THE
NATIONAL LAW REVIEW

Ninth Circuit, First Amendment, Glassdoor.com, grand jury subpoena, associational privacy and anonymous speech, common cause

Wednesday, June 27, 2018

At the end of last week, three U.S. Democratic Senators, including Connecticut's Richard Blumenthal, proposed the 44-page Data Security and Breach Notification Act ("Proposed Act"). The Proposed Act would preempt the laws of the 48 states that currently have data breach notification laws and the Federal Trade Commission ("FTC") would have enforcement authority. State Attorneys General would be permitted to pursue violations of the Proposed Act as civil actions in federal court if the FTC has not already initiated an action. The Proposed Act also provides for sizable civil penalties up to $5 million and criminal penalties including imprisonment for up to 5 years for willful failure to notify those impacted. Congress has considered proposed legislation on data security measures and breach notification in the past and it is unclear whether this effort will be more successful than the others, but given the recent Uber and Equifax incidents, lawmakers may be more motivated to act.

Article By Murtha Cullina
Dena M. Castricone
Privacy and Cybersecurity Perspectives

Communications, Media & Internet
All Federal

The Proposed Act would require any business, nonprofit, educational institution or charity that acquires, maintains or uses personal information ("Covered Entity"): (1) to establish and implement policies and procedures related to security practices; and (2) to notify impacted individuals and the FTC not later than 30 days after discovery of a breach with limited exceptions and, under certain circumstances, to notify each major consumer credit reporting agency, the Department of Homeland Security and/or other federal agencies. A breach is defined as the acquisition or access of electronically maintained personal information without authorization (or a reasonable belief that personal information was accessed or acquired without authorization). Violations of either the policy or notification provision would be deemed an unfair trade practice under section 5 of the Federal Trade Commission Act.

Personal information under the Proposed Act is defined as: (1) a full social security number; (2) a financial account, credit or debit card number with any applicable access or security code; or (3) the first and last name or first initial and last name in combination with at least one of the following: (a) driver's license, passport, alien registration number or other seminal government issued number; (b) unique biometric data; or (c) unique account identifier such as a user name along with the password to give access to something of value; or (4) two of the following: (a) home address or telephone number; (b) mother's maiden name; or (c) complete birth date.

Unlike the data breach notification law in Connecticut and in some other states, the Proposed Act does not mandate credit monitoring. It does, however, require that the Covered Entity provide an impacted individual with copies of his or her consumer credit report upon request and at certain intervals for 2 years after the request when certain information is involved in the breach.

Notably, financial institutions and health care entities will be deemed to be in compliance with the policy and notification requirements under the Proposed Act if the entities comply with their comparable requirements under other federal statutes and regulations (e.g. Gramm-Leach-Bliley Act and HIPAA/HITECH).

Source URL: https://www.natlawreview.com/article/ninth-circuit-first-amendment-glassdoorcom-grand-jury-subpoena-associational-privacy