 1282 would amend RSA 7:6-b(I)(a)-(f) and require a warrant for the disclosure to a government entity of

- Names and addresses associated with listed or unlisted numbers,
- Length and types of services provided to subscribers,
- Local and long-distance records (call detail) for subscribers, and
- Any telephone number or other subscriber number/identity.

HB 1282 would provide differing protection for this type of information than federal law provides. Federal law requires a warrant only for governmental access to contents of communications (regardless of

[1] Defined in New Hampshire RSA 570-A:1 to include "person[s] engaged in providing communications services to the general public through transmission of any form of information between subscribers by means of wire, cable, radio or electromagnetic transmission, optical or fiber-optic transmission...," thus including internet and voice service providers.

time in storage)[2] and cell site location information held by electronic communications service (ECS) and remote computing service (RCS) providers (which would include the communications common carriers as defined under NH law).[3] When governmental entities are seeking call detail, IP address assignment logs, or basic subscriber or customer information like that listed in HB 1282 (not including content or location information), the federal Stored Communications Act (SCA), 18 U.S.C. §§ 2701(c)(2)(A)-(F) *requires* ECS and RCS providers to disclose this exact same subscriber information as listed in HB 1282 to governmental entities in response to a federal or state administrative, grand jury, or trial *subpoena*. Moreover, the SCA provides absolute immunity from any cause of action in any court for complying with the terms of a governmental subpoena that seeks basic subscriber information like that listed in HB 1282. 18 U.S.C. § 2703(e).

The SCA also allows ECS and RCS providers to voluntarily provide information to governmental entities to protect their rights or property, in an emergency involving danger of death or serious physical injury to any person, and to the National Center for Missing and Exploited Children (NCMEC) in connection exploitation of minors in connection with suspected sex trafficking or pornography. 18 USC § 2702(c). And federal law, 18 U.S.C. § 2258A, *requires* ECS and RCS providers to disclose subscriber records and information to NCMEC, including communications content normally requiring a warrant, in connection with such child abuse activities, and NCMEC is empowered to forward relevant child abuse or exploitation information to the appropriate state or federal law enforcement agencies. New Hampshire law does not expressly allow providers to disclose such information voluntarily, but it requires providers to respond to state government *subpoenas* for information related to an investigation of a violation of state law prohibiting child pornography or exploitation. NH RSA 649-B:5. This would conflict with the provisions in HB 1282 requiring a warrant before disclosing this information to governmental authorities.

For the reasons above, we respectfully oppose 1282 and offer to work with the Committee should the Committee decide to pursue amendment.

Sincerely,

Timothy O. Wilkerson
President

---

[2] In *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), the court held that government must use a warrant to obtain the contents of emails and "in the wake of Warshak, it has apparently been the policy of the Department of Justice since 2013 always to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process." *In Matter of Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 222 n.1 (2d Cir. 2016), *citing* H.R. Rep. No. 114-528, at 9 (2016) (Lynch, concurring), *vacated and remanded on other grounds, United States v. Microsoft*, 138 S.Ct. 1186 (2018).

[3] Government access to cell site location information (CSLI) (*i.e.*, data showing time and location of a mobile device vis-à-vis cell towers) was litigated in *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018). The U.S. Supreme Court held that governmental entities must use a warrant to obtain mobile phone location data under the SCA.

Aaron Jones

From: George Harris <georgeifc@aol.com>
Sent: Wednesday, March 30, 2022 2:35 PM
To: ~Senate Commerce Committee
Subject: HB 1282

Committee Members,

I ask that you consider and pass HB 1282 as it currently reads to protect the privacy of the citizens of the State of New Hampshire.

Live Free or Die!

