What’s trending on NP Privacy Partner

The MasterCard and Target settlement reached in April is off the table, a recent FTC enforcement action is a reminder that every business should continually review and update its privacy policies, Connecticut enacts an employee social media privacy law, and the IRS announces a troubling cyber attack.

Children’s Privacy

*Bipartisan legislation pending in Congress to provide data to prospective college students*

In the United States Senate and House of Representatives, legislation titled “Student Right to Know Before You Go Act” seeks to provide college bound students and their families with expanded online data to evaluate higher education options. The legislation would significantly expand the range of available data by requiring the compilation of information such as post-graduate earnings averages at both institutional and program levels, graduation rates for part-time and transfer students and loan debt information for graduates and non-completers. Also, the legislation would require the outcome measures to be broken down based upon students’ Pell, Stafford and GI benefit status. Student records would be matched with employment and earnings data to compile the expanded data.

The Senate bill was introduced by Senators Ron Wyden (D-OR), Marco Rubio (R-FL) and Mark Warner (D-VA). Representatives Mia Love (R-UT) and Duncan Hunter (D-CA) introduced the comparable bill in the House, which Representative Paul Ryan (R-WI) has co-sponsored. The legislation would direct the Secretary of Education to make the information available online in an easily accessible format. The sponsors advocate that the expanded data will greatly aid prospective students as they face difficult personal and economic decisions about the best higher educational fit while facing the prospect of challenging job markets.

Similar bills failed to pass in prior Congressional sessions, especially as opponents cited privacy concerns. Proponents of the latest legislation contend that individual privacy would be strictly maintained with safeguards to prevent the disclosure of personally identifiable information. The online system would also be subject to audits evaluating the data quality, validity and reliability.
The United States Department of Education currently makes information available through its College Scoreboard, which sponsors of the legislation contend is too limited. We will continue to watch the course of the “Student Right to Know Before You Go Act,” as the legislation appears to be gathering more support in Congress and as all associated privacy concerns are evaluated in both the Senate and House.—Steven M. Richard

Data Breach

IRS announces breach of 100,000 tax accounts through website application

The IRS announced a major cyber attack on its “Get Transcript” web application that exposed information of 100,000 tax accounts, including past filings. Criminals used those past filings to apparently file more than $50 million in fraudulent tax returns. The IRS reports that its main computer system that handles tax filing submission is unaffected by this breach.

Though the “Get Transcript” application requires two-step authentication for access, the process was evidently breached by the attackers’ use of personal information, including Social Security information, date of birth, tax filing status and street address, which the IRS believes was gathered through other sources prior to the attempts on the IRS application. The IRS believes that a total of 200,000 attempts were made on the system.

The IRS will be contacting the 100,000 affected in the transcript attack and offering free credit monitoring to those individuals, and will also be sending letters to the other 100,000 consumers whose accounts were ultimately not accessed to make them aware that their personal information has apparently been acquired through other sources.—Kate A.F. Martinez

Employee Workplace Privacy

Connecticut enacts employee social media privacy law

On May 19, 2015, Connecticut Governor Dannel Malloy signed legislation (Senate Bill No. 426) to limit employer access to the personal social media accounts of employees and job applicants. The new law (Public Law 15-6) will take effect on October 1, 2015. Connecticut is the 21st state to approve such legislation, and several states are considering such measures during their legislative sessions.

The law prohibits an employer from undertaking any of the following actions:

1. Requesting or requiring an employee or applicant to provide a user name, password or any other authentication means for accessing a personal online account;

2. Requesting or requiring an employee or applicant to authenticate or access a personal online account in the employer’s presence;

3. Requiring an employee or applicant to invite the employer or accept the employer’s invitation to join a group affiliated with a personal online account;
4. Taking an adverse job action (such as discharge or discipline) against an employee who refuses to provide the employer with means to access a personal online account; or

5. Failing or refusing to hire an applicant who declines to provide the prospective employer with means to access a personal online account.

Despite these prohibited actions, the law provides employers with protections. An employer may request that an employee or applicant provide access to any account or service provided by the employer for business purposes, as well as any electronic device supplied or paid for by the employer. Employers may also conduct an investigation to ensure compliance with federal, state and regulatory requirements, upon the receipt of “specific information” suggesting misconduct on an employee or applicant’s personal online account. Also, an employer may investigate an employee or applicant’s unauthorized transfer of proprietary, confidential or financial information and may implement appropriate responsive actions. An employer conducting the investigation may require an employee or applicant to allow access to his or her personal online account, but the employer shall not require the employee or applicant to disclose the user name and password or other authentication means for accessing the personal online account.

