

Committee Report

CONSENT CALENDAR

February 26, 2021

HOUSE OF REPRESENTATIVES

REPORT OF COMMITTEE

The Committee on Executive Departments and Administration to which was referred HB 499,

AN ACT prohibiting the state from using a face recognition system. Having considered the same, report the same with the following amendment, and the recommendation that the bill OUGHT TO PASS WITH AMENDMENT.

Rep. Carol McGuire

FOR THE COMMITTEE

COMMITTEE REPORT

Committee:	Executive Departments and Administration
Bill Number:	HB 499
Title:	prohibiting the state from using a face recognition system.
Date:	February 26, 2021
Consent Calendar:	CONSENT
Recommendation:	OUGHT TO PASS WITH AMENDMENT 2021-0247h

STATEMENT OF INTENT

This bill prevents any state database of facial images (drivers' license photos, for one) from being used to identify a photo of an unknown person using facial recognition software. At the current time, no such photo database is used this way by the state. The committee amendment prohibits use of data from face recognition in a New Hampshire court, unless it has been authorized by a search warrant. The committee heard concerns that face recognition is used for identifying lost children and seniors, as well as victims of sexual predators and human traffickers, but decided not to exempt this use for two reasons: first, facial recognition is at its most faulty in dealing with seniors, children, people of color, and women, so it is not likely to provide more than a hint to someone's identity; secondly, under these circumstances, we were assured a warrant could be obtained very quickly.

Vote 17-1.

Rep. Carol McGuire
FOR THE COMMITTEE

Original: House Clerk
Cc: Committee Bill File

CONSENT CALENDAR

Executive Departments and Administration

HB 499, prohibiting the state from using a face recognition system. **OUGHT TO PASS WITH AMENDMENT.**

Rep. Carol McGuire for Executive Departments and Administration. This bill prevents any state database of facial images (drivers' license photos, for one) from being used to identify a photo of an unknown person using facial recognition software. At the current time, no such photo database is used this way by the state. The committee amendment prohibits use of data from face recognition in a New Hampshire court, unless it has been authorized by a search warrant. The committee heard concerns that face recognition is used for identifying lost children and seniors, as well as victims of sexual predators and human traffickers, but decided not to exempt this use for two reasons: first, facial recognition is at its most faulty in dealing with seniors, children, people of color, and women, so it is not likely to provide more than a hint to someone's identity; secondly, under these circumstances, we were assured a warrant could be obtained very quickly. **Vote 17-1.**

Original: House Clerk

Cc: Committee Bill File

Amendment to HB 499

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

2

3 AN ACT relative to the use of face recognition technology.

4

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

6

7 1 New Subdivision; Breaches of the Peace; Face Recognition Technology Prohibited. Amend
8 RSA 644 by inserting after section 22 the following new subdivision:

9 Face Recognition Technology Prohibited

10 644:23 Definitions. In this subdivision:

11 I. "Face recognition technology" means an automated or semi-automated process that assists
12 in identifying or tracking an individual or capturing information about an individual, based on the
13 physical characteristics of an individual's face. It does not include the process by which an
14 individual visually identifies another individual by viewing a representation of the individual on a
15 computer, video recording, photograph or other media.

16 II. "State" means any department, agency, bureau, or administrative unit of the state of
17 New Hampshire, including any city, town, county, school district, or municipal entity therein.

18 644:24 Use of Face Recognition Technology; Requirements. The state shall only use face
19 recognition technology if it has a search warrant supported by probable cause and signed by a
20 neutral and detached magistrate.

21 644:25 Evidence Inadmissible.

22 I. Any data or information collected or derived from the state's own use of face recognition
23 technology in violation of this subdivision shall be inadmissible in any trial, hearing, or other
24 proceeding in or before any court or regulatory agency in the state of New Hampshire.

25 II. Any evidence derived from data or information collected from any use of face recognition
26 technology in violation of this subdivision shall be inadmissible in any trial, hearing, or other
27 proceeding in or before any court or regulatory agency in the state of New Hampshire, unless
28 sufficiently attenuated from the original violation, including but not limited, to an affirmative
29 showing that no state official had requested, facilitated, or otherwise caused the use of face
30 recognition technology by an entity other than the state as defined above.

31 2 Drivers' Licenses; Use of Facial Recognition Technology Prohibited. RSA 263:40-b is repealed
32 and reenacted to read as follows:

Amendment to HB 499

- Page 2 -

1 263:40-b Use of Face Recognition Technology Prohibited. The department shall not allow access
2 to any of its digital representations of faces by any face recognition technology nor shall the
3 department use face recognition technology. No state agency, other than the department, shall
4 create or maintain a searchable database of face images.

5 3 Effective Date. This act shall take effect 60 days after its passage.

Amendment to HB 499
- Page 3 -

2021-0247h

AMENDED ANALYSIS

This bill permits the state to use face recognition technology if it has a warrant supported by probable cause.

Archived: Tuesday, April 20, 2021 9:30:56 AM
From: [Miriam Simmons](#)
Sent: Tuesday, April 20, 2021 8:59:35 AM
To: [Miriam Simmons](#)
Subject: HB 499 CR - Rep McGuire
Response requested: No
Importance: Normal

From: Carol McGuire <mcguire4house@gmail.com>
Sent: Saturday, February 27, 2021 3:44 PM
To: [Miriam Simmons](#) <miriam.simmons@leg.state.nh.us>; [Pam Smarling](#) <Pam.Smarling@leg.state.nh.us>
Subject: my blurbs

HB 499, face recognition

OTP/A, 17-1, consent

This bill prevents any state database of facial images (drivers' license photos, for one) from being used to identify a photo of an unknown by facial recognition software. At the current time, no such photo database is used this way by the state. The committee amendment prohibits use of data from face recognition in a New Hampshire court, unless it has been authorized by a search warrant. The committee heard concerns that face recognition is used for identifying lost children and seniors, as well as victims of sexual predators and human traffickers, but decided not to exempt this use for two reasons: first, facial recognition is at its most faulty in dealing with seniors, children, people of color, and women, so it is not likely to provide more than a hint to someone's identity; secondly, under these circumstances, we were assured a warrant could be obtained very quickly.

Carol McGuire for the committee

Voting Sheets

HOUSE COMMITTEE ON EXECUTIVE DEPARTMENTS & ADMINISTRATION

EXECUTIVE SESSION on Bill # ^{HB} 499

BILL TITLE: PROHIBITING THE STATE FROM USING A FACE RECOGNITION SYSTEM

DATE: 2-26-21

LOB ROOM: 301-303

MOTION: (Please check one box)

OTP ITL Retain (1st year) Adoption of Amendment # 0247H (if offered)
 Interim Study (2nd year)
 Moved by Rep. M. GROVE Seconded by Rep. GOLEY Vote: 19-0

MOTION: (Please check one box)

OTP OTP/A ITL Retain (1st year) Adoption of Amendment # _____ (if offered)
 Interim Study (2nd year)
 Moved by Rep. M. GOVINE Seconded by Rep. GOLEY Vote: 17-1

MOTION: (Please check one box)

OTP OTP/A ITL Retain (1st year) Adoption of Amendment # _____ (if offered)
 Interim Study (2nd year)
 Moved by Rep. _____ Seconded by Rep. _____ Vote: _____

MOTION: (Please check one box)

OTP OTP/A ITL Retain (1st year) Adoption of Amendment # _____ (if offered)
 Interim Study (2nd year)
 Moved by Rep. _____ Seconded by Rep. _____ Vote: _____

CONSENT CALENDAR: YES _____ NO

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

Respectfully submitted: John Sytek
 Rep. John Sytek, Clerk



2021 SESSION

Executive Departments and Administration

Bill #: HB 499 Motion: ADOPT AMENDMENT AM #: 024741 Exec Session Date: 2-26-21

<u>Members</u>	<u>YEAS</u>	<u>Nays</u>	<u>NV</u>
McGuire, Carol M. Chairman	X		
Roy, Terry Vice Chairman	X		
Sytek, John Clerk	X		
Pearson, Stephen C.	X		
Yakubovich, Michael	X		
Lekas, Tony	X		
Alliegro, Mark C.	X		
Bailey, Glenn	X		
Lanzara, Tom E. TANLIVER DOUCETTE	X		
Santonastaso, Matthew	8		
Goley, Jeffrey P.	X		
Schuett, Dianne E.	X		
Judy, Jean L.	X		
Schmidt, Peter B.	X		
Schultz, Kristina M.	X		
Fellows, Sallie D.	X		
Fontneau, Timothy J. TANNER	X		
Grote, Jaci L.	X		
O'Brien, Michael B. PIMENTEL	X		
TOTAL VOTE:			

19-0



2021 SESSION

Executive Departments and Administration

Bill #: HB 499 Motion: ORP/A AM #: 0247H Exec Session Date: 2-26-21

<u>Members</u>	<u>YEAS</u>	<u>Nays</u>	<u>NV</u>
McGuire, Carol M. Chairman	X		
Roy, Terry Vice Chairman	X		
Sytek, John Clerk		X	
Pearson, Stephen C.	X		
Yakubovich, Michael	X		
Lekas, Tony	X		
Alliegro, Mark C.	X		
Bailey, Glenn	X		
Lanzara, Tom E. <i>DOVLOTTE</i>	X		
Santonastaso, Matthew			X
Goley, Jeffrey P.	X		
Schuett, Dianne E.	X		
Jeudy, Jean L.	X		
Schmidt, Peter B.	X		
Schultz, Kristina M.	X		
Fellows, Sallie D.	X		
Fentribeau, Timothy J. <i>TANNER</i>	X		
Grote, Jaci L.	X		
O'Brien, Michael B. <i>PRIMENTEL</i>	X		
TOTAL VOTE:			

17-1

Amendment to HB 499

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

2

3 AN ACT relative to the use of face recognition technology.

4

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

6

7 1 New Subdivision; Breaches of the Peace; Face Recognition Technology Prohibited. Amend
8 RSA 644 by inserting after section 22 the following new subdivision:

9 Face Recognition Technology Prohibited

10 644:23 Definitions. In this subdivision:

11 I. "Face recognition technology" means an automated or semi-automated process that assists
12 in identifying or tracking an individual or capturing information about an individual, based on the
13 physical characteristics of an individual's face. It does not include the process by which an
14 individual visually identifies another individual by viewing a representation of the individual on a
15 computer, video recording, photograph or other media.

16 II. "State" means any department, agency, bureau, or administrative unit of the state of
17 New Hampshire, including any city, town, county, school district, or municipal entity therein.

18 644:24 Use of Face Recognition Technology; Requirements. The state shall only use face
19 recognition technology if it has a search warrant supported by probable cause and signed by a
20 neutral and detached magistrate.

21 644:25 Evidence Inadmissible.

22 I. Any data or information collected or derived from the state's own use of face recognition
23 technology in violation of this subdivision shall be inadmissible in any trial, hearing, or other
24 proceeding in or before any court or regulatory agency in the state of New Hampshire.

25 II. Any evidence derived from data or information collected from any use of face recognition
26 technology in violation of this subdivision shall be inadmissible in any trial, hearing, or other
27 proceeding in or before any court or regulatory agency in the state of New Hampshire, unless
28 sufficiently attenuated from the original violation, including but not limited, to an affirmative
29 showing that no state official had requested, facilitated, or otherwise caused the use of face
30 recognition technology by an entity other than the state as defined above.

31 2 Drivers' Licenses; Use of Facial Recognition Technology Prohibited. RSA 263:40-b is repealed
32 and reenacted to read as follows:

1 263:40-b Use of Face Recognition Technology Prohibited. The department shall not allow access
2 to any of its digital representations of faces by any face recognition technology nor shall the
3 department use face recognition technology. No state agency, other than the department, shall
4 create or maintain a searchable database of face images.

