Published on *The National Law Review* https://www.natlawreview.com

Data Privacy Whistleblowers Would be Protected Under Proposed Comprehensive Data Privacy Legislation

Article By:

Jason Zuckerman

Dallas Hammer

Yesterday Senators Maria Cantwell, Brian Schatz, Amy Klobuchar, and Ed Markey introduced comprehensive federal online privacy legislation to establish privacy rights, outlaw harmful and deceptive practices, and improve data security safeguards. The Consumer Online Privacy Rights Act (COPRA) codifies privacy as a right and authorizes the Federal Trade Commission (FTC) to hold companies accountable when they misuse or fail to safeguard consumers' information and creates a private right of action to enforce privacy rights. According to a summary, COPRA would:

- Create a strong data security right that requires companies to regularly assess security vulnerabilities and take preventive and corrective actions to protect consumer data.
- Create heightened privacy standards for collecting and sharing sensitive data such as biometric data and geolocation data.
- Create new enforcement powers for the FTC to take action against unlawful discrimination in the digital economy.
- Create data minimization standards and new data quality control mechanisms.
- Empower consumers with a strong private right of action.
- Give states the authority to fully enforce COPRA.
- Create accountability requirements so that senior executives take responsibility for decisions that impact privacy, and risk penalties when they fall short.

As whistleblowers have been instrumental in exposing the misuse or negligent safeguarding of consumer data, COPRA includes a whistleblower protection provision that would empower whistleblowers to assist the government in enforcing data privacy rights. For more information about why data privacy legislation should protect whistleblowers, see our recent article *Effective*

Cybersecurity and Data Protection Legislation Should Protect Whistleblowers.

Protecting Data Privacy Whistleblowers Against Retaliation

Section 204 of COPRA creates a private right of action for whistleblowers, referred to in COPRA as "covered individuals," that have suffered retaliation for disclosing a violation of any provision of COPRA. A ''covered individual'' means "an applicant, current or former employee, contractor, subcontractor, grantee, or agent of an employer."

COPRA Protected Whistleblowing

The whistleblower protection provision of COPRA would protect a broad range of disclosures about violations of data privacy rights, including disclosures made to an employer. In particular, protected conduct includes:

- Any lawful action in providing to the Federal Government, a State Attorney General, or a supervisor information relating to any act or omission that the covered individual reasonably believes to be a violation of COPRA or any regulation promulgated under COPRA;
- Testifying in an investigation or judicial or administrative proceeding concerning a violation of COPRA; or
- Assisting or participating in such an investigation or judicial or administrative proceeding.

Prohibited Retaliation Against Data Privacy Whistleblowers

Section 204 of COPRA prohibits a wide range of retaliatory acts, including discharging, demoting, suspending, threatening, harassing, or in any other manner discriminating against a covered individual. The catch-all category of retaliation ("in any other manner" discriminating against a whistleblower) includes non-tangible employment actions, such as "outing" a whistleblower or any act that would deter a reasonable employee from engaging in protected whistleblowing.

Favorable Causation Standard for Data Privacy Whistleblowers

COPRA's whistleblower protection provision applies the causation standard and burden-shifting framework set forth in the AIR21 Whistleblower Protection Law. Under that framework, whistleblowers prevail by proving that their protected whistleblowing was a contributing factor in the unfavorable personnel action taken by their employers. The DOL ARB has emphasized that the standard is low and "broad and forgiving"; protected activity need only play some role, and even an "[in]significant" or "[in]substantial" role suffices. *Palmer v. Canadian Nat'l R.R.*, ARB No. 16-035, ALJ No. 2014-FRS-154, at 53 (ARB Sept. 30, 2016)(emphasis in original). Examples of circumstantial evidence that can establish "contributing factor" causation include:

- temporal proximity;
- the falsity of an employer's explanation for the adverse action taken;
- inconsistent application of an employer's policies;

- an employer's shifting explanations for its actions;
- animus or antagonism toward the whistleblower's protected activity; and
- a change in the employer's attitude toward the whistleblower after they engage in protected activity.

Once the whistleblower proves that their protected conduct was a contributing factor in the adverse action, the employer can avoid liability only if it proves by clear and convincing evidence that it would have taken the same adverse action in the absence of the whistleblower engaging in protected conduct.

Remedies for Data Privacy Whistleblowers

A prevailing COPRA whistleblower would be entitled to a broad range of remedies, including:

- reinstatement;
- three times back pay with interest;
- uncapped compensatory damages;
- temporary relief while the case is pending; and
- attorney fees, litigation costs, and expert witness fees.

Procedures Governing Data Privacy Whistleblower Retaliation Claims

The statute of limitations for a COPRA whistleblower retaliation claim would be 90 days and the claim would be filed initially with OSHA, which would investigate the claim. If OSHA determines that there is reasonable cause to believe that a violation occurred, OSHA would order relief, including reinstatement of the whistleblower.

Either party would be able to appeal OSHA's determination by requesting a de novo hearing before the DOL Office of Administrative Law Judges (OALJ), but an employer's objection to an order of preliminary relief would not stay the order of reinstatement. Once a COPRA retaliation claim has been pending before the DOL for more than 180 days, the whistleblower could elect to remove the claim to federal court and try the case before a jury. COPRA retaliation claims would be exempt from mandatory arbitration.

Limited Current Protection for Data Privacy Whistleblowers

The existing patchwork of whistleblower protection laws offers minimal protection for data privacy and cybersecurity whistleblowers. A cybersecurity professional at a public company may find protection under the Sarbanes-Oxley Act. Likewise, an employee disclosing cybersecurity issues at a federal contractor or grantee might be protected under the False Claims Act and NDAA whistleblower protection laws. But all too often, cybersecurity and data privacy whistleblowers are not protected

against retaliation. Therefore, COPRA's whistleblower protection provision would be an important step forward to encourage workers to report the misuse or negligent safeguarding of consumer data.

For more information about current protections for cybersecurity and data privacy whistleblowers, see the following resources:

- Practitioners Guide to Cybersecurity Whistleblowing
- Cybersecurity Whistleblowing: What Employees at Public Companies Should Know Before Reporting Information Security Concerns
- The Rise of Cybersecurity Whistleblowing, NYU Law Compliance & Enforcement Blog (December 2016)
- Cybersecurity Whistleblowing: What Employees at Public Companies Should Know Before Reporting Information Security Concerns, ISSA Journal (June 2016)

National Law Review, Volumess IX, Number 331

Source URL:https://www.natlawreview.com/article/data-privacy-whistleblowers-would-be-protected-under-proposed-comprehensive-data