Employee Privacy Laws: New Jersey
State Q&A
Theresa A. Kelly and Heather Weine Brochin, Day Pitney LLP, with Practical Law Labor & Employment
Yes - TOC required

Review Completed on June 12, 2019

This resource was reviewed on June 12, 2019 to ensure that it reflects the most current law and market practice. There were no substantive changes made to the document.

Abstract:

A Q&A guide to employee privacy laws for private employers in New Jersey. This Q&A addresses employee privacy rights and the consequences for employers that violate these rights. Federal, local, or municipal law may impose additional or different requirements.

Overview of State Privacy Law

1. Please list each state law relating to employee privacy (for example, employee right to privacy, access to personnel files, electronic communications, surveillance and monitoring, medical examinations, and lawful off-duty activity laws), EXCEPT state laws on background checks and drug testing. For each, please describe:
    - What activity the law protects.
    - Which employers are covered.
    - Which employees are covered, including any exceptions for interns, independent contractors, minors or others.
    - Whether the law protects employees from their co-workers' actions in addition to their supervisor's actions.
    - Whether it provides for a private right of action.
    - For statutes and regulations, the entity that administers the statute or regulation(s).

New Jersey Wiretapping and Electronic Surveillance Control Act: N.J.S.A. 2A:156A-1 to 2A:156A-37

Protected Activity

The New Jersey Wiretapping and Electric Surveillance Control Act (Wiretap Act) prohibits any person from purposefully:

- Intercepting, trying to intercept, or having another person intercept any wire, electronic or oral communication.
- Knowing the information was obtained through a wire, electronic, or oral communication interception, either:
  - disclosing or attempting to disclose the contents or any evidence from the communication; or
  - using or attempting to use the contents or any evidence from the communication.

(N.J.S.A. 2A:156A-3.)

Covered Employers

The Wiretap Act covers all persons, including private employers. However, the following exceptions apply to most New Jersey employers:

- It is lawful for a switchboard operator or an officer, agent, or employee of a wire or electronic communication service provider to intercept a communication if the interception is either:
  - during the normal course of employment and part of the employee's duties; or
  - to protect the employer's rights or property.

  (N.J.S.A. 2A:156A-4(a).)
- One of the parties to the communication has given prior consent to the interception (N.J.S.A. 2A:156A-4(d).)

In addition, the law exempts devices given to employees by their employers and which are used in the normal course of business from the definition of "electronic, mechanical or other devices" (N.J.S.A. 2A:156A-2(d)(1)). The statute does not clarify what "subscribers" means, but it is generally understood that the Wiretap Act excludes devices used by employees in the course of their business.

Covered Employees

The Wiretap Act covers all persons, including employees.

Co-Worker Violations

The Wiretap Act prohibits interception of wire, electronic, or oral communications by co-workers.

Private Right of Action

The law provides for a private right of action. Any person whose communication is intercepted, disclosed or used in violation of the Wiretap Act may recover:

- **Actual damages**, but not less than liquidated damages computed at a rate of $100 per day of violation or $1,000, whichever is higher.
- **Punitive damages**.
- Attorneys' fees.
- Reasonably incurred litigation costs.

(N.J.S.A. 2A:156A-24.)

Administration

The Wiretap Act does not specify an administering agency.

The New Jersey Social Media Act: N.J.S.A. 34:6B-5 to 34:6B-10

Protected Activity

The Social Media Act prohibits employers from requiring or requesting that current or prospective employees provide for personal social media accounts:

- A user name or password.
- Any other means of access.

(N.J.S.A. 34:6B-6.)

Employers are also prohibited from:

- Requiring individuals to waive their rights under this statute as a condition of either applying for employment or receiving a job offer. An agreement to waive any right or protection under the Social Media Act is unenforceable. (N.J.S.A. 34:6B-7.)
- Retaliating or discriminating against individuals who exercise their rights under the Social Media Act (N.J.S.A. 34:6B-8).

The Social Media Act does **not:**

- Prohibit employers from accessing or using information about a current or prospective employee obtained in the public domain (N.J.S.A. 34:6B-10(d)).
- Apply to social media accounts created, maintained, used, or accessed by a current or prospective employee for purposes related to the employer's business (N.J.S.A. 34:6B-5).
- Prohibit employers who have received specific information about the employee's actions from accessing information to investigate:
  - a violation of law;
  - employee misconduct; or
  - the improper transfer of confidential information or financial data.

  (N.J.S.A. 34:6B-10(c).)

Covered Employers

The law covers all New Jersey employers except:

- The Department of Corrections.
- The State Parole Board.
- County corrections departments.
- Any state or local law enforcement agency.