5 3 Effective Date. This act shall take effect 60 days after its passage.

UNAPPROVED

2021-0247h

AMENDED ANALYSIS

This bill permits the state to use face recognition technology if it has a warrant supported by probable cause.

UNAPPROVED

Hearing Minutes

HOUSE COMMITTEE ON EXECUTIVE DEPARTMENTS AND ADMINISTRATION

PUBLIC HEARING ON HB 499

BILL TITLE: prohibiting the state from using a face recognition system.

DATE(s): FEB 11th and February 18, 2021

LOB ROOM: LOB Hybrid **Time Public Hearing Called to Order:** FEB 11th

Time Adjourned: FEB 18th

FEB 11th ATTENDANCE

2021-02-11

RECESSED
Time Adjourned: 11:30
TO 11 AM 2/18

(please circle if present)

Committee Members: Reps. McGuire, Roy, Sytek, S. Pearson, Yakubovich, Lekas, Alliegro, Bailey, Lanzara, Santonastaso, P. Schmidt, Schultz, Goley, Judy, Schuett, Fellows, Fontneau, Grote, M. O'Brien *all present*

FEB 18th ATTENDANCE

ALL Members Present

Bill Sponsors:

Rep. McGuire
Rep. Hopper
Sen. Reagan

Rep. M. Smith
Rep. T. Lekas

Rep. Berch
Rep. Merchant

TESTIMONY

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

HB 499 prohibiting the state from using face recognition system. (10:45/recessed at 11:30 to 11 AM, Feb. 18 so as not to interfere with Governor's budget address)

Rep. McGuire introduced the bill and spoke in favor.

She said that there are two parts to the bill. The first was developed by Rep. Berch and deals with restrictions as to how face recognition can be used in court.

There is another amendment dealing with restrictions more broadly. *She could support either.* She was concerned with the second part of the bill which would prohibit the state from engaging in a face recognitions system. The DOT could not use its data base (driver's license photos) for face recognition use, allowing other state agencies to use the DOT data base and would prohibit other state agencies from keeping a searchable face recognition date base.

She said that Dept of HHS had a data base of photos but that it was not searchable by face recognition. This is not being done at this time; this bill is preventive. This bill would not affect private entities.

Rep. Marjorie Smith spoke in favor.

She gave a history of previous similar legislation that was passed by the House and sent to Judiciary which voted ITL. She feels that this bill is important; her concern is privacy and civil rights and liberties.

She has an amendment (0247h) which allows the correct use of facial recognition (Rep. McGuire is also a sponsor of the amendment) and prevents the deleterious “minuses” of facial recognition when used badly – especially towards people of color and women. The amendment would require the police to get a warrant to use facial recognition. There were many questions.

Albert “Buzz” Scherr, a professor at the UNH School of Law spoke in opposition to the bill as written but supports the amendment.

Cites his involvement and interest in privacy rights. He cites the difficulty in applying the 4th amendment of the Bill of Rights since new technology deals with non-tangible data. *He raised many possible current issues:* putting a GPS on a suspect’s car, getting DNA from discarded cigarette butts, do you lose all privacy rights when you are out in public? He discussed the shortcomings of the original bill and felt that the amendment was very important.

Public hearing recessed at 11:30 a.m. to be reconvened on February 18, 2021

HB 499 prohibiting the state from using face recognition system. (This hearing was recessed on Feb. 11. It was reopened at 11:05, Feb. 18 and closed at 12:05)

Rep. Berch, co-sponsor, spoke in support of the unamended bill. He described his experience as a public defender and was knowledgeable concerning pedophile offenders and their use of the internet; how warrants work. He said that internet facial recognition was not evidence; that it was a tool by police to pursue leads and to develop evidence and gave examples of its use and described a typical case might be investigated and to develop probable cause. He said that the problem with the amendment is that a warrant would not be issued in a typical case and would prevent further investigation. He said that pedophiles were very knowledgeable in this area and that no other state has this amendment and would result, in his opinion, pedophiles who are mobile being drawn to NH.

He was asked by the prime sponsor that would balance facial recognition with civil liberties. He said this bill was based on a bipartisan bill in the US Senate where he felt nothing much was moving. He described the principles underlying the bill: a guardrail protecting privacy and the circumstances under which facial recognition could be used with safeguards as with any other investigative tool. He described the circumstances under which a warrant would be required.

Question: In answer to a question as to whether a middle ground between the bill and the amendment was possible, he said this bill was the compromise.

Jeanne Hruska, Political Director of the ACLU, supports a ban on facial recognition and is opposed to this bill. The main concern is that it is invasive and inaccurate especially with respect to people of color, older people and children. She could support the amendment as a compromise. She wanted this controlled because you couldn’t “get the genie back in the bottle” once facial recognition was in ubiquitous use. She also said that there should be no 72-hour window; a warrant should be obtained immediately. She said that warrants are ordinary business.

Capt. Joe Ebert, state police, oversees the investigative division, spoke against the amendment because of the difficulty of getting a warrant. He answered questions concerning how facial recognition would be used in NH and whether the bill without amendment would act as a draw for predators visiting NH.

Albert “Buzz” Scherr, a professor at UNH School of Law, disagreed with Rep. Berch about the difficulty of obtaining a warrant. His experience is that if the police come with a picture with an underage possibility a judge would issue a warrant. He pointed out the bill does not mention warrant but rather “court order.”

Rep. Altschiller spoke and disagreed with Prof. Scherr about the ability to get a speedy warrant when time was of the essence and wanted a carve out to prevent its use for seniors and for children.

Ross Connolly Deputy Director of Americans For Prosperity NH, spoke in favor. He said facial recognition was a powerful tool for law enforcement and that this bill strikes the right balance.

Public Hearing adjourned on FEB 18th.

**Respectfully submitted by,
Rep. John Sytek
Committee Clerk**

HOUSE COMMITTEE ON EXECUTIVE DEPARTMENTS & ADMINISTRATION

PUBLIC HEARING on Bill # HB 499

BILL TITLE: PROHIBITING THE STATE FROM USING FACIAL RECOGNITION SYSTEMS

DATE: 2-11-21
ROOM: 306-308

Time Public Hearing Called to Order: 10:45 AM
RECESS
Time Adjourned: 11:30
TO 11 AM 2/18

(please circle if present)

Committee Members: Reps. McGuire, Roy, Sytek, S. Pearson, Yakubovich, Lekas, Alliegro, Bailey, Lanzara, Santonastaso, P. Schmidt, Schultz, Goley, Jedy, Schuett, Fellows, Fontneau, Grote, M. O'Brien *all present*

TESTIMONY

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

HB 499 prohibiting the state from using face recognition system. (10:45/recessed at 11:30 to 11 AM, Feb. 18 so as not to interfere with Governor's budget address)

Rep. McGuire introduced the bill and spoke in favor. She said that there are two parts to the bill. The first was developed by Rep. Berch and deals with restrictions as to how face recognition can be used in court. There is another amendment dealing with restrictions more broadly. She could support either. She was concerned with the second part of the bill which would prohibit the state from engaging in a face recognition system. The DOT could not use its data base (driver's license photos) for face recognition use, allowing other state agencies to use the DOT data base and would prohibit other state agencies from keeping a searchable face recognition data base. She said that Dept of HHS had a data base of photos but that it was not searchable by face recognition. This is not being done at this time; this bill is preventive. This bill would not affect private entities.

>Rep. Marjorie Smith spoke in favor. She gave a history of previous similar legislation that was passed by the House and sent to Judiciary which voted ITL. She feels that this bill is important; her concern is privacy and civil rights and liberties. She has an amendment (0247h) which allows the correct use of facial recognition (Rep. McGuire is also a sponsor of the amendment) and prevents the deleterious "minuses" of facial recognition when used badly – especially towards people of color and women. The amendment would require the police to get a warrant to use facial recognition. There were many questions.

>Albert "Buzz" Scherr, a professor at the UNH School of Law spoke in opposition to the bill as written but supports the amendment. Cites his involvement and interest in privacy rights. He cites the difficulty in applying the 4th amendment of the Bill of Rights since new technology deals with non-tangible data. He raised many possible current issues: putting a GPS on a suspect's car, getting DNA from discarded cigarette butts, do you lose all privacy rights when you are out in public? He discussed the shortcomings of the original bill and felt that the amendment was very important.

Respectfully submitted,
Rep. John Sytek
EDA Committee Clerk

House Remote Testify

Executive Departments and Administration Committee Testify List for Bill HB499 on 2

Support: 168 Oppose: 8 Neutral: 1 Total to Testify: 5

<u>Name</u>	<u>Email Address</u>	<u>Phone</u>	<u>Title</u>	<u>Representing</u>	<u>Position</u>	<u>Testifying</u>	<u>Support</u>
Berch, Paul	pberch@myfairpoint.net	111.111.1111	An Elected Official	Myself	Support	Yes (6m)	1
Smith, Marjorie	Msmithpen@aol.com	603.868.7500	An Elected Official	Myself	Support	Yes (3m)	1
kurk, neal	rep03281@aol.com	111.111.1111	A Member of the Public	Myself	Support	Yes (3m)	1
Hruska, Jeanne	Jeanne@aclu-nh.org	307.272.8727	A Lobbyist	ACLU-NH	Support	Yes (3m)	1
Connolly, Ross	rconnolly@afphq.org	603.530.1151	A Lobbyist	Americans for Prosperity New Hampshire	Support	Yes (3m)	1
mcclure, melissa	melissamcclure@gmail.com	510.439.6662	A Member of the Public	Myself	Support	No	1
Fogarty, Maggie	mfogarty@afsc.org	603.988.7115	A Lobbyist	American Friends Service Committee - NH	Support	No	1
Manning, Talia	talia.manning+politics@gmail.com	781.752.7087	A Member of the Public	Myself	Support	No	1
Koch, Helmut	helmut.koch.2001@gmail.com	603.491.3306	A Member of the Public	Myself	Support	No	1
Garland, Ann	annhgarland@gmail.com	603.678.8143	A Member of the Public	Myself	Support	No	1
Wood, Jackie	Jackie_wood47@hotmail.com	603.303.0887	A Member of the Public	Myself	Support	No	1
Oxenham, Evan	evan.oxenham@gmail.com	603.727.9368	A Member of the Public	Myself	Support	No	1
Reed, Judith	jureed@keene.edu	603.357.4905	A Member of the Public	Myself	Support	No	1
Mott-Smith, Wiltrud	wmottsm@worldpath.net	603.267.7566	A Member of the Public	Myself	Support	No	1
Carter, Lilian	lcarter0914@gmail.com	603.560.7047	A Member of the Public	Myself	Support	No	1
Perencevich, Ruth	rperence@comcast.net	603.225.7641	A Member of the Public	Myself	Support	No	1
Corell, Elizabeth	Elizabeth.j.corell@gmail.com	603.545.9091	A Member of the Public	Myself	Support	No	1
Hamer, Heidi	heidi.hamer@leg.state.nh.us	603.625.4895	An Elected Official	Myself	Support	No	1
Kelly, Fran	fr.kelly01@gmail.com	603.673.0457	A Member of the Public	Myself	Support	No	1
Lane, Connie	connie.lane@leg.state.nh.us	603.491.7379	An Elected Official	Merrimack 12	Support	No	1
Rettew, Annie	abrettw@gmail.com	603.651.7000	A Member of the Public	Myself	Support	No	1
Richman, Susan	susan7richman@gmail.com	603.343.6314	A Member of the Public	Myself	Support	No	1
M, Sandra	S-l-robinson@hotmail.com	603.555.5555	A Member of the Public	Myself	Support	No	1
Hackmann, Kent	hackmann@uidaho.edu	603.934.3225	A Member of the Public	Myself	Support	No	1
Wilbur, Kathleen	kathy.wilbur55@gmail.com	603.437.1882	A Member of the Public	Myself	Support	No	1
Voelcker, Elsa	elsavoelcker1@gmail.com	603.831.1434	A Member of the Public	Myself	Support	No	1
Bruce, Susan	susanb.red@mac.com	603.730.7078	A Member of the Public	Myself	Support	No	1
Hinebauch, Mel	melhinebauch@gmail.com	603.224.4866	A Member of the Public	Myself	Support	No	1
Rich, Cecilia	ceciliarich@hotmail.com	603.380.8679	An Elected Official	Myself	Support	No	1
Booras, Efstathia	Efstathia.Booras@leg.state.nh.us	603.595.7699	An Elected Official	Constituents	Support	No	1
KOLIFRATH, LAUREN	LULUKOLIF@GMAIL	603.548.5405	A Member of the Public	Myself	Support	No	1
Ferrara, Crissie	cmferrara@gmail.com	917.963.3568	A Member of the Public	Myself	Support	No	1
Katzman, Jacki	jackisue@aol.com	603.869.3289	A Member of the Public	Myself	Support	No	1
Evankow, Abby	abbyaustin89@gmail.com	4663037	A Member of the Public	Myself	Support	No	1
Brown, Angela	angela_f_brown@yahoo.com	603.466.2578	A Member of the Public	Myself	Support	No	1
DePuy, Charles	c.depuy@yahoo.com	603.448.0063	A Member of the Public	Myself	Support	No	1
Blank, Kim	blank.kimberly@gmail.com	518.944.1173	A Member of the Public	Myself	Support	No	1
QUISUMBING-KING, Cora	coraq@comcast.net	603.343.4347	A Member of the Public	Myself	Support	No	1
Kingston, Bill	DC9guy@comcast.net	603.431.7876	A Member of the Public	Myself	Support	No	1
Cross, John	jc938272@gmail.com	781.879.5442	A Member of the Public	Myself	Support	No	1
Dejoie, John	jdejoie@kamerbluestrategies.com	603.682.8531	A Lobbyist	National Association of Social Workers - NH Chapter	Support	No	1
Wotowiec, Peter	ticonel@gmail.com	603.852.0459	A Member of the Public	Myself	Support	No	1

