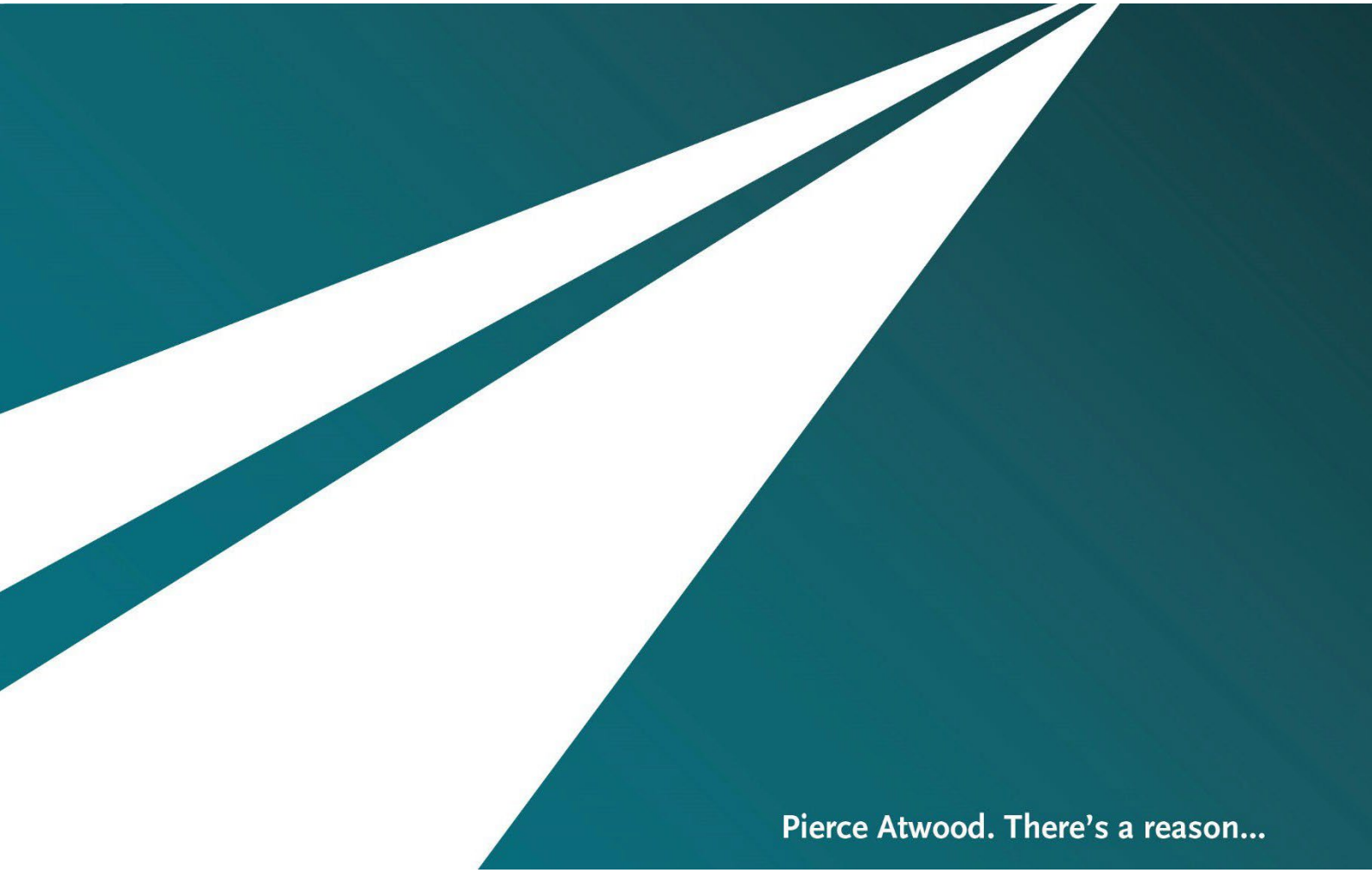
PIERCE ATWOOD LLP

New Hampshire: Cookies & Similar Technologies

Updated October 2025



PIERCEATWOOD.COM

New Hampshire: Cookies & Similar Technologies

1. GOVERNING TEXTS

1.1 Legislation

In New Hampshire, the relevant laws are the Act relative to the expectation of privacy (the Act) and the Regulation of Business Practices for Consumer Protection under Chapter 358-A of Title XXXI – Trade of Commerce of the New Hampshire Revised Statutes (New Hampshire Consumer Protection Act) (NHCPA).