(N.J.S.A. 34:6B-5.)

Covered Employees

The law covers all current and prospective employees of covered employers (N.J.S.A. 34:6B-5).

Co-Worker Violations

The Social Media Act does not address violations by co-workers.

Private Right of Action

The law does not provide a private right of action.

Administration

The New Jersey Department of Labor and Workforce Development (NJDLWD) administers this law.

Genetic Privacy Act: N.J.S.A. 10:5-43 to 10:5-49

Protected Activity

Under New Jersey's Genetic Privacy Act, a person must receive informed consent before obtaining or retaining genetic information from any individual **except**:

- By state, county, or federal law enforcement agencies during a criminal investigation or prosecution.
- To determine paternity.
- To determine a deceased person's identity.
- For anonymous research where the subject's identity is not released.
- For newborn screening requirements as required by state and federal law.
- As authorized by federal law for identification purposes.

(N.J.S.A. 10:5-45 and 10:5-46.)

In addition, a person may not disclose or be compelled to disclose, by subpoena or any other means:

- The identity of the individual receiving genetic tests.
- Genetic information about the individual that permits identification of the individual, except in certain circumstances.

(N.J.S.A. 10:5-47.)

Covered Employers

The law covers all employers.

Covered Employees

The law covers all employees.

Co-Worker Violations

The statute does not differentiate between employers and co-workers.

Private Right of Action

Anyone disclosing an individual's genetic information is liable to that individual for all actual damages proximately caused by the disclosure, including:

- Economic damages.
- Bodily damages.
- Emotional harm.

(N.J.S.A. 10:5-49(c).)

Administration

The New Jersey Commissioner of Health and Senior Services administers this law in consultation with the New Jersey Commissioner of Banking and Insurance (N.J.S.A. 10:5-45).

Driving Records: N.J.S.A. 39:2-3.3 to 39:2-3.7

Protected Activity

The New Jersey Motor Vehicle Commission (NJMVC) cannot knowingly disclose or make available to any person personal information about any individual the NJMVC obtains in connection with a motor vehicle record (N.J.S.A. 39:2-3.4(a)).

"Personal information" includes any information identifying an individual, including:

- A photograph.
- A social security number.
- A driver identification number.
- A name.

- An address other than the five-digit zip code.
- A telephone number.
- Medical or disability information.

"Personal information" does **not** include the following information:

- Vehicular accidents.
- Driving violations.
- Driver's status.

(N.J.S.A. 39:2-3.3.)

The NJMVC may disclose personal information for use in the normal course of business to either:

- Check the accuracy of personal information submitted by an individual to the business.
- Obtain correct information if the information submitted by the individual is not correct, but only to prevent fraud by, pursue legal remedies against, or recover on a debt or security interest against the individual.

(N.J.S.A. 39:2-3.4(c)(3).)

The statute also allows:

- Employers to obtain personal information to verify whether an individual holds a commercial driver's license required by the Commercial Motor Vehicle Safety Act (N.J.S.A. 39:2-3.4(c)(8)).
- The disclosure of personal information to any requestor with the individual's notarized written consent (N.J.S.A. 39:2-3.4(c)(10)).

Covered Employers

The law covers all private employers.

Covered Employees

The law covers all employees.

Co-Worker Violations

The statute does not specifically address co-worker violations.

Private Right of Action

The statute provides for a private right of action and remedies including:

- Actual damages, which cannot be less than the liquidated damages amount of $2,500.

- Punitive damages.
- Equitable relief.
- Reasonable attorneys' fees and costs.

(N.J.S.A. 39:2-3.6.)

Administration

The NJMVC administers the law.

Freedom from Intimidation Law: N.J.S.A. 34:19-9 to 34:19-14

Protected Activity

Employers may not require their employees to either attend an employer-sponsored meeting or participate in any communications with the employer or its agents regarding the employer's opinion about:

- Religious matters.
- Political matters.

(N.J.S.A. 34:19-10.)

Employer may permit employees to voluntarily attend an employer-sponsored meeting or provide other communications if the employer informs employees that they may, without penalty, refuse to either:

- Attend the meetings.
- Accept the communications.

(N.J.S.A. 34:19-10.)

Employers may communicate information about religious or political matters to their employees that they are required by law to communicate, but only to the extent required by law (N.J.S.A. 34:19-11(a)).

Employers may not discharge, discipline, or otherwise penalize or threaten an employee because the employee reports a violation or suspected violation of the statute in good faith (N.J.S.A. 34:19-12).

Covered Employers

The law covers all employers except:

- Religious organizations.
- Political organizations.
- Educational institutions, if the institution requires a student or instructor to attend lectures on political or religious matters that are part of the regular coursework.