George Harris
President & CEO
International Firearms Consultants, LLC.
P.O. Box 720
Kingston, N.H. 03848

(O) 603-642-7291
(C) 603-498-1730

Aaron Jones

From: Amy Peikoff <apeikoff@PARLER.COM>
Sent: Tuesday, April 5, 2022 7:41 AM
To: Harold French; William Gannon; Kevin Cavanaugh; Donna Soucy; Aaron Jones; josh.yokela@leg.state.nh
Subject: House Bill 1282

To the Honorable Members of the New Hampshire Senate Commerce Committee:

I am writing to express support for House Bill 1282, under your consideration today, sponsored by Representative Josh Yokela. In my capacity as Chief Policy Officer for Parler, I am familiar with our social media platform's policies and processes for responding to government requests for user and subscriber information.

While I am not aware of Parler having yet received a written demand for subscriber information pursuant to Section 7:6-b, "Certain Records of Communications Common Carriers," it is my understanding that there is precedent for a social media platform to be considered a "common carrier" pursuant to that section. As a consequence, New Hampshire law as it currently stands would require social media platforms like Parler to provide government with private user data, without benefit of a warrant based on probable cause and particularized suspicion.

In federal law, such a practice is still largely upheld due to the so-called "third-party doctrine." (But see, *Carpenter v. United States*, 2018, which carved out a significant exception.) it is my belief that the application of this doctrine to information shared by customers to service providers, in the ordinary course of a lawful business, was a mistake. (See " Of Third-Party Bathwater: How to Throw Out the Third-Party Doctrine While Preserving Government's Ability to Use Secret Agents," St. John's Law Review, 2014.) It is perhaps an implicit understanding of this error which has led various courts and legislators to carve out exceptions to the application of the doctrine, or even to reject its application entirely.

Parler, while best known as a free speech platform, also differentiates itself as a platform which respects user privacy. Consequently, Parler welcomes judicial rulings, legislation, and constitutional provisions which recognize the right of individuals to protect their private information by means of lawful contracts with service providers. Presenting a warrant, based on probable cause and particularized suspicion, is, in my view, the proper way for any government agent or entity to obtain information which is kept private pursuant to a lawful contract.

I thank Representative Yokela for his continuing efforts to protect New Hampshire citizens' rights to protect their privacy via their legal rights to property and contract, and urge this Committe to support HB 1282.

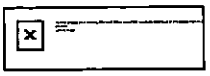
Sincerely,

Amy Peikoff

Amy Peikoff

Chief Policy Officer

@Amy
parler.com



Voting Sheets

Senate Commerce Committee
EXECUTIVE SESSION RECORD
2021-2022 Session

Bill # HB 1282

Hearing date: 4/5/22

Executive Session date: 4/26/22

Motion of: TS **Vote:** 5-0

Committee Member	Made by	Second	Yes	No
Sen. French, Chair			✓	
Sen. Gannon, V-Chair	✓		✓	
Sen. Bradley		✓	✓	
Sen. Cavanaugh			✓	
Sen. Soucy			✓	

Motion of: Consent **Vote:** 5-0

Committee Member	Made by	Second	Yes	No
Sen. French, Chair			✓	
Sen. Gannon, V-Chair			✓	
Sen. Bradley		✓	✓	
Sen. Cavanaugh			✓	
Sen. Soucy	✓		✓	

Motion of: _____ **Vote:** _____

Committee Member	Made by	Second	Yes	No
Sen. French, Chair				
Sen. Gannon, V-Chair				
Sen. Bradley				
Sen. Cavanaugh				
Sen. Soucy				

Reported out by: Sen. French

Notes: _____

Committee Report

STATE OF NEW HAMPSHIRE

SENATE

REPORT OF THE COMMITTEE
FOR THE CONSENT CALENDAR

Tuesday, April 26, 2022

THE COMMITTEE ON Commerce

to which was referred **HB 1282**

AN ACT relative to the records of communication common carriers.