The Act

The Act is a comprehensive consumer privacy law that has implications for cookies and similar tracking technologies, although it does not specifically address the topic of cookies directly. Subject to certain exceptions that are common among state consumer privacy laws, the Act applies to persons who conduct business in New Hampshire or who produce products or services that are targeted to residents of New Hampshire and who satisfy one of the following thresholds during a one year period (§507-H:2):

- control or process the personal data of not less than 35,000 unique New Hampshire consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- control or process the personal data of not less than 10,000 unique New Hampshire consumers and derive more than 25% of gross revenue from the sale of personal data.

Similar to other comprehensive consumer privacy laws, the Act includes a variety of requirements that indirectly apply to cookies and similar tracking technologies used to process personal data for purposes of 'targeted advertising.'

NHCPA

The NHCPA is a general consumer protection law similar to the Federal Trade Commission Act of 1914 (the FTC Act). However, the NHCPA is fairly unique in that it allows for statutory damages, nonetheless, statutory damages only apply to private actions and thus may not extend to violations of the Act which, as discussed below in the section on Penalties, are subject to exclusive enforcement by the New Hampshire Attorney General (AG).

1.2. Regulatory Authority Guidance

Not applicable. The Act does not grant a state agency rulemaking authority, although it does authorize the New Hampshire Secretary of State to establish forms and processes for certain requirements under the Act. Specifically, the Secretary of State is responsible for:

- developing a secure and reliable means by which consumers may exercise their rights; and

- establishing standards for privacy notices, including references to the means by which consumers may exercise their rights.

  No information is available yet from the Secretary of State.

2. DEFINITIONS

Cookies & similar technologies: There is no definition of 'cookies' in New Hampshire law. The relevant definition in the Act is that of 'targeted advertising,' which may apply to a range of tracking technologies when used to facilitate targeted advertising, including:

- Cookies: A data file placed on a device when it is used to visit a website.
- Web beacons: Small graphic images or other web programming code inserted into a website or email, alternatively known as web bugs, clear GIFs, or pixel tags, that are often used to track user behavior, such as clicks on links or email opens.
- Tracking scripts: Small bits of code embedded within web pages that track user behavior and share the resulting data with the website owner or with a third-party for analysis.
- Browser fingerprinting: A combination of user-specific browser information (such as precise browser and OS version, time zone, installed apps, precise hardware details, etc.) that may identify a unique individual.
- Entity tag (ETag): A part of the HTTP protocol usually used to confirm that client-side content matches server-side content; however, ETags may be used to identify a return user even in scenarios where cookies are cleared.
- Session replay: A technology that reconstructs all of the events undertaken by a user on a website, producing a video of the user's experience.

Consent: Under the Act, 'consent' means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer (§507-H:1(VII)). It may include:

- a written statement, including by electronic means; or
- any other unambiguous affirmative action.

Consent does not include:

- the acceptance of a general or broad terms of use or similar document;
- hovering over, muting, pausing, or closing a given piece of content; or
- an agreement obtained through the use of dark patterns.

Dark pattern: Under the Act, 'dark pattern' or 'deceptive design pattern' means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission (FTC) refers to as a 'dark pattern' (§507-H:1(XII)).

Personal data: Under the Act, 'personal data' means any information that is linked or reasonably linkable to an identified or identifiable individual. It does not include de-identified data or publicly available information (§507-H:1(XIX)).

Data processing: Under the Act, 'process' or 'processing' means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data (§507-H:1(XXI)).

Online identifiers: Not applicable.

Sale of personal data: Under the Act, 'sale of personal data' means the exchange of personal data for monetary or other valuable consideration by the controller to a third party (§507-H:1(XXVII)). 'Sale of personal data' excludes, among other things:

- the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; and
- the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party.