(N.J.S.A. 34:19-11(b).)

Covered Employees

The law covers all employees.

Co-Worker Violations

The law does not address co-worker violations.

Private Right of Action

The statute provides for a private right of action and remedies including:

- A restraining order against continuing violations.
- Reinstatement.
- Back pay.
- Attorneys' fees and costs.
- Punitive damages.

(N.J.S.A. 34:19-13.)

The statute does not limit or impair an employee's:

- Right to bring a wrongful termination claim against the employer.
- Rights under a **collective bargaining agreement**.

(N.J.S.A. 34:19-14.)

Administration

The NJDLWD administers the law.

Identity Theft Prevention Act: N.J.S.A. 56:11-44 to 56:11-53 and N.J.S.A. 56:8-161 to 56:8-166

Protected Activity

The Identity Theft Prevention Act prohibits individuals or businesses from:

- Publicly posting or displaying:
  - an individual's social security number; or
  - four or more consecutive numbers of the individual's social security number.
- Printing an individual's social security number on any materials mailed to the individual, unless required by law.
- Printing an individual's social security number on any card necessary to access products or services the entity provides.
- Intentionally releasing or otherwise making available to the general public an individual's social security number.

- Requiring an individual to electronically send his social security number unless:
  - the internet connection is secure; or
  - the social security number is encrypted.
- Requiring an individual to use his social security number to access an internet web site, unless one of the following is also required:
  - a password;
  - a unique personal identification number; or
  - another authentication device.

(N.J.S.A. 56:8-164(a).)

Employers must destroy all paper or electronic records containing personal information when they no longer need to be retained (N.J.S.A. 56:8-162).

Personal information means an individual's first name or initial and last name linked with one or more of the following:

- A social security number.
- A driver's license number.
- A state identification card number.
- A credit or debit account number with any required security code, access code or password that permits access to an individual's financial account.
- Otherwise dissociated data that would be personal information when combined together, if the means to link the data was also accessed.

(N.J.S.A. 56:8-161.)

The statute also contains explicit requirements in the event of a data breach in which an unauthorized person accesses an individual's personal information (see Question 7: Identity Theft Prevention Act).

Covered Employers

The law covers all employers.

Covered Employees

The law covers all employees.

Co-Worker Violations

The law does not address co-worker violations.

Private Right of Action

Individuals have a private right of action to address willful, knowing or reckless violations (N.J.S.A. 56:8-166.)

Administration

The Division of Consumer Affairs in the New Jersey Department of Law and Public Safety administers this law.

Computer Related Offenses Act: N.J.S.A. 2A:38A-1 to 2A:38A-6

Protected Activity

The Computer Related Offenses Act (CROA) prohibits a person from, without authorization, purposefully or knowingly:

- Altering, damaging, taking or destroying any data, database, computer program, computer software, internal or external computer equipment, computer system, or computer network.
- Altering, damaging, taking, or destroying a computer, computer system, or computer network.
- Accessing or attempting to access any computer, computer system, or computer network.
- Altering, accessing, tampering with, obtaining, intercepting, damaging, or destroying a financial instrument.
- Accessing and recklessly altering, damaging, destroying, or obtaining of any data, database, computer, computer program, computer software, computer equipment, computer system, or computer network.

(N.J.S.A. 2A:38A-3.)

Covered Employers

The law covers all persons and enterprises.

Covered Employees

The law covers all persons and enterprises.

Co-Worker Violations

The law does not address co-worker violations.

Private Right of Action

The CROA provides for a private right of action and remedies including:

- Compensatory damages.
- Punitive damages.

- Costs of investigation and litigation.
- Attorneys' fees.

(N.J.S.A. 2A:38A-3.)

Administration

The statute does not specify an administering agency.

Personnel Files

2. For any law in Question 1 regarding employer maintenance of personnel files, please describe:
   - What constitutes a personnel file in your jurisdiction.
   - Which records employers must maintain and for how long.
   - Any records that must be kept separately.
   - Any records that should not be included in an employee's personnel file.
   - How records must be maintained (for example, in digital or paper form, or in locked drawers or rooms).
   - Any requirements or prohibitions regarding destruction of records.

Definition of Personnel File

None of the laws listed in Question 1 provide a definition of personnel file.

Required Records and Maintenance Period

New Jersey employers must keep a record for each employee, for six years, containing the following information:

- The employee's name.
- The employee's address.
- The employee's birth date, if he is under the age of 18.
- The total hours the employee worked each day and each workweek, if the employee is classified as **nonexempt**.
- The employee's earnings.
- The total amount of gratuities the employee received during the payroll week.
- For employees who receive gratuities, daily or weekly reports completed by the employee with the following information:
  - the employee's name, address, and social security number;
  - the employer's name and address;

- the calendar day or week covered by the report; and
- the total amount received in gratuities.

