On June 18, 2020, Sen. Sherrod Brown introduced the Data Accountability and Transparency Act of 2020 (DATA 2020), which would establish enforceable privacy rights, limit the amount of data companies can collect, and hold companies accountable for misusing personal data. According to a summary issued by Sen. Brown, the bill would:

- Ban the collection, use, or sharing of personal data unless specifically allowed by law;
- Ban the use of facial recognition technology;
- Prohibit the use of personal data to discriminate in housing, employment, credit, insurance, and public accommodations;
- Require anyone using decision-making algorithms to provide new accountability reports;
- Create an independent agency dedicated to protecting individuals’ privacy and implementing DATA 2020 – the new agency would have rulemaking, supervisory, and enforcement authority, the ability to issue civil penalties for violations of...
the Act, and a dedicated Office of Civil Rights to protect individuals from discrimination;

- Empower individuals and state attorneys general to enforce privacy protections and would not preempt more protective state laws; and

- Require CEO certification of compliance with the Act and contain potential criminal and civil penalties for CEOs and Board of Directors.

This bill includes a whistleblower protection provision, which is critical to ensure that workers with firsthand knowledge of unlawful or unethical data privacy practices can oppose and expose those practices.

Covered Employees

Section 502 of DATA 2020 would protect an applicant, current or former employee, contractor, subcontractor, grantee, or agent of a data aggregator or service provider. A “data aggregator” is “any person that collects, uses, or shares an amount of personal data that is not de minimis,” but that term does not “include an individual who collects, uses, or shares personal data solely for personal reasons.” The law would also protect those who work for employers that provide services to data aggregators.

Protected Whistleblowing

The bill would provide broad protection to cybersecurity and data privacy whistleblowers. DATA 2020 would protect a covered worker who lawfully provides to the federal government or state attorney general information relating to what the worker reasonably believes to be a violation of the Act or its regulations. The law would also protect internal disclosures of information the worker reasonably believes to evidence such a violation. To be protected, a worker could make disclosures through their supervisory chain or to anyone else who the worker reasonably believes would have the ability to investigate, stop, or otherwise address the violation. The provision would also protect workers’ assistance or participation, including testimony in investigations or proceedings concerning violations of DATA 2020 or its regulations. Finally, the provision would protect any other action the worker takes to assist in carrying out DATA 2020’s purposes.

Because DATA 2020 would be a sweeping law that would implement a much-needed federal regulatory regime for data privacy, the anti-retaliation provision would cover a broad range of privacy and information security disclosures. Further, the proposed data privacy whistleblower protection law employs a reasonable belief standard. As long as the plaintiff’s belief is reasonable, the whistleblower is protected, even if the whistleblower makes a mistake of law or fact about the underlying violation of law or regulation.

Finally, in addition to the broad scope of protected activity, the bill would extend its whistleblower protections to anyone who is perceived as assisting the whistleblower, as well as preemptive retaliation.
Scope of Prohibited Retaliation Against Data Privacy Whistleblowers

Section 502 of DATA 2020 would prohibit a broad range of retaliatory acts, including directly or indirectly discharging, threatening, harassing, suspending, demoting, terminating, or in any other manner discriminating against a covered individual. The latter catch-all category of retaliation would encompass any act that would dissuade a reasonable worker from engaging in protected whistleblowing.

Enforcing the Data Privacy Whistleblower Protection Provision

Data privacy whistleblower retaliation claims would be governed by the rules, procedures, statute of limitations, and legal burdens of proof set forth in the AIR21 whistleblower protection law that protects whistleblowers in the airline industry. A retaliation claim would be filed initially within 90 days of when the whistleblower knew or should have known of the retaliatory adverse action.

OSHA would investigate the claim to determine whether there is reasonable cause to believe that protected activity was a contributing factor in the alleged adverse action. If OSHA finds a violation, it could order reinstatement of the whistleblower and other relief.

If the Department of Labor has not issued a final decision within 180 days of the complaint’s filing, the whistleblower could remove the case to federal court and try it before a jury. Arbitration agreements would not apply to data privacy whistleblower retaliation claims.

To prevail, the whistleblower would need to prove that their protected conduct was a contributing factor in the adverse employment action, i.e., that the protected activity, alone or in combination with other factors, affected in some way the outcome of the employer’s decision. The Department of Labor Administrative Review Board has emphasized that the standard is low, “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 Include Three Times Back Pay**

The [data privacy whistleblower protection provision](#) provides a range of remedies, including:

- Temporary relief while the case is pending;
- Reinstatement with the same seniority status that the individual would have had, but for the discharge or discrimination;
- Three times the amount of back pay otherwise owed to the individual, with interest; and
- Consequential and compensatory damages and compensation for litigation costs, expert witness fees, and reasonable attorneys’ fees.

**Current Protections for Data Privacy and Cybersecurity Whistleblowers**

In our practice representing cybersecurity and data privacy whistleblowers, we have found that federal law provides inadequate protection, especially where the whistleblower works at a company that is not publicly-traded. And we have found a disturbing pattern of retaliation against cybersecurity and data privacy whistleblowers. As former Amazon Vice President executive Tim Bray noted when he resigned a few weeks ago in protest of the firing of whistleblowers:

Firing whistleblowers isn’t just a side-effect of macroeconomic forces, nor is it intrinsic to the function of free markets. It’s evidence of a vein of toxicity running through the company culture. I choose neither to serve nor drink that poison.


We applaud Sen. Brown for introducing comprehensive data privacy legislation that includes a strong whistleblower protection provision. For more information about cybersecurity and data privacy whistleblower protections, see these resources:

- [Federal Law Should Protect Data Privacy Whistleblowers](#)
- [Effective Cybersecurity and Data Protection Legislation Should Protect Whistleblowers](#), NYU Law Compliance & Enforcement Blog (May 2019)
- [Practitioners Guide to Cybersecurity Whistleblowing](#)
- [Cybersecurity Whistleblower Protections for Employees of Federal Contractors and Grantees](#)
• Protections and Rewards for Cybersecurity Whistleblowers

• 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)

• Cybersecurity Whistleblowers Are Growing Corporate Challenge, Wall Street Journal (May 15, 2018)

© 2020 Zuckerman Law