Sensitive data: Under the Act, 'sensitive data' means personal data that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying an individual; personal data collected from a known child; or precise geolocation data (§507-H:1(XXVIII)).

Targeted advertising: Under the Act, 'targeted advertising' means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet websites or online applications to predict such consumer's preferences or interests (§507-H:1(XXIX)). It does not include:

- advertisements based on activities within a controller's own internet websites or online applications;
- advertisements based on the context of a consumer's current search query, visit to an internet website, or online application;
- advertisements directed to a consumer in response to the consumer's request for information or feedback; or
- processing personal data solely to measure or report advertising frequency, performance, or reach.

3. CONSENT MANAGEMENT

3.1. Is consent required?

Under the Act, consent is required for the processing of:

- personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes (§507-H:6(I)(b));
- sensitive data (§507-H:6(I)(d)); and
- personal data for purposes of targeted advertising or sale where the controller has actual knowledge, and willfully disregards, that the consumer is at least 13 years of age but younger than 16 years of age (§507-H:6(I)(g)).

Note that consumers have the right to opt out of processing in certain scenarios where consent is not required, including (§507-H:4 (I)(e)):

- the processing of personal data for purposes of targeted advertising;
- the sale of personal data; or
- profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Recent court rulings in jurisdictions with similar laws indicate that cookies may process sensitive data in some scenarios. The Act does not explicitly address this issue. To the extent the data being collected by cookies is 'sensitive data,' the use of cookies requires consent under the Act.

3.2. Conditions for valid consent

As indicated above in the section of definitions, under the Act, 'consent' means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement.

Where a controller or processor complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act of 1998 (COPPA), they are also compliant with any requirement to obtain parental consent under Act.

3.3. Analytics and audience measurement cookies

There are no specific requirements regarding consent for analytics and audience measurement cookies. The definition of 'targeted advertising' under the Act, as provided above in the section on definitions, excludes processing personal data solely to measure or report advertising frequency, performance, or reach. However, the Act uses a broad definition of sale, as provided above in the section of definitions. Other jurisdictions have interpreted the term sale, where broadly defined, to include the use of third-party analytics and audience measurement cookies in certain circumstances (e.g., where the third-party provider is not contractually prohibited from processing the personal data for its own purposes).

3.4. Exemptions

The Act lists a range of exemptions to the requirements under the law, including in order to comply with regulations, investigations, or subpoenas, to provide a product or service specifically requested by a consumer, to take steps at the request of a consumer prior to

entering into a contract, to engage in research or public health, and for internal purposes, among other exemptions (§507-H:10(I)).

3.5. Cookie information requirements

Under the Act, a controller must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that meets the standards established by the Secretary of State and that includes (§507-H:6(III)):

- the categories of personal data processed by the controller;
- the purposes for processing personal data;
- how consumers may exercise their consumer rights (e.g., the right to opt out of processing for purposes of targeted advertising), including how a consumer may appeal a controller's decision with regard to the consumer's request;
- the categories of personal data that the controller shares with third parties, if any;
- the categories of third parties, if any, with which the controller shares personal data; and
- an active email address or other online mechanism that the consumer may use to contact the controller.

Additionally, the Act requires controllers to clearly and conspicuously disclose any sales of personal data to third parties or processing of personal data for targeted advertising, as well as the manner in which a consumer may exercise the right to opt out of such sale or processing (§507-H:6(IV)).

Finally, businesses should be aware of the potential applicability of the NHCPA and should not mislead consumers as to their practices related to cookies, including in representations made within their privacy notices or terms of use.

With respect to the right to opt out of targeted advertising or the sale of personal data, the Act requires controllers to provide a clear and conspicuous link on the controller's website to a webpage that enables a consumer, or a consumer's agent, to exercise such right (§507-H:6(V)(a)(1)(A)). Further, controllers must allow consumers to opt-out through a browser opt-out preference signal no later than January 1, 2025 (§507-H:6(V)(a)(1)(B)).

3.6. Cookie consent mechanism

The Act does not contain specific content, design, or configuration requirements for cookie consent mechanisms. As indicated above in the section on definitions, consent may include (§507-H:6(III)):

- a written statement, including by electronic means; or
- any other unambiguous affirmative action.