- For employers claiming a credit for food and lodging as a cash substitute, information supporting the cost of furnishing the food and lodging.

(N.J. Admin. Code 12:56-4.1 to 12:56-4.10.)

In addition, for unemployment compensation, employers must maintain, for four preceding calendar years, the following employee information:

- Name.
- Address.
- Social security number.
- Hiring and termination date.
- Days worked.
- Weeks worked.
- Total remuneration.

(N.J.S.A. 43:21-1 to 43:21-24.4.)

Separate Records

New Jersey law does not address this issue.

Exclusions from Personnel Files

New Jersey law does not address this issue.

How to Maintain Records

New Jersey law does not address this issue.

Destruction of Records

New Jersey employers must properly destroy records containing personal information when they are no longer needed (see Question 1: Identity Theft Prevention Act).

3. For any law in Question 1 regarding employer access to personnel files, please describe:
    - Who may access the files, such as employees, applicants and former employees.
    - Whether individuals may copy the files or only inspect them.
    - When access must be granted (and whether it must be granted within a set period of time).

- Any limitations on access.

Right of Access

In New Jersey, employees do not have a statutory right to access their personnel files. However, employees may have a cause of action under state law if they request access to personnel files to investigate possible discrimination and are discharged in retaliation (*Velantzas v. Colgate-Palmolive Co.*, 109 N.J. 189, 191-195 (N.J. 1988)).

Current and former public employees must be informed of and are entitled to access records of their exposure to toxic chemicals (N.J.S.A. 34:6A-40(c)).

Copying or Inspection

Employees in New Jersey do not have a statutory right to access their personnel files.

Required Response Time

Employees in New Jersey do not have a statutory right to access their personnel files.

Limitations on Access

Employees in New Jersey do not have a statutory right to access their personnel files.

Medical or Other Test Results

4. For any law in Question 1 that protects employees from medical examinations, including AIDS/HIV tests, or other tests, such as psychological or personality tests, please describe any limitations on access to test results or the protection of records.

Genetic Privacy Act: N.J.S.A. 10:5-43 to 10:5-49

Under the Genetic Privacy Act, employers must obtain informed consent before receiving genetic information from any individual, with limited exceptions (see Question 1: Genetic Privacy Act).

In addition, a person may not disclose or be compelled to disclose, by subpoena or any other means:

- The identity of the individual receiving genetic tests.
- Genetic information about the individual that permits identification of the individual.

Genetic information may be disclosed in the following circumstances:

- Disclosure is necessary for either:
  - a criminal or death investigation; or

- a criminal or juvenile proceeding.

- To determine paternity.
- A court of competent jurisdiction authorizes the disclosure.
- As authorized by the DNA Database and Databank Act of 1994 (N.J.S.A. 53:1-20.17 to 53:1-20.37).
- The tested individual or his representative consents to the disclosure in writing.
- To provide genetic information relating to a deceased individual for medical diagnosis of the individual's blood relatives.
- To identify a body or bodies.
- Disclosure is made under the state or federal newborn screening requirements.
- Federal law authorizes the disclosure for identification purposes.
- An insurer discloses the information under the requirements New Jersey's insurance laws (N.J.S.A. 17:23A-1 to 17:23A-22).

(N.J.S.A. 10:5-47.)

Employee Electronic Communications

5. For any law in Question 1 that governs the monitoring or recording of employees' electronic communications, please describe what monitoring or recording is permitted or prohibited in each of the following media:
   - Telephone.
   - Internet.
   - Email.
   - Other.

New Jersey Wiretapping and Electronic Surveillance Control Act: N.J.S.A. 2A:156A-1 to 2A:156A-37

Telephone Communications

The New Jersey Wiretapping and Electronic Surveillance Control Act (Wiretap Act) covers all wire, electronic or oral communication, including telephone communications (N.J.S.A. 2A:156A-2).

However, most telephone conversations in the workplace fall within the exception allowing telephone recordings:

- In the normal course of business.
- That are necessary for either:

- business purposes; or
- to protect the employer's rights or property.

(N.J.S.A. 2A:156A-4(a).)

Internet Usage

The Wiretap Act allows internet service providers to disclose certain subscriber information when:

- A law enforcement agency obtains a grand jury or trial subpoena (*State v. Reid*, 194 N.J. 386, 403-406 (N.J. 2008)).
- The New Jersey State Commission of Investigation issues a subpoena.