Having considered the same, the committee recommends that the Bill

BE REFERRED TO INTERIM STUDY

BY A VOTE OF: 5-0

Senator Harold French
For the Committee

This bill would have prohibited communications common carriers from releasing customer information to government entities unless it was requested through a valid search warrant or exempted under an exception to a warrant. The Committee heard that this bill could have potentially unintended consequences on the operation of all state government agencies. For example, the Department of Revenue believed this bill could impact their ability to conduct communication services tax audits. Also, the Committee heard concerns that this bill could impact the ability of the National Center for Missing and Exploited Children from reporting cyber tips to task forces across the country.

Aaron Jones 271-4063

FOR THE CONSENT CALENDAR

COMMERCE

HB 1282, relative to the records of communication common carriers.
Interim Study, Vote 5-0.
Senator Harold French for the committee.

This bill would have prohibited communications common carriers from releasing customer information to government entities unless it was requested through a valid search warrant or exempted under an exception to a warrant. The Committee heard that this bill could have potentially unintended consequences on the operation of all state government agencies. For example, the Department of Revenue believed this bill could impact their ability to conduct communication services tax audits. Also, the Committee heard concerns that this bill could impact the ability of the National Center for Missing and Exploited Children from reporting cyber tips to task forces across the country.

General Court of New Hampshire - Bill Status System

Docket of HB1282

Docket Abbreviations

Bill Title: relative to the records of communication common carriers.

Official Docket of **HB1282.**:

Date	Body	Description
11/19/2021	H	**Introduced** 01/05/2022 and referred to Criminal Justice and Public Safety
1/19/2022	H	Public Hearing: 01/28/2022 02:30 pm LOB 202-204
2/22/2022	H	Executive Session: 01/28/2022 02:30 pm LOB 202-204
2/22/2022	H	Majority Committee Report: Ought to Pass (Vote 14-6; RC)
2/22/2022	H	Minority Committee Report: Inexpedient to Legislate
3/10/2022	H	Lay HB1282 on Table (Rep. Roy): MF DV 160-174 03/10/2022 **HJ 5**
3/10/2022	H	**Ought to Pass**: MA DV 197-137 03/10/2022 **HJ 5**
3/15/2022	S	Introduced 02/24/2022 and Referred to Commerce; **SJ 5**
3/29/2022	S	**Hearing:** 04/05/2022, Room 100, SH, 09:30 am; **SC 14**
4/26/2022	S	Committee Report: Referred to Interim Study, 05/05/2022; Vote 5-0; CC; **SC 18**
5/5/2022	S	Refer to Interim Study, MA, VV; 05/05/2022; **SJ 11**

NH House | NH Senate

Other Referrals

Senate Inventory Checklist for Archives

Bill Number: HB 1282 **Senate Committee:** Commerce

Please include all documents in the order listed below and indicate the documents which have been included with an "X" beside

X Final docket found on Bill Status

Bill Hearing Documents: {Legislative Aides}

X Bill version as it came to the committee

X All Calendar Notices

X Hearing Sign-up sheet(s)

X Prepared testimony, presentations, & other submissions handed in at the public hearing

X Hearing Report

N/A Revised/Amended Fiscal Notes provided by the Senate Clerk's Office

Committee Action Documents: {Legislative Aides}

All amendments considered in committee (including those not adopted):

___ - amendment # _____ ___ - amendment # _____

___ - amendment # _____ ___ - amendment # _____

X Executive Session Sheet

X Committee Report

Floor Action Documents: {Clerk's Office}

All floor amendments considered by the body during session (only if they are offered to the senate):

___ - amendment # _____ ___ - amendment # _____

___ - amendment # _____ ___ - amendment # _____

Post Floor Action: (if applicable) {Clerk's Office}

___ Committee of Conference Report (if signed off by all members. Include any new language proposed by the committee of conference):

___ Enrolled Bill Amendment(s)

___ Governor's Veto Message

All available versions of the bill: {Clerk's Office}

___ as amended by the senate ___ as amended by the house

___ final version

Completed Committee Report File Delivered to the Senate Clerk's Office By:

Aaron Jones 7/7/22

Committee Aide **Date**

Senate Clerk's Office AK