Cranage, Amy	cranhan@comcast.net	603.252.8531	A Member of the Public	Myself	Support	No	2
Benham, Linda	benhamblab@outlook.com	603.373.8741	A Member of the Public	Myself	Support	No	2
Bennett, Olivia	helloodb@gmail.com	603.801.7596	A Member of the Public	Myself	Support	No	2
Mousseau, Cynthia	cynthia.mousseau@gmail.com	518.593.2219	A Member of the Public	Myself	Oppose	No	2
Snyder, Logan	snyder.h.a@gmail.com	603.783.0370	A Member of the Public	Myself	Support	No	2
Stevens, Representative Deb	debstevens4ward7@gmail.com	603.820.0866	An Elected Official	Nashua Ward 7 Hillsborough 34	Support	No	2
Schwartzman, Anne	akey5@nycap.rr.com	518.693.6395	A Member of the Public	Myself	Support	No	2
King, Walter	genedocwk@gmail.com	603.975.9775	A Member of the Public	Myself	Support	No	2
Marchi, Lisa	lisamarchi@comcast.net	603.743.3369	A Member of the Public	Myself	Support	No	2
Smith-Lopez, Maria	mngsl.21@dartmouth.edu	307.760.9316	A Member of the Public	Myself	Support	No	2
Barnes, Ken	kbarnes@kenbarneslaw.com	603.496.9605	A Member of the Public	Myself	Support	No	2
Bosman, Jim	jimbosman@me.com	111.111.1111	A Member of the Public	Myself	Support	No	2
Babladelis, Ashley	ash.hatch@gmail.com	111.111.1111	A Member of the Public	Myself	Support	No	2
Millman, Linda	jdm73@phreego.com	111.111.1111	A Member of the Public	Myself	Support	No	2
Pedersen, Michael	PedersenUSA@aim.com	603.801.0878	An Elected Official	Hillsborough 32	Support	No	2
Phillips, margery	margeryphillips@gmail.com	603.277.2991	A Member of the Public	Myself	Support	No	2
Carter, Sarah	sarahvcarter3@gmail.com	603.918.6032	A Member of the Public	Myself	Support	No	2
Lionel, Steven	steve@stevlionel.com	603.505.8764	A Member of the Public	Myself	Support	No	2
Shanks, Barry	barry.shanks@gmail.com	603.210.2554	A Member of the Public	Myself	Support	No	2
Webb, David	david.l.webb@dartmouth.edu	603.643.5895	A Member of the Public	Myself	Support	No	2
olson, alix	alixmartha22@gmail.com	603.523.7955	A Member of the Public	Myself	Support	No	2
haagen, mary ann	mahaagen@icloud.com	603.448.0063	A Member of the Public	Myself	Support	No	2
Lynch, Chrisinda	cmmelynch@comcast.net	603.225.5614	A Member of the Public	Myself	Support	No	2
Edelson, Rachel	redelson@hotmail.com	603.943.7635	A Member of the Public	Myself	Support	No	2
Lamb, Albert	alamb@pobox.com	603.722.0304	A Member of the Public	Myself	Support	No	2
Lamb, Ashley	campioa@gmail.com	603.722.0304	A Member of the Public	Myself	Support	No	2
Harris, Pamela	pampsharris@aol.com	203.613.2201	A Member of the Public	Myself	Support	No	2
Harris, Jeffrey	Jharris@jmhwealth.com	603.667.6603	A Member of the Public	Myself	Support	No	2
Ellis, Donna	donna.ellis@state.nh.us	603.332.5266	An Elected Official	Myself	Support	No	2
Blair, David	orionblair@gmail.com	603.828.6804	A Member of the Public	Myself	Support	No	2
Gordon, Carolyn	csgordon@dartmouth.edu	603.643.5895	A Member of the Public	Myself	Support	No	2
Davis, Melissa	melissalynndavis@gmail.com	408.627.9877	A Member of the Public	Myself	Support	No	2
Thompson, Laura	nicnmom@hotmail.com	603.553.0100	A Member of the Public	Myself	Support	No	2
Lister, Charlotte	lister@gsinet.net	603.887.4185	A Member of the Public	Myself	Support	No	2
Feder, Marsha	marshafeder@gmail.com	603.860.8743	A Member of the Public	Myself	Support	No	2
Fordey, Nicole	nikkif610@gmail.com	516.318.2296	A Member of the Public	Myself	Oppose	No	2
Fordey, Patrick	patrick.fordey@googlemail.com	781.999.3172	A Member of the Public	Myself	Oppose	No	2
Gould, Rep. Linda	lgouldr@myfairpoint.net	603.472.3877	An Elected Official	Myself	Support	No	2
Bouchard, Donald	donaldjbouchard@gmail.com	603.622.0388	An Elected Official	Myself	Support	No	2
Feder, Robert	robertfeder1@gmail.com	603.860.2593	A Member of the Public	Myself	Support	No	2
Hatcher, Phil	phil.hatcher@gmail.com	603.988.8034	A Member of the Public	Myself	Support	No	2
Grossi, Anne	adgrossi7982@gmail.com	603.674.1181	A Member of the Public	Myself	Support	No	2
Koch, Laurie	kochlj@aol.com	603.491.2000	A Member of the Public	Myself	Support	No	2
Blanchard, Sandra	sandyblanchard3@gmail.com	603.724.3768	A Member of the Public	Myself	Support	No	2
Spillers, Jessica	jspillers102@gmail.com	603.801.6772	A Member of the Public	Myself	Support	No	2
Spencer, Louise	kentstusa@aol.com	603.491.1795	A Member of the Public	Myself	Support	No	2
Spencer, Rob	kentstusa@aol.com	603.555.5555	A Member of the Public	Myself	Support	No	2
Long, Julian	julianleelong@yahoo.com	603.767.1953	A Member of the Public	Myself	Support	No	2
Damon, Claudia	cordsdamon@gmail.com	603.226.4561	A Member of the Public	Myself	Support	No	2
Larson, Ruth	ruthlarson@msn.com	603.364.4003	A Member of the Public	Myself	Support	No	2
Torpey, Jeanne	jtorp51@comcast.net	603.493.8262	A Member of the Public	Myself	Support	No	2
Yokela, Josh	josh.yokela@leg.state.nh.us	603.722.0501	An Elected Official	Rockingham 33	Support	No	2
Garen, June	jzanesgaren@gmail.com	603.393.8134	A Member of the Public	Myself	Support	No	2
HARRIS, COLE	Cethanharris@gmail.com	603.727.2943	A Member of the Public	Myself	Support	No	2
Farley, Teresa	tdfarley@outlook.com	425.890.4413	A Member of the Public	Myself	Support	No	2
Harris, Anna	sirrahfa10@gmail.com	603.727.2942	A Member of the Public	Myself	Oppose	No	2

Layon, Erica	erica.layon@leg.state.nh.us	603.479.9595	An Elected Official	Myself	Support	No	2
Dontonville, Roger	rdontonville@gmail.com	603.632.7719	An Elected Official	Myself	Support	No	2

HB 499 prohibiting the state from using face recognition system. (This hearing was recessed on Feb. 11. It was reopened at 11:05, Feb. 18 and closed at 12:05)

>Rep. Berch, co-sponsor, spoke in support of the unamended bill. He described his experience as a public defender and was knowledgeable concerning pedophile offenders and their use of the internet; how warrants work. He said that internet facial recognition was not evidence; that it was a tool by police to pursue leads and to develop evidence and gave examples of its use and described a typical case might be investigated and to develop probable cause. He said that the problem with the amendment is that a warrant would not be issued in a typical case and would prevent further investigation. He said that pedophiles were very knowledgeable in this area and that no other state has this amendment and would result, in his opinion, pedophiles who are mobile being drawn to NH. He was asked by the prime sponsor that would balance facial recognition with civil liberties. He said this bill was based on a bipartisan bill in the US Senate where he felt nothing much was moving. He described the principles underlying the bill: a guardrail protecting privacy and the circumstances under which facial recognition could be used with safeguards as with any other investigative tool. He described the circumstances under which a warrant would be required. In answer to a question as to whether a middle ground between the bill and the amendment was possible, he said this bill was the compromise.

>Jeanne Hruska, Political Director of the ACLU, supports a ban on facial recognition and is opposed to this bill. The main concern is that it is invasive and inaccurate especially with respect to people of color, older people and children. She could support the amendment as a compromise. She wanted this controlled because you couldn't "get the genie back in the bottle" once facial recognition was in ubiquitous use. She also said that there should be no 72-hour window; a warrant should be obtained immediately. She said that warrants are ordinary business.

>Capt. Joe Ebert, state police, oversees the investigative division, spoke against the amendment because of the difficulty of getting a warrant. He answered questions concerning how facial recognition would be used in NH and whether the bill without amendment would act as a draw for predators visiting NH.

>Albert "Buzz" Scherr, a professor at UNH School of Law, disagreed with Rep. Berch about the difficulty of obtaining a warrant. His experience is that if the police come with a picture with an underage possibility a judge would issue a warrant. He pointed out the bill does not mention warrant but rather "court order."

>Rep. Altschiller spoke and disagreed with Prof. Scherr about the ability to get a speedy warrant when time was of the essence and wanted a carve out to prevent its use for seniors and for children.