The information that may be disclosed includes:

- Name.
- Address.
- Telephone number.
- Length of service and types of services used.
- Means and source of payment, including the credit card or bank account number used.

(N.J.S.A. 2A:156A-29(f).)

Email Communications

The Wiretap Act covers all wire, electronic, or oral communication, including email (N.J.S.A. 2A:156A-2).

However, many employers fall into one of the exceptions (see Question 1: The New Jersey Wiretapping and Electronic Surveillance Control Act: Covered Employers).

An employee who has email communications with his attorney through a personal, password-protected web-based email account that are sent and received using an employer-provided computer, are:

- Private.
- Protected by attorney-client privilege.

(*Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 317-321 (N.J. 2010).)

Other Forms of Communication

The Wiretap Act applies to all wire, electronic, or oral communication (N.J.S.A. 2A:156A-2).

The New Jersey Social Media Act: N.J.S.A. 34:6B-5 to 34:6B-10

Telephone Communications

The statute does not apply to telephone communications.

Internet Usage

The Social Media Act prohibits employers from requiring or requesting that current or prospective employees provide for personal social media accounts:

- A username or password.
- Any other means for access.

(N.J.S.A. 34:6B-6.)

Employers are also prohibited from:

- Requiring individuals to waive their rights under this statute as a condition of either applying for employment or receiving a job offer. An agreement to waive any right or protection under the Social Media Act is unenforceable. (N.J.S.A. 34:6B-7.)
- Retaliating or discriminating against individuals who exercise their rights under the Social Media Act (N.J.S.A. 34:6B-8).

The Social Media Act does **not:**

- Prohibit employers from accessing or using information about a current or prospective employee obtained in the public domain (N.J.S.A. 34:6B-10(d)).
- Apply to social media accounts created, maintained, or accessed by a current or prospective employee for purposes related to the employer's business (N.J.S.A. 34:6B-5).
- Prohibit employers from accessing information to investigate:
  - a violation of law;
  - employee misconduct; or
  - the improper transfer of confidential information or financial data.

  (N.J.S.A. 34:6B-10(c).)

Email Communications

The statute does not address email communication through social medial accounts.

Other Forms of Communication

The statute does not address additional forms of communication.

Searches, Surveillance, and Biometric Information

6. For any law in Question 1 that governs searches and surveillance, please describe:
    - Any limits on employer searches (such as searches in common areas or individual offices).
    - What kind of surveillance, tracking or monitoring of workplaces or employees is permitted (such as GPS or video, or surveillance of an employee's computer or phone usage) and whether there are any limitations on the areas that can be monitored or recorded.
    - Any limits on the use of biometric information (such as fingerprints, retina or voiceprint scans used for identification).

New Jersey Wiretapping and Electronic Surveillance Control Act: N.J.S.A. 2A:156A-1 to 2A:156A-37

Workplace Searches

The New Jersey Wiretapping and Electronic Surveillance Control Act (Wiretapping Act) does not address workplace searches.

Surveillance and Tracking

The New Jersey Board of Public Utilities (NJBPU) has issued orders regarding the use of monitoring and recording equipment. Before an employer monitors telephone calls, it must:

- Be a business subscriber and notify in writing the NJBPU of its intention to monitor.
- Only use monitoring and service-observing equipment for training, retraining, supervisory assistance, and measuring service levels.
- Notify all employees in writing that they are subject to monitoring before the monitoring begins.
- Label the telephone devices being monitored with notification stickers.
- Arrange through the telephone companies providing service in New Jersey for notification in telephone directories to potential callers that the employer uses monitoring equipment.

(Board of Public Utilities, Decision and Order, Docket No. 752-110.)

Biometric Information

The Wiretap Act does not address biometric information.

Notice to Employees

7. For each privacy law listed in response to Question 1, what obligations does an employer have to inform its employees of their rights?

New Jersey Wiretapping and Electronic Surveillance Control Act: N.J.S.A. 2A:156A-1 to 2A:156A-37

Employers must provide employees with written notice that they are subject to monitoring before the monitoring begins (Board of Public Utilities, Decision and Order, Docket No. 752-110).

The New Jersey Social Media Act: N.J.S.A. 34:6B-5 to 34:6B-10

The law does not address notice to employees.

Genetic Privacy Act: N.J.S.A. 10:5-43 to 10:5-49

The law does not address notice to employees.

Driving Records: N.J.S.A. 39:2-3.3 to 39:2-3.7

The law does not address notice to employees.

Freedom from Intimidation Law: N.J.S.A. 34:19-9 to 34:19-14

Employers may allow employees to voluntarily attend employer-sponsored meetings or provide other communications if the employer notifies the employees that they may, without penalty, refuse to either:

- Attend the meeting.
- Accept the communications.