The newly enacted law allows an employee or applicant to file a complaint with the Connecticut Labor Commissioner alleging an employer’s violations of the prohibited activities. The Commissioner may levy fines up to $1,000 and award “all other appropriate relief,” including rehiring, reinstatement, payment of back pay, reinstatement of benefits, and any other remedies necessary to redress the violation. Any party aggrieved by the Commissioner’s decision may file an appeal to the Connecticut Superior Court.—Steven M. Richard

---

**Enforcement & Litigation**

**Recent FTC enforcement action against technology startup underscores the need to continually monitor and update company privacy policies**

Many companies now consider mobile applications, or “apps,” for smartphones an integral part of their business—they collect reusable data, including a user’s location, preferences, daily habits, photos, videos and calendar entries. Contrary to what you might think, however, there currently is no law or regulation that requires the inclusion of a privacy policy for internet websites or mobile apps. Nonetheless, privacy policies are important disclosure documents (as are the Terms and Conditions, Site May and About Us documents). In early 2013, the Federal Trade Commission (“FTC”) published privacy guidelines for mobile app developers and for the first time suggested that developers include privacy policies that can be easily accessed through app stores, and recommended that apps disclose if user information is shared to third parties.

Just last month, the FTC took its next large leap forward in its focus on mobile device privacy. On April 23, 2015, the federal agency agreed to settle claims stemming from alleged misrepresentations in an online privacy policy of a technology startup company called Nomi Technologies. According to the complaint filed by the FTC, Nomi is a data analytics company that uses sensors placed in its clients’ retail stores to collect information from consumers’ mobile devices. This service, marketed by the name of Listen, helps retail companies understand customer traffic patterns. Nomi does not require its retail clients to post disclosures or otherwise notify consumers that they may be tracked in or near a retail store using the Nomi Listen service and almost none of the forty Nomi retail clients disclosed their use of the service to customers.
Interestingly, that wasn’t the focus of the complaint against the company. Instead, the FTC took issue with what it viewed as false and misleading representations in the privacy policy located on the Nomi website. While the Nomi privacy policy pledged to “always allow consumers to opt out of Nomi’s service on its website as well as at any retailer using Nomi’s technology,” there was no opt-out mechanism on the website or in retail stores, and consumers were not made aware that the Listen service was even being used. The terms of the settlement prohibit Nomi from misrepresenting consumers’ control over whether information is collected, used or shared about them or their devices, and the extent to which consumers will be notified about how their information is collected or shared. The FTC will retain oversight responsibility to enforce the agreement for several years.

For companies large and small, the Nomi action should serve as an important reminder to ensure the accuracy of any posted privacy policy. Refrain from simply cutting and pasting policies found on other websites; post only those policies and procedures adhered to by your company. Also, keep in mind that company policies change over time, particularly those of new stage businesses. Periodically review company privacy policies and update them to ensure accuracy. Finally, continually monitor federal and state data privacy laws as disclosure requirements may heighten over time. A failure to institute these best practices could result in legal action for the unsuspecting business.—Cameron Cloar-Zavaleta

MasterCard and Target fail to finalize settlement in data breach suit

The data breach settlement reached last month between Target and MasterCard is off the table. Target offered $19 million to MasterCard issuers for operational costs and fraud-related losses on MasterCard branded payment cards. As we discussed last month, the deal required buy-in from at least 90% of the eligible MasterCard issuers as of May 20, 2015. The May deadline came and went without the required number of acceptances and so that settlement offer is no longer viable. Trial is currently scheduled for March 2016.

The Target consumer settlement, reached weeks before the announcement of the proposed settlement with MasterCard, is unaffected by this development.

We will keep you posted on further developments.—Kate A.F. Martinez

Consumer Privacy

Song-Beverly credit card opinion highlights need for retailers to review their procedures for credit card transactions

Retailers take note—having clear and uniform procedures for requesting personal data at the point of sale can save litigation headaches. That’s how Levi Strauss & Co. recently defeated a class action for improper solicitation of personal data in connection with credit card transactions under the Song-Beverly Credit Card Act. Read more here.—Karl D. Belgum
For more information, please contact:

— Karl D. Belgum at kbelgum@nixonpeabody.com or
— Cameron Cloar-Zavaleta at ccloarzavaleta@nixonpeabody.com or 415-984-8285
— Kate A.F. Martinez at kmartinez@nixonpeabody.com or 585-263-1332
— Steven M. Richard at srichard@nixonpeabody.com or 401-454-1020

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team.