>Ross Connolly Deputy Director of Americans For Prosperity NH, spoke in favor. He said facial recognition was a powerful tool for law enforcement and that this bill strikes the right balance.

House Remote Testify

Executive Departments and Administration Committee Testify List for Bill HB499 on 2

Support: 43 Oppose: 3 Neutral: 0 Total to Testify: 1

<u>Name</u>	<u>City, State</u> <u>Email Address</u>	<u>Title</u>	<u>Representing</u>	<u>Position</u>	<u>Testifying</u>	<u>S</u>
Hruska, Jeanne	Jeanne@aclu-nh.org	A Lobbyist	ACLU-NH	Support	Yes (3m)	2
Lamb, Ashley	campioa@gmail.com	A Member of the Public	Myself	Support	No	2
Babb, Paul	paulbabb@protonmail.com	A Member of the Public	Myself	Support	No	2
Krohn, Suzanne	suzanne.c.krohn@gmail.com	A Member of the Public	Myself	Support	No	2
Krohn, Matthew	makrohn@gmail.com	A Member of the Public	Myself	Support	No	2
Larson, Ruth	ruthlarson@msn.com	A Member of the Public	Myself	Support	No	2
Frost, Sherry	sherry.frost@leg.state.nh.us	An Elected Official	Myself	Support	No	2
Brickett, Jane	silofarm@gmail.com	A Member of the Public	Myself	Oppose	No	2
Moulton, Candace	candaceleighm@gmail.com	A Member of the Public	Myself	Support	No	2
Kallinich, Kayla	kaylakall47@gmail.com	A Member of the Public	Myself	Support	No	2
Linehan, Meg	Meganelinehan@gmail.com	A Member of the Public	Myself	Support	No	2
monahan, sean	smlblck66@hotmail.com	A Member of the Public	Myself	Support	No	2
Lambert, Georgina	georginatambert@gmail.com	A Member of the Public	Myself	Support	No	2
Hayes, Rebecca	ruptonhayes@gmail.com	A Member of the Public	Myself	Support	No	2
Key, Kyla	kykey5896@hotmail.com	A Member of the Public	Myself	Support	No	2
Hayden, Sam	hayden.sam@gmail.com	A Member of the Public	Myself	Support	No	2
Gonzalez, Gigi	Qtbabe78@aol.com	A Member of the Public	Myself	Support	No	2
Minihan, Jeremiah	Jeremiah.minihan@gmail.com	A Member of the Public	Myself	Support	No	2
Pauer, Eric	secretary@BrooklineGOP.org	A Member of the Public	Myself	Support	No	2
Lariviere, Kendal	kmlariviere@comcast.net	A Member of the Public	Myself	Support	No	2
Wallace, Andrew	andywallace25@gmail.com	A Member of the Public	Myself	Support	No	2
Carr, Joanna	Canaan, NH Jcarrjj@gmail.com	A Member of the Public	Myself	Oppose	No	2
Buck, Jeana	Evansville, IN Jeanab5@twc.com	A Member of the Public	Myself	Support	No	2
DeMark, Richard	Meredith, NH demarknh114@gmail.com	A Member of the Public	Myself	Support	No	2
kurk, neal	weare, NH rep03281@aol.com	A Member of the Public	Myself	Support	No	2
Hope, Lucinda	Tilton, NH lmhope46@gmail.com	A Member of the Public	Myself	Support	No	2
Van, Kevin	Milford, NH Kvan@gmail.com	A Member of the Public	Myself	Support	No	2
Mennella, Alexandra	Hooksett, NH amennella1@protonmail.com	A Member of the Public	Myself	Support	No	2
Carter, Marissa	Holderness, NH marissac974@outlook.com	A Member of the Public	Myself	Support	No	2

THORNTON, HARRY	Candia, NH HTHORNTON285@proton.com	A Member of the Public	Myself	Support	No	2
ARONSON, LAURA	MANCHESTER, NH laura@mlans.net	A Member of the Public	Myself	Support	No	2
Axelman, Elliot	HOOKSETT, NH aluaxelman@gmail.com	A Member of the Public	Myself	Support	No	2
Stinson, Benjamin	Concord, NH benrkstinson@gmail.com	A Member of the Public	Myself	Support	No	2
Thomas, Nicholas	Manchester, NH nicholas.w.thomas@uconn.edu	A Member of the Public	Myself	Support	No	2
Groetzing, Tonda	Farmington, NH groetzing6@aol.com	A Member of the Public	Myself	Support	No	2
Altschiller, Rep. Debra	Stratham, NH debra.altschiller@leg.state.nh.us	An Elected Official	Stratham, Rockingham 19	Oppose	No	2
Mott-Smith, Wiltrud	Loudon, NH wmottsm@worldpath.net	A Member of the Public	Myself	Support	No	2
Heslin, Mary	Concord, NH mlheslin@yahoo.com	A Member of the Public	Myself	Support	No	2
McCue, Dara	Meredith, NH daramccue@gmail.com	A Member of the Public	Myself	Support	No	2
Howard Jr., Raymond	Alton, NH brhowardjr@yahoo.com	An Elected Official	Myself	Support	No	2
Hudnall, Linda	Robertsdale, AL LHudn003@aol.com	A Member of the Public	Myself	Support	No	2
Warner, Amy	Exeter, NH amywarner81@gmail.com	A Member of the Public	Myself	Support	No	2
Bostic, Carol	South Hampton, NH carol@carolbostic.com	A Member of the Public	Myself	Support	No	2
Lekas, Alicia	Hudson, NH rep.alicia.lekas@gmail.com	An Elected Official	Hillsborough 37	Support	No	2
Perry, Apryl	Antrim, NH apryl.perry@gmail.com	A Member of the Public	Myself	Support	No	2
Richman, Susan	susan7richman@gmail.com	A Member of the Public	Myself	Support	No	2

Testimony

Facial Recognition Can Find Rioters, but May Harm Others

The AI-driven technology has been helping officials identify those who stormed the Capitol on Jan. 6, but it also has been found to have racial biases. Officials must balance the potential benefits with the risks.

Johana Bhuiyan, Los Angeles Times | February 5, 2021 | Analysis

(TNS) — In the days following the Jan. 6 riot at the nation’s Capitol, there was a rush to identify those who had stormed the building’s hallowed halls.

Instagram accounts with names like Homegrown Terrorists popped up, claiming to use AI software and neural networks to trawl publicly available images to identify rioters. Researchers such as the cybersecurity expert John Scott-Railton said they deployed facial recognition software to detect trespassers, including a retired Air Force lieutenant alleged to have been spotted on the Senate floor during the riot. Clearview AI, a leading facial recognition firm, said it saw a 26 percent jump in usage from law enforcement agencies on Jan. 7.

A low point for American democracy had become a high point for facial recognition technology.

Facial recognition’s promise that it will help law enforcement solve more cases, and solve them quickly, has led to its growing use across the country. Concerns about privacy have not stopped the spread of the technology — law enforcement agencies performed 390,186 database searches to find facial matches for pictures or video of more than 150,000 people between 2011 and 2019, according to a U.S. Government Accountability Office report. Nor has the growing body of evidence showing that the implementation of facial recognition and other surveillance tech has disproportionately harmed communities of color.

Yet in the aftermath of a riot that included white supremacist factions attempting to overthrow the results of the presidential election, it’s communities of color that are warning about the potential danger of this software.

“It’s very tricky,” said Chris Gilliard, a professor at Macomb Community College and a Harvard Kennedy School Shorenstein Center visiting research fellow. “I don’t want it to sound like I don’t want white supremacists or insurrectionists to be held accountable. But I do think because systemically most of those forces are going to be marshaled against Black and brown folks and immigrants it’s a very tight rope. We have to be careful.”

Black, brown, poor, trans and immigrant communities are “routinely over-policed,” Steve Renderos, the executive director of Media Justice, said, and that’s no different when it comes to surveillance.

“This is always the response to moments of crises: Let’s expand our policing, let’s expand the reach of surveillance,” Renderos said. “But it hasn’t done much in the way of keeping our communities actually safe from violence.”

Biases and Facial Recognition

On Jan. 9, 2020, close to a year before the Capitol riots, Detroit police arrested a Black man named Robert Williams on suspicion of theft. In the process of his interrogation, two things were made clear: Police arrested him based on a facial recognition scan of surveillance footage and the “computer must have gotten it wrong,” as the interrogating officer was quoted saying in a complaint filed by the ACLU.

The charges against Williams were ultimately dropped.

Williams' is one of two known cases of a wrongful arrest based on facial recognition. It's hard to pin down how many times facial recognition has resulted in the wrong person being arrested or charged because it's not always clear when the tool has been used. In Williams' case, the giveaway was the interrogating officer admitting it.

Gilliard argues instances like Williams' may be more prevalent than the public yet knows. "I would not believe that this was the first time that it's happened. It's just the first time that law enforcement has slipped up," Gilliard said.

Facial recognition technology works by capturing, indexing and then scanning databases of millions of images of people's faces — 641 million as of 2019 in the case of the FBI's facial recognition unit — to identify similarities. Those images can come from government databases, like driver's license pictures, or, in the case of Clearview AI, files scraped from social media or other websites.

Research shows the technology has fallen short in correctly identifying people of color. A federal study released in 2019 reported that Black and Asian people were about 100 times more likely to be misidentified by facial recognition than white people.

The problem may be in how the software is trained and who trains it. A study published by the AI Now Institute of New York University concluded that artificial intelligence can be shaped by the environment in which it is built. That would include the tech industry, known for its lack of gender and racial diversity. Such systems are being developed almost exclusively in spaces that "tend to be extremely white, affluent, technically oriented, and male," the study reads. That lack of diversity may extend to the data sets that inform some facial recognition software, as studies have shown some were largely trained using databases made up of images of lighter-skinned males.

But proponents of facial recognition argue when the technology is developed properly — without racial biases — and becomes more sophisticated, it can actually help avoid cases of misidentification.

Clearview AI chief executive Hoan Ton-That said an independent study showed his company's software, for its part, had no racial biases.

"As a person of mixed race, having non-biased technology is important to me," Ton-That said. "The responsible use of accurate, non-biased facial recognition technology helps reduce the chance of the wrong person being apprehended. To date, we know of no instance where Clearview AI has resulted in a wrongful arrest."

Jacob Snow, an attorney for the ACLU — which obtained a copy of the study in a public records request in early 2020 — called the study into question, telling BuzzFeed News it was "absurd on many levels."

More than 600 law enforcement agencies use Clearview AI, according to the *New York Times*. And that could increase now. Shortly after the attack on the Capitol, an Alabama police department and the Miami police reportedly used the company's software to identify people who participated in the riot. "We are working hard to keep up with the increasing interest in Clearview AI," Ton-That said.

Considering the distrust and lack of faith in law enforcement in the Black community, making facial recognition technology better at detecting Black and brown people isn't necessarily a welcome improvement. "It is not social progress to make black people equally visible to software that will inevitably be further weaponized against us," doctoral candidate and activist Zoé Samudzi wrote.

Responding with Surveillance

In the days after the Capitol riot, the search for the "bad guys" took over the internet. Civilian internet sleuths were joined by academics, researchers, as well as journalists in scouring social media to identify rioters. Some journalists even used facial recognition software to report what was happening inside the Capitol. The FBI put a call out for tips, specifically asking for photos or videos depicting rioting or violence, and many of those scouring

the internet or using facial recognition to identify rioters answered that call.