(N.J.S.A. 34:19-10.)

Additionally, the Freedom from Intimidation Law is included within the New Jersey Conscientious Employee Protection Act (N.J.S.A. 34:19-1 to 34:19-14), which requires employers with ten or more employees to conspicuously post and annually distribute a notice to all employees of their rights under the statute (N.J.S.A. 34:19-7).

Identity Theft Prevention Act: N.J.S.A. 56:11-44 to 56:11-53 and N.J.S.A. 56:8-161 to 56:8-166

New Jersey employers that maintain computerized records containing personal information must notify individuals when any unauthorized person accesses their personal information (N.J.S.A. 56:8-163(a)).

Notice must be provided either:

- In writing.
- Electronically.

(N.J.S.A. 56:8-163(d).)

Employers may notify employees by substitute notice if either:

- The cost of providing the notice exceeds $250,000.
- The affected class of persons to be notified exceeds 500,000.
- The business does not have sufficient contact information.

Substitute notice must include all of the following:

- Email.
- Posting the notice on the business's website.
- Notification through statewide media.

(N.J.S.A. 56:8-163(d).)

Businesses must also notify:

- The Division of State Police (N.J.S.A. 56:8-163(c)(1)).
- If the breach involved more than 1,000 individuals, the **consumer reporting agencies** (N.J.S.A. 56:8-163(f)).

Computer Related Offenses Act: N.J.S.A. 2A:38A-1 to 2A:38A-6

The law does not address notice to employees.

Consequences for Violation

8. For each privacy law listed in response to Question 1, what are possible consequences for employers that violate the law?

New Jersey Wiretapping and Electronic Surveillance Control Act: N.J.S.A. 2A:156A-1 to 2A:156A-37

Any person violating the New Jersey Wiretapping and Electric Surveillance Control Act:

- Is guilty of a crime in the third degree and subject to:
  - fines up to $15,000 (N.J.S.A. 2C:43-3(b)(1)); and
  - imprisonment between three and five years (N.J.S.A. 2C:43-6(3)).

  (N.J.S.A. 2A:156A-3.)
- May be liable for:
  - actual damages, but not less than liquidated damages computed at a rate of $100 per day of violation or $1,000, whichever is higher;
  - punitive damages;
  - reasonable attorneys' fees; and

- reasonably incurred litigation costs.

(N.J.S.A. 2A:156A-24.)

The New Jersey Social Media Act: N.J.S.A. 34:6B-5 to 34:6B-10

Employers violating the New Jersey Social Media Act are subject to civil fines up to:

- $1,000 for the first violation.
- $2,500 for a second and any subsequent violation.

(N.J.S.A. 34:6B-9.)

Genetic Privacy Act: N.J.S.A. 10:5-43 to 10:5-49

Violations of this statute constitute a disorderly persons offense and may result in either or both of the following:

- A $1,000 fine.
- A six-month prison term.

(N.J.S.A. 10:5-49(a).)

Anyone who willfully discloses an individual's genetic information to another person is subject to either or both of the following:

- A $5,000 fine.
- A one-year prison term.

(N.J.S.A. 10:5-49(b).)

In addition, anyone disclosing an individual's genetic information is liable to that individual for any actual damages proximately caused by the disclosure, including:

- Economic damages.
- Bodily damages.
- Emotional harm.

(N.J.S.A. 10:5-49(c).)

Driving Records: N.J.S.A. 39:2-3.3 to 39:2-3.7

Any person who knowingly obtains or discloses personal information from a motor vehicle record for any unpermitted reason is guilty of a crime in the fourth degree and may face:

- Imprisonment up to 18 months (N.J.S.A. 2C:43-6).
- A fine up to $10,000 (N.J.S.A. 2C:43-3).

(N.J.S.A. 39:2-3.5.)

In a civil lawsuit, the court may award the aggrieved individual the following relief:

- Actual damages, but not less than liquidated damages of $2,500.
- Punitive damages for willful or reckless violations.
- Reasonable attorneys' fees and costs.
- Any preliminary and equitable relief the court deems appropriate.

(N.J.S.A. 39:2-3.6(b).)

Freedom from Intimidation Law: N.J.S.A. 34:19-9 to 34:19-14

Any aggrieved person may bring a civil action within 90 days of the alleged violation. The court may award the prevailing party the following relief:

- A restraining order against continuing violations.
- Reinstatement.
- Back pay.
- Attorneys' fees and costs.

(N.J.S.A. 34:19-13.)

