Arnall Golden Gregory LLP
Attorneys at Law

Daily Privacy & Consumer Regulatory Alert

Published by the Privacy and Consumer Regulatory Practice | Washington, DC Office

July 10, 2018

FEDERAL DEVELOPMENTS

CFPB Deputy Director Resigns

On July 6th, Leandra English announced her resignation as the CFPB's Deputy Director and is dropping her case challenging Mick Mulvaney's appointment as Acting Director. The decision was made in light of President Trump's recent nomination of Kathy Kraninger to be permanent Director of the CFPB. English plans to leave the CFPB this week. On July 9th, the CFPB announced that Brian Johnson, who currently serves as Principal Policy Director at the CFPB, will serve as Acting Deputy Director.

STATE DEVELOPMENTS

Enacted State Legislation

- **Hawaii** enacted S.B. 2351, which prohibits employers from asking applicants about their prior compensation history. Employers that have at least one employee are covered. Under the legislation:
    - Employers, employment agencies, and their agents cannot inquire about an applicant's "current or prior wage, benefits, or other compensation." Employers are also prohibited from searching publicly available records or reports to obtain an applicant's salary history;
    - Covered entities are prohibited from relying upon an applicant's salary history to determine the applicant's compensation for the job, except in the case of a voluntary disclosure; and
    - Employers are allowed to discuss an applicant's compensation expectations and can conduct a background check to verify an applicant's disclosure of non-salary information.

- **North Carolina** enacted H.B. 744, which broadens the situations in which individuals convicted of a crime may petition for a "Certificate of Relief" and helps reduce the risks employers may face when hiring ex-offenders. The legislation takes effect in December 2018. In addition, the law protects employers from liability from most employment-related negligence claims when hiring or retaining ex-offenders with a Certificate of Relief if the employer "relied on" the certificate of relief in hiring or retaining ex-offenders, who must notify employers within 10 days of any new conviction.

COURT CASES

Time Inc. Class-Action Settlement

On July 5th, the U.S. District Court for the Eastern District of Michigan preliminarily approved a $7.4 settlement with Time Inc. for allegedly selling magazine subscribers' personal information. Lead plaintiff Carolyn Perlin filed the lawsuit in 2016 alleging that Time sold the personal data of individuals who subscribed to multiple magazines, and involved individuals' full names, home addresses, and reading habits, in violation of Michigan's Video Rental Privacy Act. The final hearing is scheduled for October 15th.

The case is Carolyn Perlin et al., Case No. 16-cv-10635, in the U.S. District Court for the Eastern District of Michigan.

INTERNATIONAL DEVELOPMENTS

UK Financial Regulators Publish Joint Discussion Paper

On July 5th, the Bank of England, the Prudential Regulation Authority, and the Financial Conduct Authority published a joint discussion paper intended to help financial firms achieve better operational resilience against operational disruptions, including cyberattacks. The paper highlights the risks associated with cyberattacks and other disruptive operational incidents and the financial system's increasing reliance on technology and data. The paper promotes several concepts for financial firms to increase operational resilience:

- Focusing on the continuity of the most important business services as an essential component of managing operational resilience;
- Setting board-approved impact tolerances which quantify the level of disruption that could be tolerated; and
- Planning on the assumption that disruption will occur as well as seeking to prevent it.

OTHER DEVELOPMENTS

Timehop Data Breach

On July 4th, Timehop, an application that compiles and posts users' old photos, announced a data breach that affected 21 million users. According to the company, the unauthorized access was discovered while in progress and was interrupted, but data was still stolen. The breach occurred because an access credential to the company's cloud computing environment was compromised, which was not protected by multifactor authentication. The compromised information included users' names, email addresses, some phone numbers, and encryption keys that allowed the application to read and share users' social media posts. Timehop has since conducted an audit and deployed enhanced security protocols to increase security. The company is also consulting with a cybersecurity firm and communicating with law enforcement.

This newsletter is published by AGG's Privacy and Consumer Regulatory Practice. For more information, please visit www.agg.com or contact Bob Belair, Kevin Coy, or Montserrat Miller. To subscribe, please email dpcra@agg.com.