The instinct to move quickly in response to crises is a familiar one, not just to law enforcement but also to lawmakers. In the immediate aftermath of the riot, the FBI Agents Assn. called on Congress to make domestic terrorism a federal crime. President Biden has asked for an assessment of the domestic terrorism threat and is coordinating with the National Security Council to “enhance and accelerate” efforts to counter domestic extremism, according to NBC News.

But there is worry that the scramble to react will lead to rushed policies and increased use of surveillance tools that may ultimately hurt Black and brown communities.

“The reflex is to catch the bad guys,” Gilliard said. “But normalizing what is a pretty uniquely dangerous technology causes a lot more problems.”

Days after the riot, Rep. Lou Correa (D-Santa Ana) helped reintroduce a bill called the Domestic Terrorism Prevention Act, which Correa said aims to make it easier for lawmakers to get more information on the persistent threat of domestic terrorism by creating three new offices to monitor and prevent it. He also acknowledged the potential dangers of facial recognition, but said it’s a matter of balancing it with the potential benefits.

“Facial recognition is a sharp double-edged dagger,” Correa said. “If you use it correctly, it protects our liberties and protects our freedoms. If you mishandle it, then our privacy and our liberties that we’re trying to protect could be in jeopardy.”

Aside from facial recognition, activists are concerned about calls for civilians to scan social media as a means to feed tips to law enforcement.

“Untrained individuals sort of sleuthing around in the internet can end up doing more harm than good even with the best of intentions,” said Evan Greer, the director of digital rights and privacy group Fight for the Future. Greer cited the response to the Boston marathon bombing on Reddit, when a Find Boston Bombers subreddit wrongly named several individuals as suspects.

“You always have to ask yourself, how could this end up being used on you and your community,” she said.

Historically, attacks on American soil have sparked law enforcement and surveillance policies that research suggests have harmed minority communities. That’s a cause for concern for Muslim, Arab and Black communities following the Capitol riot.

After the Oklahoma City bombing, when anti-government extremists killed 168 people, the federal government quickly enacted the Antiterrorism and Effective Death Penalty Act of 1996, which, the Marshall Project wrote, “has disproportionately impacted Black and brown criminal defendants, as well as immigrants.”

Even hate crime laws have a disproportionate effect on Black communities, with Black people making up 24 percent of all accused of a hate crime in 2019 though they only make up 13 percent of the U.S. population according to Department of Justice statistics.

“Whenever they’ve enacted laws that address white violence, the blowback on Black people is far greater,” Margari Hill, the executive director of the Muslim Anti-Racism Collaborative, said at an inauguration panel hosted by Muslim political action committee Emgage.

In response to 9/11, federal and local governments implemented several blanket surveillance programs across the country — most notoriously in New York City — which the ACLU and other rights groups have long argued violated the privacy and civil rights of many Muslim and Arab Americans.

Many civil rights groups representing communities of color aren’t confident in the prospects of law enforcement using the same tools to root out right-wing extremism and, in some cases, white supremacy.

“[Law enforcement] knows that white supremacy is a real threat and the folks who are rising up in vigilante violence are the real threat,” Lau Barrios, a campaign manager at Muslim grass-roots organization MPower Change, said, referring to a Department of Homeland Security report that identified white supremacists as the most persistent and lethal threat facing the country in October 2020.

Instead, they focus their resources on movements like Black Lives Matter, she said. “That was what gave them more fear than white supremacist violence even though they’re not in any way comparable.”

These groups also say any calls for more surveillance are unfounded in reality. The Capitol riots were planned in the open, in easy-to-access and public forums across the internet and the Capitol police were warned ahead of time by the NYPD and the FBI, they argue. There’s no shortage of surveillance mechanisms already available to law enforcement, they say.

The surveillance apparatus in the U.S. is vast and entails hundreds of joint terrorism task forces, hundreds of police departments equipped with drones and even more that have partnered with Amazon’s Ring network, Renderos said.

“To be Black, to be Muslim, to be a woman, to be an immigrant in the United States is to be surveilled,” he said. “How much more surveillance will it take to make us safe? The short answer is, it won’t.”

©2021 Los Angeles Times. Visit at [latimes.com](https://www.latimes.com). Distributed by Tribune Content Agency, LLC.

Featured Resources

Presented by

[Tweets by IBM Security](#)

[Protecting the Enterprise: A Blueprint for Strengthening Cybersecurity in State and Local Government](#)

[Cybersecurity for State and Local Governments: Protecting Public Infrastructure](#)

[Creating the First-of-its-Kind Cyberthreat Sharing Group](#)

[2020 CODB Calculator/Digital Experience](#)

[IRIS Breach Breaker](#)

More From THE FUTURE OF Security



[Kansas Unemployment Hopes New System Will Stop Fraud](#)

The state has installed improved technology that it hopes will help stop thousands of fraudulent unemployment benefits claims from flooding the system. The new tech blocked 576,000 fraudulent login attempts in one day.

[GOV What's the Difference Between 'Smart City' and Surveillance?](#)

Speakers at the recent Micromobility World conference debated the future of smart city tech and whether it's actually been improving urban mobility, or simply facilitating a growth of the surveillance state.

[Washington Unemployment Hack Leaves Personal Data Vulnerable](#)

Already flooded with fraudulent claims, the state's unemployment agency now must mitigate a data breach that compromised social security numbers, employment data and bank account information for about 1.4 million people.

The Future of States & Localities

Where Government is Going – One Headline at a Time Delivered to your inbox everyday.

Sign Up Now

Special Projects

 [Salesforce Government of the Future](#)

 [Government 360](#)

 [IBM Put Smart to Work](#)

 [Funding IT: Strategies and Tactics to Take Advantage of CARES Act Funding](#)

 [Cisco Next Generation Government](#)

 [Google Future Ready](#)

 [Verizon Public Sector Ready](#)

 [Veritas Data Management](#)

Archived: Wednesday, April 7, 2021 12:50:54 PM
From: [Rachel Edelson](#)
Sent: Saturday, February 6, 2021 2:13:32 PM
To: ~House Executive Departments and Administration
Subject: Writing To Urge Passing of HB499
Importance: Normal

I am writing to urge the House to Pass HB 499.

HB499 would restrict the use of facial recognition technology by the state, preventing NH from becoming a surveillance state.

Facial recognition is invasive and unreliable. It is particularly unreliable in identifying people of color, women, elderly people, and young people.

There are multiple instances of this technology wrongly identifying someone, resulting in the police arresting an innocent Black man. [Read about one such incident here.](#)

If this technology improves and the government has a legitimate reason to use it in the future, the government can return to the legislature down the road and request specific and narrow permission to use it.

The alternative is to enable this invasive and unreliable technology to become widespread and then attempt to put the genie back into the bottle after the fact. We know from experience that reviving privacy rights after a technology is in use is particularly difficult. This bill is an opportunity to learn from history and ensure privacy rights are upheld from the onset.

Sincerely,
Rachel Edelson
Nashua NH

Sent from [Mail](#) for Windows 10

Archived: Wednesday, April 7, 2021 12:50:54 PM
From: [Barry Shanks](#)
Sent: Saturday, February 6, 2021 12:15:38 PM
To: [~House Executive Departments and Administration](#)
Subject: HB499
Importance: Normal

This bill ought to pass.

Both state and federal constitutions protect our right to privacy.

Facial recognition technology is used to violate our privacy.

Restrict its use in new Hampshire before more mistakes are made.

Barry Shanks

Archived: Wednesday, April 7, 2021 12:50:54 PM
From: diana@bolanderlaw.net
Sent: Monday, February 8, 2021 3:29:26 PM
To: ~House Executive Departments and Administration
Subject: HB 499
Importance: Normal

Dear Chairperson McGuire and Members of the Executive Departments and Administration Committee:

I am writing in support of HB 499 that limits the use of facial recognition. With the expansion of technology, we have seen a lessening of our right to privacy. I understand that if people put their photographs on line by selfies or videos, that may be public (unless limited to the private part of a social media website) and their choice. What I want to draw your attention to, and is of particular concern to me, is when the government requires citizens to provide the photograph.

I would request that you amend HB 499 so that all images/photographs taken for driver's licenses and NH identification cards now in the possession of the government of New Hampshire be destroyed. This is not difficult or time consuming. The images are on computer. They just need to be deleted. If it does take time, that is a small price to pay for taking the images for the purpose of facial recognition without the consent or knowledge of those citizens who merely thought they were getting a driver's license and nothing more. That is the issue here. No one having their photographs/images taken were informed that the photograph/image would be used for facial recognition and were not asked if he/she consented for it to be used for that purpose. When the personnel at the division of motor vehicles was asked whether the photograph/image was being used in connection with facial recognition, they denied that it was. It is that deception that requires a purging of the photographs/images.

The amendment should also require the division of motor vehicles to inform each person obtaining a driver's license or NH identification card that the photograph/image can be used for facial recognition only if they consent to that and the division must obtain a written consent before a photograph/image can be placed into a facial recognition data base or used for facial recognition. This written consent must be separate from any other document, in a large enough font to be read easily and in simple language so it is understood. If a person does not give consent, the photograph/image cannot be placed in the data base or used for facial recognition.

With this bill, you hold in your hands the ability to allow the right to privacy to continue to have meaning. It is a right I highly cherish. I hope you do as well.

I ask you to consider my request and thank you for your consideration.

Sincerely,
Diana G. Bolander

Diana G. Bolander, Esq.

Attorney at Law | Law Office of Diana G. Bolander, PC
PO Box 90, Wolfeboro, NH 03894
Tel: (603)569-2924
Fax: (603)569-9555
Email: diana@bolanderlaw.net
Web: www.bolanderlaw.net

Statement of Confidentiality: *This email and any attachments, is intended for use by the addressee and may contain legally privileged or confidential information. If you are not the intended recipient of this email, any*

dissemination, distribution or copying of this email, and any attachments, is prohibited. If you have received this email in error, please immediately notify me, and permanently delete the original and any copy of the email. Thank you.

Archived: Wednesday, April 7, 2021 12:50:54 PM
From: [Lisa Marchi](#)
Sent: Tuesday, February 9, 2021 3:11:19 PM
To: [~House Executive Departments and Administration](#)
Subject: HB499- ought to pass
Importance: Normal

Dear Committee Members,

HB499 would restrict the use of facial recognition technology by the state, preventing NH from becoming a surveillance state.

Facial recognition is invasive and unreliable. It is particularly unreliable in identifying people of color, women, elderly people, and young people. If this technology improves and the government has a legitimate reason to use it in the future, the government can return to the legislature down the road and request specific and narrow permission to use it. The alternative is to enable this invasive and unreliable technology to become widespread and then attempt to put the genie back into the bottle after the fact. We know from experience that reviving privacy rights after a technology is in use is particularly difficult. This bill is an opportunity to learn from history and ensure privacy rights are upheld from the onset. This is an opportunity to be proactive and not reactive.

Therefore I urge the committee to vote HB499 ought to pass.

Sincerely,

Lisa Marchi
Somersworth NH

Archived: Wednesday, April 7, 2021 12:50:54 PM


From: [Scherr, Albert](#)

Sent: Wednesday, February 10, 2021 8:01:11 PM

To: ~House Executive Departments and Administration

Subject: HB 499

Importance: Normal

Attachments: [Statement by Albert Scherr before the House ED & A Committee \(2-11-21\).docx](#) 

;

Committee Members

Attached is a copy of my testimony on HB 499. Please feel free to contact me if you have any questions about my testimony or HB 499.