Additionally, the court may award the prevailing party either:

- Punitive damages not greater than treble damages.
- An assessment of a civil fine, payable to the state treasurer, up to:
    - $1,000 for the first violation; and
    - $5,000 for a second and any subsequent violation.

(N.J.S.A. 34:19-13.)

Identity Theft Prevention Act: N.J.S.A. 56:11-44 to 56:11-53 and N.J.S.A. 56:8-161 to 56:8-166

The statute does not include consequences for violations.

Computer Related Offenses Act: N.J.S.A. 2A:38A-1 to 2A:38A-6

The statute provides for a private right of action and remedies including:

- Injunctions.
- Compensatory damages.
- Punitive damages.
- Costs of investigation and litigation.
- Reasonable attorneys' fees.

(N.J.S.A. 2A:38A-3 and 2A:38A-5.)

Consent

9. For each privacy law listed in response to Question 1, is employee consent required? If not, will employee consent protect the employer from liability?

New Jersey Wiretapping and Electronic Surveillance Control Act: N.J.S.A. 2A:156A-1 to 2A:156A-37

Having one party's consent is an exception to liability under the New Jersey Wiretapping and Electronic Surveillance Control Act (N.J.S.A. 2A:156A-4).

The New Jersey Social Media Act: N.J.S.A. 34:6B-5 to 34:6B-10

The New Jersey Social Media Act prohibits employers from requiring an applicant to waive any protections under this law as a condition of:

- Applying for employment.
- Receiving an officer of employment.

Any agreement waiving rights under the Social Media Act is against New Jersey public policy and void and unenforceable. (N.J.S.A. 34:6B-7.)

Genetic Privacy Act: N.J.S.A. 10:5-43 to 10:5-49

Employers must obtain an employee's informed consent before obtaining genetic information (N.J.S.A. 10:5-45).

Driving Records: N.J.S.A. 39:2-3.3 to 39:2-3.7

The statute permits disclosing personal information to any requestor with the notarized written consent of the individual to whom the information pertains (N.J.S.A. 39:2-3.4(c)(10)).

Freedom from Intimidation Law: N.J.S.A. 34:19-9 to 34:19-14

Employers may allow employees to voluntarily attend employer-sponsored meetings or provide other communications if the employer notifies the employees that they may refuse, without penalty, to either:

- Attend the meeting.
- Accept the communications.

(N.J.S.A. 34:19-10.)

Identity Theft Prevention Act: N.J.S.A. 56:11-44 to 56:11-53 and N.J.S.A. 56:8-161 to 56:8-166

The law does not address consent.

Computer Related Offenses Act: N.J.S.A. 2A:38A-1 to 2A:38A-6

The statute prohibits unauthorized:

- Altering, damaging, taking, or destroying any data, data base, computer program, computer software, computer equipment, computer system, or financial instrument.
- Accessing or attempt to access any computer, computer system, or computer network.

(N.J.S.A. 2A:38A-3.)

Recordkeeping

10. What are the recordkeeping obligations for each privacy law listed in response to Question 1?

New Jersey Wiretapping and Electronic Surveillance Control Act: N.J.S.A. 2A:156A-1 to 2A:156A-37

The law does not address recordkeeping obligations.

The New Jersey Social Media Act: N.J.S.A. 34:6B-5 to 34:6B-10

The law does not address recordkeeping obligations.

Genetic Privacy Act: N.J.S.A. 10:5-43 to 10:5-49

Records of genetic tests cannot be retained without first obtaining informed consent from either the individual or their representative unless retention is:

- Necessary for either a:
  - criminal or death investigation; or
  - criminal or juvenile proceeding.
- Necessary to determine paternity.
- Authorized by a court of competent jurisdiction.
- Made under the provisions of the DNA Database and Databank Act of 1994 (N.J.S.A. 53:1-20.17 to 53:1-20.37).
- For anonymous research where the individual's identity is not released.

(N.J.S.A. 10:5-46.)

DNA samples must be destroyed immediately on the individual's specific request (N.J.S.A. 10:5-46(b)).

Driving Records: N.J.S.A. 39:2-3.3 to 39:2-3.7

The law does not address recordkeeping obligations.

Freedom from Intimidation Law: N.J.S.A. 34:19-9 to 34:19-14

The law does not address recordkeeping obligations.

Identity Theft Prevention Act: N.J.S.A. 56:11-44 to 56:11-53 and N.J.S.A. 56:8-161 to 56:8-166

Employers must destroy all records containing "personal information," which includes all documents in either paper or electronic form containing an individual's first name or initial and last name linked with any one or more of the following:

- A social security number.
- A driver's license number.
- A state identification card number.
- A credit or debit account number with any required security code, access code or password that would permit access to an individual's financial account.