However, consent does not include:

- the acceptance of a general or broad terms or use or similar document;
- hovering over, muting, pausing, or closing a given piece of content; or
- an agreement obtained through the use of dark patterns.

The Act requires businesses to honor an opt-out preference signal when such signal conflicts with a consumer's existing controller-specific privacy setting, however, the business may notify the consumer of the conflict and provide the consumer with the choice to confirm the existing setting (§507-H:6(V)(a)(1)(B)).

3.7. Cookie walls

The Act does not restrict cookie walls, as long as they meet the consent requirements as described above (in scenarios where consent is required).

3.8. Consent duration

Under the Act, consent persists until revoked.

4. COOKIES & THIRD PARTIES

4.1. Conditions for placement of third-party cookies

The Act does not specify requirements for third-party cookies. However, any sharing of personal data with third parties must be disclosed in the controller's reasonably accessible, clear, and meaningful privacy notice. Moreover, sales of personal data to third parties and the processing of personal data for targeted advertising, as well as the manner in which a consumer may opt out of such sales and processing, must be clearly and conspicuously disclosed (§507-H:6(III)).

Prior to engaging in a processing activity that presents a heightened risk of harm to a consumer, the Act requires controllers to conduct and document a data protection assessment (§507-H:8(I)). The Act specifically requires a data protection assessment for the processing of personal data for the purposes of targeted advertising, the sale of personal data, and the processing of sensitive data (§507-H:8(I)). The placement of third-party cookies may qualify as one or more of these activities and thus require a data protection assessment.

Note that as indicated above in the section on definitions, the definition of 'sale of personal data' excludes, among other things (§507-H:1(XXVII)):

- the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; and
- the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party.

4.2. Roles and responsibilities

As discussed above in the section on the conditions for placement of third-party cookies, the controller is responsible for providing a reasonably accessible, clear, and meaningful privacy notice that discloses the controller's sharing of personal data with third parties, including the categories of personal data shared and the categories of third parties with which personal data is shared (§507-H:6(III)).

Under the Act, a controller is not liable for a third party's violation of the Act as long as the controller does not have actual knowledge that the violations would occur. Similarly,

a third party is not liable for a controller's violation of the law as long as their receipt of personal data from the controller complied with the law (§507:H-10(IV)).

4.3. International data transfers

The Act does not restrict or impose specific requirements on international data transfers.

5. COOKIE RETENTION

The retention of personal data collected through the use of cookies or similar technologies is governed by the general requirement under the Act that the processing of personal data be adequate, relevant, and limited to what is necessary in relation to the purposes provided in the privacy notice or as otherwise allowed under New Hampshire law (§507-H:10(VI)).

Where cookie or similar data is retained, the Act requires such data to be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to customers relating to such retention (§507-H:6(I)(c)).

6. ADDITIONAL INFORMATION

No further information.

7. CASE LAW & ENFORCEMENT DECISIONS

Not applicable.

8. PENALTIES

The Act

The Act grants the AG the exclusive authority to enforce its provisions (§507-H:11(I)). There is no private right of action for violations of the Act (§507-H:11(IV)).

The AG formed a new Data Privacy Unit that will be primarily responsible for enforcing the Act.

Between January 1, 2025, and December 31, 2025, the AG shall provide controllers with a 60-day cure period after issuing a notice of violation. After December 31, 2025, such a cure period is not required and is up to the AG's discretion (§507-H:11(II)). When

determining whether to grant a cure period after December 31, 2025, the AG may consider (§507-H:11(III)):

- the number of violations;
- the size and complexity of the controller or processor;
- the nature and extent of the controller's or processor's processing activities;
- the substantial likelihood of injury to the public;
- the safety of persons or property; and
- whether such alleged violation was likely caused by human or technical error.

A violation of the Act shall constitute an unfair method of competition or any unfair or deceptive act or practice in violation of §358-A:2 of the NHCPA (§507-H:11(V) of the Act).

NHCPA

A violation of Section 358-A:2 of the NHCPA is a misdemeanor for a natural person and a felony for any other person. Additionally, the court may award to the state all legal costs and expenses.