Best,

Albert (Buzz) Scherr
Professor of Law
UNH School of Law
2 White Street
Concord, NH 03301
cell: 603-828-6515



Archived: Wednesday, April 7, 2021 12:50:55 PM
From: [Jeanne Hruska](#)
Sent: Thursday, February 11, 2021 7:48:45 AM
To: ~[House Executive Departments and Administration](#)
Subject: ACLU-NH testimony in support of HB499
Importance: Normal
Attachments:
ACLU-NH testimony on HB499 021121.pdf ;

Dear Representatives,

In anticipation of this morning's hearing on HB499, I'm submitting my written testimony. The ACLU-NH supports the concept of HB499 and urges the committee to amend the bill to provide more meaningful safeguards against the dangers of facial recognition technology, as this Committee did when it passed [HB1642](#) with a vote of 18-2 last session. This technology is invasive and inaccurate, and its growing use sends us down the road to being a surveillance state. Too often, we are playing catch up when it comes to privacy rights, trying to erect safeguards around a technology already in abundant use. Think of all the bills introduced to try to restrict the use and collection of GPS location data, which is ubiquitously used today. It's nearly impossible to put the genie back in the bottle. We are urging the NH Legislature to be proactive in establishing safeguards around a dangerous technology that is ripe for abuse.

Kindest regards,
Jeanne

Jeanne Hruska
Pronouns: she, hers

Political Director
American Civil Liberties Union of New Hampshire
18 Low Avenue, Concord, NH 03301
(c) 307-272-8727 | jeanne@aclu-nh.org
aclu-nh.org  



This message may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply email that this message has been inadvertently transmitted to you and delete this email from your system.

Archived: Wednesday, April 7, 2021 12:50:55 PM
From: HCS
Sent: Thursday, February 11, 2021 7:55:24 AM
To: ~House Executive Departments and Administration
Cc: Miriam Simmons
Subject: FW: Testimony on HB 499
Response requested: No
Importance: Normal

Testimony submitted HB 499

From: Marjorie Smith <msmithpen@aol.com>
Sent: Wednesday, February 10, 2021 6:26 PM
To: HCS <HCS@leg.state.nh.us>
Subject: Testimony on HB 499

Please forward this to House EDA Committee before Thursday's hearing. Thank you

TESTIMONY ON HB 499 PROHIBITING THE STATE FROM USING A FACIAL
RECOGNITION SYSTEM AS AMENDED BY 0247H
DELIVERED BY REPRESENTATIVE MARJORIE SMITH BEFORE THE HOUSE
EXECUTIVE DEPARTMENTS AND ADMINISTRATION COMMITTEE, FEBRUARY 11,
2021

Last term, this committee devoted significant time and effort to producing an amended bill addressing facial recognition. The bill passed the committee, the full house and was sent to the judiciary committee. I was chair of judiciary and I considered the judiciary committee's rejection of the bill to my most significant disappointment of my chairmanship.

In the time that has passed since then we have experienced the damage that can be done by the inappropriate application of facial recognition systems.

Understanding that careful application by trained professionals can make facial recognition systems a positive addition to law enforcement tools; we must also acknowledge that misuse can cause grave harm, with particular injustices felt by people of color and women.

The amendment that the chair and I have proposed attempts to minimize the harm and maximize the benefit by providing a uniform warrant requirement to use this technology. We take privacy seriously in New Hampshire. Face recognition technology is invasive and if not monitored will move us closer and closer to a surveillance state. Watching British detective stories while I wait for the end of my Covid-induced house arrest, I have been appalled by the reliance on surveillance – block by block, house by house. There is no privacy under such systems

This amendment makes the bill easier to understand and easier for the police to use. Warrants, as required in the amendment, are common law enforcement tools with well-established standards.

This amendment strikes a balance between the potential benefits of this technology and concerns about privacy rights and misuse

STATEMENT BY ALBERT SCHERR
PROFESSOR OF LAW, UNH FRANKLIN PIERCE SCHOOL OF LAW
HOUSE EXECUTIVE DEPARTMENTS & ADMINISTRATION COMMITTEE
HOUSE BILL 499
FEBRUARY 11, 2021

I have been on the faculty at UNH Law for over 25 years and, prior to that, I was a public defender in New Hampshire for 13 years. I teach, write and lecture about privacy issues in the criminal justice system. I have been involved in the criminal justice system in New Hampshire for almost 39 years and have worked closely and on a bipartisan basis with many legislators on criminal justice reform issues. In particular, I worked with then Representative Neal Kurk on what became Part I, Article 2b of the New Hampshire Constitution, NH's constitutional amendment on privacy. Recently, I chaired the Portsmouth Police Commission's sub-committee on bodycams, tasked with deciding whether the Portsmouth Police Department should adopt bodycams.

As always, I make this statement in my individual capacity, and the opinions I am expressing are solely mine and are not those of either UNH Franklin Pierce School of Law or of the University of New Hampshire. I appreciate the opportunity to provide this statement to this committee and ask you to amend HB 499 as written with the proposed amendment and *Ought to Pass* on the amended HB 499.

THE EVER-INCREASING WAVE OF 21ST CENTURY TECHNOLOGY I have been involved in the criminal justice system in New Hampshire long enough to have witnessed the transition from 20th century technology like fingerprints, pen registers, wiretaps and house searches to 21st century technology like surreptitious DNA harvesting, geolocation cellphone searches and Global Positioning System (GPS) surveillance. Facial surveillance systems are another, newer installment of 21st century technology that, like others, focuses much more on the acquisition of intangible information than physical objects.

Facial surveillance technology allows the government, if it so desires, to track your whereabouts in public; to capture a digital representation of your face; to store your digital face in a database with millions of others forever and to search it whenever they wish for whatever purpose they wish. Currently, it is estimated that 117 million American adults – approximately half of all American adults - are in a law enforcement face recognition network.

Effectively, this technology allows the police to replace live and photo-lineup eyewitness identification procedures that are well-regulated in terms of reliability, suggestiveness and other issues by tight constitutional due process and right to counsel concerns with an unregulated, freestyle artificial intelligence system driven by technician-generated algorithms.

The use of facial recognition technology implicates several concerns, constitutional as well as practical. In this statement, I intend to discuss the constitutional concerns and then to focus primarily on the paramount practical concern with facial recognition technology: its verified unreliability. In essence, putting aside the very real legal concerns, permitting this technology does not make practical sense.

CONSTITUTIONAL CONCERNS WITH FACIAL RECOGNITION TECHNOLOGY

Constitutionally, 20th century technology was regulated reasonably well by the U.S. Supreme Court's interpretation of the 4th Amendment and the NH Supreme Court's interpretation of Part I, Article 19 of the New Hampshire Constitution. Though both read like they protect our privacy in physical objects or locations, the courts have worked hard to adapt the language to circumstances where the invasion of privacy was not technically physical but rather a collection-of-non-tangible-information.

The 21st Century has brought vastly more sophisticated technologies to the table. Several of those technologies implicate privacy-in-public issues. Let me speak of one U.S. Supreme Court case that captures the problem that courts have been confronting with 21st century technology, particularly with acquiring personal information from someone in a public place. In *U.S. v. Jones*, the Washington D. C. police put a GPS tracking device on the bottom of Jones's SUV. They suspected him of being a drug dealer and wanted to track his whereabouts. They then tracked him for 10 days and acquired a wealth of information about his daily habits in public. The issue in the case was whether the police needed a search warrant to place the GPS on the SUV to gather the public-whereabouts information.

The U.S. Supreme Court said yes, the police needed a search warrant as Jones had a 4th Amendment reasonable expectation of privacy even in his public whereabouts as gathered by the police. This is a very important decision that explicitly protects a version of publicly-available personal information.

There is no question that if a police officer had simply tailed Jones in the old-fashioned way, no 4th Amendment privacy interest would have been implicated. But, a high-tech tailing that collected the same publicly-available information received 4th Amendment protection. Acquisition by the police of a digital representation of one's face and its placement in a massive database implicates the same 4th Amendment concerns. The use of such a digital representation to track someone's whereabouts similarly invokes the 4th Amendment.

What's even more concerning is that the use of any digital facial representation with the database is unreliable.

FACIAL SURVEILLANCE TECHNOLOGY & THE NOT-READY-FOR-PRIME-TIME PROBLEM

New Hampshire is not the first to contemplate banning this invasive technology. Nationally, several municipalities have already banned facial surveillance technology, including San Francisco & Oakland in California and Cambridge and Somerville in Massachusetts. Internationally, the European Union is seriously considering a five-year pause in the use of facial surveillance technology. My understanding is other municipalities and the State of New York are also considering bans.

The primary issue in these jurisdictions has been the unreliability of facial surveillance technology. A recent federal report from the National Institute of Standards & Technology (NIST) found that the technology was unreliable when used to identify people of color, women, the elderly and youth. What's more, its unreliability included both false positives and false negatives.

Specifically, it found that “false positives are higher in women than in men and are higher in the elderly and the young compared to middle-aged adults. Regarding race, we measured higher false positive rates in Asian and African American faces relative to those of Caucasians. There are also higher false positive rates in Native American, American Indian, Alaskan Indian and Pacific Islanders. These effects apply to most algorithms, including those developed in Europe and the United States.” Not infrequently, these false positive rates were of an order of magnitude or more greater. In one instance, it found that Asian and African American faces were sometimes misidentified 100 times more than their white counterparts.

Beyond such state and municipality regulatory efforts, businesses have assessed the reliability and usefulness of facial recognition technology. Axon Corporation is one of the leading providers of police-technology in the United States. For example, they provide bodycam technology to many police departments, including some in New Hampshire. As a part of their commitment to corporate responsibility, they have an Artificial Intelligence (AI) and Policing Technology Ethics Board.

The Board “operates independently from the company and is made up of experts in the fields of AI, computer science, privacy, law enforcement, civil liberties, and public policy. The Board advises Axon around ethical issues relating to the development and deployment of AI-powered policing technologies and works to ensure these technologies ultimately serve the communities where they will be used.”

Significantly, based on recommendations from this independent Board, Axon made the decision that it was not good business for them to make facial recognition technology a part of their bodycam packages they were selling to police departments. They said:

“Face recognition technology is not currently reliable enough to ethically justify its use on body-worn cameras. At the least, face recognition technology should not be deployed until the technology performs with far greater accuracy and performs equally well across races, ethnicities, genders, and other identity groups. Whether face recognition on body-worn cameras can ever be ethically justifiable is an issue the Board has begun to discuss, and will take up again if and when these prerequisites are met.”

<https://www.policingproject.org/axon-fr>

Appreciate carefully what Axon has decided. They make money off technology packages they sell to police departments. They would make more money off packages that include facial-recognition technology. Nonetheless, they have decided not to include that technology in the packages they sell ***because facial recognition technology is not currently reliable enough to ethically justify its use on body-worn cameras. Its use is not good business for them.***

CONCERNS WITH HB 499 AS WRITTEN

As currently written, HB 499 is legislation that is pro-facial recognition technology (FRT) surveillance. It allows its use for 72 hours without a warrant; without probable cause and without even reasonable suspicion. After 72 hours, it either allows its use with a “court

order” that, as written, requires neither probable cause nor that the police meet any other set of criteria for issuance.

It also creates exceptions that allow the police to surveil an individual or a group of individuals without even an ill-defined court order if they think – that is, they have “reasonable grounds” - that they’ll be able to get a court order after the fact. It also speaks of an officer being able to surveil someone with FRT as long as they have “exigent circumstances” but it leaves out the primary requirement of the use of the exigent-circumstances exception under the Fourth Amendment: the existence of probable cause to believe a crime has been committed and evidence of that crime will be found by use of FRT surveillance.


As currently written, HB 499 is a pro-FRT bill.