(N.J.S.A. 56:8-161 and 56:8-162.)

Computer Related Offenses Act: N.J.S.A. 2A:38A-1 to 2A:38A-6

The law does not address recordkeeping obligations.

Employees' Lawful, Off-duty Activity

11. To the extent not described in Question 1, please state whether an employee's lawful, off-duty use of or activity in any of the following is protected and describe any limits to the protections:
    - Tobacco use or use of other consumable goods.
    - Online activities, including posting on social media sites.
    - Other activities, including gun ownership or political activities.

Tobacco or Consumable Goods Use

Smokers' Rights: N.J.S.A. 34:6B-1 to 34:6B-4

New Jersey employers may not refuse to hire an individual or take any adverse employment action against an employee because that person does or does not:

- Smoke.
- Use tobacco products.

The only exception is if an employer has a rational basis that is reasonably related to the employment, including the responsibilities of the employee or applicant. (N.J.S.A. 34:6B-1.)

The statute provides for a private right of action and remedies including:

- Injunctive relief, including reinstatement of the employee to the same position.
- Compensatory and consequential damages.
- Attorneys' fees and costs.

(N.J.S.A. 34:6B-3.)

The New Jersey Department of Labor and Workforce Development may also impose civil penalties up to:

- $2,000 for the first violation.
- $5,000 for a second and any subsequent violation.

(N.J.S.A. 34:6B-4.)

Online Activities

The Social Media Act prohibits employers from requiring or requesting that current or prospective employees provide for social media accounts:

- A user name or password.
- Any other means for access.

(N.J.S.A. 34:6B-6.)

For more information, see Question 1: The New Jersey Social Media Act, Practice Note: Disciplining Employees for Social Media Posts in View of the NLRA and Disciplining Employees for Social Media Posts Checklist.

Other Activities

There are no other restrictions on lawful, off-duty activities in New Jersey. For information on New Jersey's medical marijuana laws, see State Q&A: Drug Testing Laws: New Jersey.

Invasion of Privacy Claims

12. For invasion of privacy claims in your jurisdiction, please describe:
    - The elements of an invasion of privacy claim, or factors relevant to the analysis.
    - Affirmative or other defenses available to the employer.
    - Examples of circumstances in which employees have been found to have a reasonable expectation of privacy in the workplace.

Claim Elements

New Jersey courts recognize the common law privacy tort of intrusion upon seclusion. Intrusion upon seclusion:

- Applies when an individual intentionally intrudes, physically or otherwise, on another's:
  - solitude or seclusion; or
  - private affairs or concerns.
- Subjects the individual intruding to liability to the other for the invasion of privacy if the intrusion would be highly offensive to a reasonable person.

(Restatement (Second) of Torts, § 652B.)

An invasion of privacy claim does not need to be a physical intrusion. A claim can arise "by the use of defendant's senses… to oversee or overhear the plaintiff's private affairs." The plaintiff is not required to prove publication of information to establish an intrusion upon seclusion claim. (*Hennessey v. Coastal Eagle Point Oil Co.*, 129 N.J. 81, 95 (N.J. 1992).)

Employer Defenses

An invasion of privacy is not "highly offensive" if the plaintiff had limited or no expectation of privacy. An individual’s expectation of privacy must be objectively reasonable. A subjective belief in privacy is irrelevant. (*White v. White*, 344 N.J. Super. 211, 223 (Ch. Div. 2001)).

Reasonable Expectation of Privacy

The Supreme Court of New Jersey noted that employees may have privacy rights based on the language and jurisprudence of the New Jersey Constitution and common law. However, an employee's right to privacy must be weighed against the competing public interest in safety. (*Hennessey*, 129 N.J. 81, 112-15.)

The Supreme Court of New Jersey has held:

- That a random drug test of an at-will employee in a safety-sensitive position did not violate public policy (*Hennessey*, 129 N.J. at 107).
- That an employee's email communications with her attorney were privileged because the plaintiff had a reasonable expectation of privacy in the emails that she exchanged with her attorney, even though the emails were transmitted through an employer-provided computer (*Stengart*, 201 N.J. at 321).

Other Employee Privacy Laws

13. Please list and briefly describe any additional employment-related workplace privacy laws not previously addressed.

There are no additional laws relating to employee rights with respect to privacy in the workplace in New Jersey.

In addition to the laws stated in Question 1, New Jersey may have additional laws on background checks and drug testing. For information on state laws on:

- Background checks, see State Q&A, Background Check Laws: New Jersey.
- Drug testing, see State Q&A, Drug Testing Laws: New Jersey.