PROPOSED AMENDMENT TO HB 499

The proposed amendment to HB 499 simplifies and clarifies HB 499. IT says simply, to use FRT you must have a search warrant supported by probable cause and issued by a neutral and detached magistrate. It cures any constitutional problems with FRT surveillance as it does not have a 72-hour unrestrained-freedom-of-use provision; it does not have the expansive exceptions to the illusion of an FRT surveillance ban contained in HB 499 as written and it is abundantly clear that probable cause as determined by a neutral and detached magistrate is required.

CONCLUSION

New Hampshire needs to confront the constitutional privacy issues that face recognition and surveillance technology raises. Those constitutional concerns are adequately addressed by HB 499 with the proposed amendment. I ask you to amend HB 499 as written with the proposed amendment and *Ought to Pass* on the amended HB 499.

Archived: Wednesday, April 7, 2021 12:59:08 PM
From: [Miriam Simmons](#)
Sent: Monday, February 8, 2021 10:57:35 AM
To: ~House Executive Departments and Administration
Cc: [Pam Smarling](#); [Miriam Simmons](#)
Subject: Article : Facial Recognition Can Find Rioters, but May Harm Others
Response requested: No
Importance: Normal
Attachments:
[Article -Facial Recognition Can Find Rioters-.pdf](#) 

I am forwarding an Article that came in for the ED&A Committee.
.. saved in the attachment
..or in the URL link below (that was confirmed safe by our General Court IT dept).

Miriam

From: Carol McGuire <mcguire4house@gmail.com>
Sent: Monday, February 8, 2021 9:10 AM
To: [Miriam Simmons <miriam.simmons@leg.state.nh.us>](mailto:miriam.simmons@leg.state.nh.us)
Subject: Re: Facial Recognition Can Find Rioters, but May Harm Others

On Mon, Feb 8, 2021 at 8:47 AM Marjorie Smith <msmithpen@aol.com> wrote:

Please share this with your committee

thank you

<https://www.governing.com/security/Facial-Recognition-Can-Find-Rioters-but-May-Harm-Others.html>

Sent from [Mail](#) for Windows 10

Archived: Wednesday, April 7, 2021 12:59:08 PM
From: [Chrisinda Lynch](#)
Sent: Saturday, February 20, 2021 11:53:24 AM
To: [~House Executive Departments and Administration](#)
Subject: HB 499
Importance: Normal

Dear Representatives,

I urge you to vote OTPA on this bill. HB 499 offers privacy protection for NH citizens. The amendment added to this legislation is a good one that helps guard against abuses from the use of facial recognition technology.

Thank you for your consideration,
Chrisinda M. Lynch
Concord, NH

Archived: Wednesday, April 7, 2021 12:59:08 PM
From: [Mike Breen](#)
Sent: Monday, February 22, 2021 7:44:25 PM
To: [~House Executive Departments and Administration](#)
Subject: Why we can't have Critical Race Theory style racism in our schools.
Importance: Normal

MORE INFORMATION ABOUT THE CRITICAL RACE THEORY INSPIRED ENVIRONMENT OF RACISM, INTIMIDATION, AND STIGMATIZING OF STAFF AND STUDENTS AT SMITH

[US NEWS](#)

Smith College Staffer Quits Over Anti-White Racism

BY [PETR SVAB](#)

February 21, 2021 Updated: February 22, 2021

[bigger smaller](#)

[Print](#)

A staffer at Smith College has resigned, publishing a letter accusing the elite women's university of creating a "racially hostile environment" against white people. Jodi Shaw used to be a student support coordinator at the Massachusetts college but recently sent a resignation letter to its leadership saying the environment left her "physically and mentally debilitated." "I can no longer work in this environment, nor can I remain silent about a matter so central to basic human dignity and freedom," said the letter, [published](#) by columnist Bari Weiss. Smith College didn't immediately respond to a request for comment.

An alumna of the private liberal arts institution, Shaw said the culture had changed forcefully after a 2018 incident when a black student accused a white staffer of racism for calling campus security on her. An investigation showed no evidence of racial bias, but the college put in place a list of initiatives aimed at fighting "systemic racism" on campus. Yet the ideology driving the efforts seemed more concerned with inflaming anti-white sentiment rather than mitigating any form of racism, based on Shaw's account.

“I endured racially hostile comments, and was expected to participate in racially prejudicial behavior as a continued condition of my employment. I endured meetings in which another staff member violently banged his fist on the table, chanting ‘Rich, white women! Rich, white women!’ in reference to Smith alumnae. I listened to my supervisor openly name preferred racial quotas for job openings in our department. I was given supplemental literature in which the world’s population was reduced to two categories—‘dominant group members’ and ‘subordinated group members’—based solely on characteristics like race,” Shaw’s letter says. “Every day, I watch my colleagues manage student conflict through the lens of race, projecting rigid assumptions and stereotypes on students, thereby reducing them to the color of their skin. I am asked to do the same, as well as to support a curriculum for students that teaches them to project those same stereotypes and assumptions onto themselves and others. I believe such a curriculum is dehumanizing, prevents authentic connection, and undermines the moral agency of young people who are just beginning to find their way in the world.” She said other staffers she spoke to were “deeply troubled” by the developments but were “too terrified to speak out about it.”

In January 2020, Shaw said, she attended a mandatory staff retreat “focused on racial issues.” She said she wasn’t comfortable answering personal questions from the hired facilitator about race and “racial identity.” “Later, the facilitators told everyone present that a white person’s discomfort at discussing their race is a symptom of ‘white fragility.’ They said that the white person may seem like they are in distress but that it is actually a ‘power play,’” she wrote. “In other words, because I am white, my genuine discomfort was framed as an act of aggression. I was shamed and humiliated in front of all of my colleagues.”

I was shamed and humiliated in front of all of my colleagues.

— *JODI SHAW, Smith College student support coordinator*

She filed a workplace complaint, but felt it wasn’t taken seriously enough on account of her race. “I was told that the civil rights law protections were not created to help people like me,” she wrote. She was stripped of duties, which she suspected was a retaliation for her filing the complaint.

Quasi-Marxist Ideology She blamed the change in environment on [critical race theory](#), a quasi-Marxist ideology that reinterprets history as a struggle between whites and other races, labelling people as “oppressors” and “oppressed” on account of their skin color, echoing Marxism’s division of society based on class. “Under the guise of racial progress, Smith College has created a racially hostile environment in which individual acts of discrimination and hostility flourish. In this environment, people’s worth as human beings, and the degree to which they deserve to be treated

with dignity and respect, is determined by the color of their skin,” Shaw said. “It is an environment in which dissenting from the new critical race orthodoxy—or even failing to swear fealty to it like some kind of McCarthy-era loyalty oath—is grounds for public humiliation and professional retaliation.”

Critical race theory has been spreading through American institutions, starting at universities and seeping into K-12 education, government structures, the non-governmental sector, and the corporate world, commonly through supposedly “anti-racist” training sessions and internal social justice policies.

Former President Donald Trump dealt a significant blow to the ideology’s spread last year when he banned trainings based on the ideology from the federal government, and even federal contractors and some grantees. President Joe Biden, however, reversed the order shortly after taking office. Biden went as far as issuing an order that seems to [open the door](#) for instituting the ideology more widely [across the federal government](#). In Shaw’s view, the ideology exacerbates divisions among people. “It taps into humanity’s worst instincts to break down into warring factions, and I fear this is rapidly leading us to a very twisted place,” she said.

Michael D. Breen, MPA, Ph.D. 42 Marvin Road Moultonborough, NH 03254 Telephone:
603 253 9114



Statement by Jeanne Hruska, Political Director ACLU-NH
House Executive Departments and Administration Committee
House Bill 499
February 11, 2021

I submit this statement 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 over fifty years. **The ACLU-NH strongly supports enacting safeguards around the use of facial recognition technology and encourages this committee to amend HB499 to provide stronger privacy protections.** This technology is invasive, inaccurate, and sends us down the road of being a surveillance state. If the state is going to use this technology, there must be safeguards enacted to protect Granite Stater’s privacy.

HB499 needs substantial revisions as it is currently written.

Last year, this Committee passed HB1642, which would have banned the use of facial recognition technology by the state.¹ Unlike HB1642, HB499 endorses the use of facial recognition technology and would allow law enforcement to readily use facial recognition technology with next to no safeguards. For instance, as written, HB499 would allow law enforcement to freely use facial recognition technology for up to 72 hours without a warrant, even without reasonable suspicion. The dangers of this technology apply equally within its first 72 hours of usage as the hours afterwards. Applying safeguards only after the first 72 hours is to apply no safeguards.

This bill also does nothing to address concerns about the use of facial recognition technology to identify someone, as opposed to surveilling them. Passage of HB499, as written, risks giving legislators and the public a false sense of security, as this bill would do little to protect our privacy rights in practice. Rather than pass this minor band aid, we strongly urge the committee to provide stronger protections for Granite Staters against this technology, by at least imposing a warrant requirement for its usage.

What it means to be facially surveilled, all the time, everywhere you go.

Facial recognition technology turns your face into a digital identification card that you have to carry with you everywhere you go and display everywhere you go. Imagine, every time you go out in public, you have to wear a T-shirt with an enlarged picture of your driver’s license on it, with all the information displayed, and have a GPS chip implanted under your skin that only the government can track. This is not about your face being private. It is about the government using the data contained on your face to ID you, track you, and surveil you. You can never put your face away. You cannot not be surveilled – not even by wearing a mask, as new facial recognition technology can reportedly identify people using only eyes and eyebrows.²

Facial recognition technology is about more than just ID’ing you in public. It is about being able to identify where you go, when you go there, and everyone with whom you meet. Imagine a reporter meeting with a whistleblower? Imagine someone going to a clinic or to a therapist’s office? Imagine people meeting up to plan a protest? As technology becomes better and cheaper, facial recognition

¹ HB1642: gencourt.state.nh.us/bill_status/billText.aspx?sy=2020&id=1202&txtFormat=html

² New Facial Recognition Tech Only Needs Your Eyes and Eyebrows

<https://onezero.medium.com/new-facial-recognition-tech-only-needs-your-eyes-and-eyebrows-9e7dc155cd7f>

technology will become more prevalent. There does not have to be someone monitoring you. Computers will ID you, track you, store that data, and provide it on demand to the government.

False positives and demographic biases.

Making matters worse, this invasive technology is inaccurate and unreliable. It is particularly unreliable in identifying people of color, women, the elderly, and young people. In essence, it can reliably identify middle-aged, white men.³

The ACLU previously conducted a test using Amazon’s facial recognition tool, “Rekognition,” to identify members of the U.S. Congress. Rekognition incorrectly recognized 28 members of Congress as other people who had been arrested for a crime. The false matches were disproportionately of people of color, including six members of the Congressional Black Caucus.⁴

More recently, the National Institute of Standards and Technology, which develops standards for emerging tech, “found ‘empirical evidence’ that most of the facial-recognition algorithms exhibit ‘demographic differentials’ that can worsen their accuracy based on a person’s age, gender or race.”⁵

Inaccuracy here is not about the technology failing to identify you. It is about false positives - identifying you as the wrong person. False positives result in the police arresting and jailing the wrong person, as has happened multiple times across the country.⁶ This is not just traumatizing for those who are wrongly identified, it can result in law enforcement being misled and expending resources chasing incorrect leads. This is compounded by false negatives – when the technology fails to identify the correct person who is in the database. Put simply, facial recognition technology is invasive and unreliable. Granite Staters need safeguards against this technology.

Privacy rights given away during times of crisis are rarely restored.

History teaches us that government is most prone to power grabs and civil rights violations in times of crisis. History’s warning cry has particular resonance for privacy rights. We have spent twenty years working to reclaim the privacy rights that we lost to the Patriot Act in the wake of 9/11. The Patriot Act was intended to respond to the unique circumstances that followed the September 11th attacks. And yet, the U.S. Congress just reauthorized this surveillance scheme last year, twenty years after those attacks.

Other countries have significantly expanded their use of this technology in response to COVID-19, using it for contact tracing and to enforce compliance with quarantine orders. Privacy sacrificed in a time of crisis is hard to take back even after the crisis has abated. Instead, the loss of privacy becomes the “new norm,” with people having to adjust their expectations of privacy accordingly. This is why the ACLU-NH is committed to protecting Granite Staters’ privacy rights by supporting

³ [Study finds gender and skin-type bias in commercial artificial-intelligence systems | MIT News | Massachusetts Institute of Technology](#)

⁴ Nearly 40 percent of Rekognition’s false matches in the ACLU’s test were of people of color, even though they make up only 20 percent of Congress.

⁵ Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use. <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>

⁶ [Black man in New Jersey misidentified by facial recognition tech and falsely jailed, lawsuit claims \(nbcnews.com\)](#)

restrictions on the government's use of facial recognition technology, if not a complete ban, and working to ensure that surveillance does not become normalized.

Being proactive in protecting privacy, for once.

Rather than waiting for cameras to be erected everywhere, the ACLU-NH urges this committee to be proactive and protect privacy now. So often, when it comes to personal privacy, we are playing catch up. We are trying to prohibit or regulate something that is already in abundant use. Think of the number of bills pursued in recent sessions to regulate the use of GPS location data, which is ubiquitously used by the government and security companies alike. This reactionary strategy is challenging for everyone involved. Too often, it is impossible to put the genie back in the bottle. To avoid that, we support banning or severely restricting this invasive technology before it is commonplace, as it already is in select cities and countries.

Facial recognition technology is currently unregulated. There are no national standards for the underlying algorithms. There are no reporting standards for the frequency of errors. This means that there is a litany of different companies producing this technology with different capabilities, flaws, and potential for abuse. There are also no standards for notifying the public about its usage, meaning government agencies can use it without the public's knowledge.

In New Hampshire, there is no existing mechanism to inform the public of the day that our government opts to use facial recognition technology. If there were a structure whereby the public weighed in on any new technology adopted by police, that would be one thing. But, there isn't. Police departments can receive technology from in-kind donations from private companies, in which case there would be no budget trail or public oversight. Companies routinely give technology to law enforcement agencies for free and then charge the departments for data usage and storage. In these cases, the only budget item that the public would see would be data storage and usage.

If we wait for facial recognition technology to be in abundant use by state agencies, it will be too late to walk it back or restrict its application.

Continuing New Hampshire's legacy of protecting personal privacy.

This bill builds off the 2018 constitutional amendment that received support from more than 81 percent of Granite State voters and enshrined in our state constitution a short, but powerful, right:

An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent.

Facial surveillance is the definition of governmental intrusion into our personal information.

The budding trend to ban this invasive and unreliable technology.

Facial surveillance technology has already been banned in San Francisco, Oakland, Portland, Maine, and several towns in Massachusetts, including Boston. The Massachusetts legislature actually passed a bill last year that would ban this technology statewide. California has banned the software's use in police body cameras. The European Union is considering banning the technology.⁷ This is a small list, but we fully expect it will grow. There is a growing effort to ban

⁷ <https://www.bbc.com/news/technology-51148501>

this technology in New York City, but there we see the challenges of banning a technology already in widespread use.⁸

Even Amazon has acknowledged the dangers of its facial recognition technology by police. Last June, Amazon voluntarily imposed a one-year moratorium on the use of its facial recognition tech by law enforcement.⁹ While one year is better than none, it is not enough. And we should not rely on private companies to protect consumer privacy over the long term. We need our state to protect the public from this technology.

The cost of doing nothing because of the exception.

Concerns about facial recognition technology are countered often by pointing to how it was used in the Boston bomber crisis. However, in the Boston Bomber scenario, the technology used did not identify the suspects until after they were identified already by other means. It merely confirmed what the police already knew. This was despite the system having an array of pictures of the suspects with which to work. Contemplate what might have happened if the technology had produced false positives and identified other people as the suspects.

There will inevitably be scenarios where this technology works and helps. It might even help with contact tracing in certain scenarios. The question, however, is whether the adverse effects justify the lottery ticket odds of it actually working in a significant way. After the Boston bombing, law enforcement could have arrested every single person in the vicinity to ensure that they captured the suspect, but at what cost? Do we want to permanently undermine the privacy of every single person in the Granite State because theoretically there might one day be a scenario where the technology can help?

As a state, we should not allow our communities to be the guinea pigs of this technology. If this technology becomes refined, accurate, and reliable, this legislature can consider permitting broad use of this technology down the road. Too often, we are playing catch up when it comes to privacy. We are urging this legislature to play offense.

For these reasons, the ACLU-NH urges the members of this committee to strengthen and pass HB499.

⁸ [Critics Of Facial Recognition Technology Target NYC And The State With 'Ban The Scan' Campaign \(msn.com\)](#)

⁹ [Amazon bans police use of facial recognition technology for one year \(cnbc.com\)](#)

In the Year of Our Lord Two Thousand Twenty

AN ACT prohibiting the state or a state official from using a face recognition system.

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

1 1 New Subdivision; Breaches of the Peace; Face Recognition Technology Prohibited. Amend
2 RSA 644 by inserting after section 22 the following new subdivision:

3 Face Recognition Technology Prohibited

4 644:23 Definitions. In this subdivision:

5 I. "Face recognition technology" means an automated or semi-automated process that assists
6 in identifying or tracking an individual or capturing information about an individual, based on the
7 physical
8 characteristics of an individual's face. It does not include the process by which an individual visually
9 identifies another individual by viewing a representation of the individual on a computer, video
10 recording, photograph or other media.

11 II. "State" means any department, agency, bureau, or administrative unit of the state of
12 New Hampshire, including any city, town, county, school district, or municipal entity therein.

13 644:24 Face Recognition Technology Prohibited.

14 The State shall only use a face recognition technology if it has a search warrant supported by
15 probable cause and signed by a neutral and detached magistrate ***subject to the exigent***

16 ***circumstances exception to the warrant requirement under Part I, Article 19 of the
New Hampshire Constitution or the Fourth Amendment of the United States Constitution.***

17 644:25 Evidence Inadmissible.

18 I. Any data or information collected or derived from the State's own use of face recognition
19 technology in violation of this subdivision shall be inadmissible in any trial, hearing, or
20 other proceeding in or before any court or regulatory agency in the state of New Hampshire.

21 II. Any evidence derived from data or information collected from any use of face recognition
22 technology in violation of this subdivision shall be inadmissible in any trial, hearing, or
23 other proceeding in or before any court or regulatory agency in the state of New
24 Hampshire, unless sufficiently attenuated from the original violation, including but not limited,
25 to an affirmative showing that no state official had requested, facilitated or otherwise caused
26 the use of face recognition technology by an entity other than the State as defined above.

1 Drivers' Licenses; Use of Facial Recognition Technology Prohibited. Amend RSA
263:40-b to read as follows:

2 263:40-b Use of Face Recognition Technology Prohibited. The department shall not allow
3 access to any of its digital representations of faces by any face recognition technology nor
4 shall the department use face recognition technology. No state agency, other than the
5 department, shall create or maintain a searchable database of face images.

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

Bill as
Introduced

HB 499 - AS INTRODUCED

2021 SESSION

21-0023

04/11

HOUSE BILL **499**

AN ACT prohibiting the state from using a face recognition system.

SPONSORS: Rep. McGuire, Merr. 29; Rep. M. Smith, Straf. 6; Rep. Berch, Ches. 1; Rep. Hopper, Hills. 2; Rep. T. Lekas, Hills. 37; Rep. Merchant, Sull. 4; Sen. Reagan, Dist 17

COMMITTEE: Executive Departments and Administration

ANALYSIS

This bill prohibits the state from using face recognition technology.

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.

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Twenty One

AN ACT prohibiting the state from using a face recognition system.

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

1 1 New Subdivision; Breaches of the Peace; Face Recognition Technology Prohibited. Amend
2 RSA 644 by inserting after section 22 the following new subdivision:

3 Face Recognition Technology Prohibited

4 644:23 Definitions. In this subdivision:

5 I. "Face recognition technology" means an automated or semi-automated process that assists
6 in identifying an individual or capturing information about an individual, based on the physical
7 characteristics of an individual's face. It shall not include the process by which an individual
8 visually identifies another individual by viewing a representation of the individual on a computer,
9 video recording, photograph, or other media.

10 II. "Ongoing surveillance" means the utilization of facial recognition technology to engage in
11 a sustained effort to track the physical movements of an identified individual through one or more
12 public places where such movements occur over a period of time greater than 72 hours, whether in
13 real time or through application of such technology to historical records. Ongoing surveillance shall
14 not include instances where facial recognition technology is utilized for a single identification or
15 attempted identification of an individual, if no subsequent attempt is made to track that individual's
16 movement in real time or through the use of historical records after the individual has been
17 identified.

18 III. "State" means any department, agency, bureau, or administrative unit of the state of
19 New Hampshire, including any city, town, county, school district, or municipal entity therein.

20 644:24 Face Recognition Technology Prohibited.

21 I. No officer or employee of a state agency shall use facial recognition technology to engage
22 in ongoing surveillance of an individual or group of individuals in a public space, unless:

23 (a) The use of the facial recognition technology is in support of a law enforcement
24 activity; and

25 (b)(1) A court order has been obtained to allow the use of facial recognition technology
26 for ongoing surveillance of the individual or group of individuals; or

27 (2) An investigative or law enforcement officer:

28 (A) Reasonably determines that exigent circumstances and compelling law
29 enforcement needs make it impractical to obtain a court order;

30 (B) Reasonably determines that there are grounds for which a court order could
31 be obtained under subparagraph (A); and

1 (C) Causes an application for a court order to be made in accordance with
2 subparagraph (A) not later than 48 hours after the use of facial recognition technology to engage in
3 ongoing surveillance.

4 644:25 Evidence Inadmissible.

5 I. Any data or information collected or derived from the state's own use of face recognition
6 technology in violation of this subdivision shall be inadmissible in any trial, hearing, or other
7 proceeding in or before any court or regulatory agency in the state of New Hampshire.

8 II.(a) An aggrieved individual who has been the subject of ongoing surveillance using facial
9 recognition technology, in any trial, hearing, or proceeding in or before any court, department,
10 officer, agency, regulatory body, or other authority of the state of New Hampshire or a political
11 subdivision thereof, may move to suppress information directly obtained through the use of facial
12 recognition technology, or evidence derived therefrom, in violation of this section, on the grounds
13 that:

14 (1) The information was unlawfully obtained;

15 (2) The order of authorization or approval under which the information was obtained
16 is insufficient on its face; or

17 (3) The use of facial recognition technology was not used in conformity with the
18 order of authorization or approval.

19 (b) Evidence obtained through the use of facial recognition technology that would
20 otherwise violate this section shall not be suppressed if the evidence was acquired by an officer or an
21 employee of an agency with an objectively reasonable belief that the use of facial recognition
22 technology was in compliance with this section.

23 2 Drivers' Licenses; Use of Face Recognition Technology Prohibited. RSA 263:40-b is repealed
24 and reenacted to read as follows:

25 263:40-b Use of Face Recognition Technology Prohibited. The department shall not allow access
26 to any of its digital representations of faces by any face recognition technology nor shall the
27 department use face recognition technology. No state agency, other than the department, shall
28 create or maintain a searchable database of face images.

29 3 Effective Date. This act shall take effect 60 days after its passage.