BNA, INC.

ELECTRONIC COMMERCE & LAW

BNA Employee-Owned Since 1947

REPORT

Privacy

Attorneys Say Facebook's Privacy Woes Show Traps in 'Notice and Choice' Paradigm

Complaints about Facebook's new privacy controls highlight the challenges companies face in effectively executing the prevailing ''notice and choice'' approach to protecting consumer privacy online, particularly when a company's privacy practices change over time, privacy attorneys told BNA.

In an effort to alert users to privacy impacts of recent changes to Facebook's social network, company executives and policy staff Dec. 9 published blog posts and presented site users with a pop-up menu containing suggested default privacy settings. Company officials said this information would help users understand and control access to their personal information in the face of new privacy policy changes. However, privacy advocates complained that the company's talking points and transition tools should have highlighted that the company now considers certain user information to be publicly accessible, a shift from its former policies.

The backlash to Facebook's updated policies—including a complaint filed Dec. 17 by the Electronic Privacy Information Center with the Federal Trade Commission (*In the Matter of Facebook Inc.*, FTC, *docket number unavailable, complaint filed* 12/17/09)—comes at a time when the FTC is reportedly contemplating changes to its ''notice and consent''-focused privacy protection regime. The commission hosted the first of three scheduled online privacy workshops Dec. 7; two more will be held in January and March 2010.

The FTC has taken the position that a company may not retroactively apply a privacy policy—in which terms have been materially modified—to previously collected consumer information unless the consumer affirmatively consents to the new policy.

In 2004, the FTC investigated Gateway Learning Corp. for suspected unfair practices violating Section 5 of the FTC Act (15 U.S.C. § 45) under the changed-terms theory. The commission concluded that Gateway's application of an updated privacy policy, which permitted data-sharing, to data collected under a more restrictive policy, was unfair. Through a subsequent settlement the company was enjoined from sharing personal data collected under the earlier policy without obtaining express affirmative consent (9 ECLR 622, 7/14/04).

Notice and Choice: An Ongoing Obligation. Lisa J. Sotto, head of Hunton & Williams' privacy and information management practice, told BNA that, while Facebook did provide notice—and forced users to make a choice, even if it was the service's most-open defaults—the very fact that there were so many complaints shows that the service probably should have been configured differently.

''Consumers need to feel they have meaningful control over their information, and the pushback suggests that didn't happen,'' Sotto said.

Giving consumers notice about data privacy and an opportunity to opt-out of collection and sharing is not a one-time obligation. Notice and choice have to recur in a meaningful way as companies' business practices and privacy policies evolve, Fred Cate, professor and director of the Center for Applied Cybersecurity Research at Indiana University Maurer School of Law, explained.

''I do think it is unfair for services to collect user information under one policy, and then distribute it under one that provides less protection,'' Cate said. ''If information was provided under one set of rules, then a company should obtain clear consent before applying new standards to that information,'' he advised.

Potential Changes for FTC Privacy Approach. Section 5 empowers the FTC to investigate and enjoin unfair and deceptive trade practices. Unfair practices cause or are likely to cause substantial harm to consumers that is

not outweighed by countervailing benefits to consumers or competition. Deceptive actions are likely to mislead consumers acting reasonably in the circumstances.

Since 1995, the commission has conducted workshops, initiated investigations, and issued policy statements applying Section 5's consumer protection principles to online commerce.

Most recently, the commission has taken a notice and choice approach to online privacy issues. But as the commission reviews its privacy perspective, companies could see a change in the regulatory status quo.

In February, the commission published principles the FTC said were designed to guide the industry's self-regulatory efforts related to online marketing. The principles include four governing concepts: transparency and control, data security and limited data retention, material changes to privacy policies, and affirmative express consent for collection of sensitive data.

The transparency and control aspect states that companies should provide meaningful disclosures to customers about their data-collection practices, and give consumers a choice about whether they want to allow it.

The report also said that companies should tell consumers about policy changes, and give them the option to accept or reject their application to previously collected information. ''[B]efore a company uses behavioral data in a manner that is materially different from promises made when the company collected the data, it should obtain affirmative express consent from the consumer.''

FTC Chairman Jon Leibowitz has not had very many kind things to say about the prevailing ''notice and choice'' privacy paradigm. ''Notice and choice and harm-based approaches haven't worked as well as we would have liked,'' Leibowitz said during a recent privacy event. He stressed that he has long been a supporter of consumer opt-in as a prerequisite to the use of personal information (14 ECLR 1728, 12/9/09).

FTC: Privacy Policy Updates Can Be Unfair. In the Gateway Learning proceeding, the FTC wanted to send a message to all companies that retroactive changes to privacy policies could bring FTC scrutiny, Jessica Rich, who was then assistant director of the FTC Division of Financial Practices, said at the time (9 ECLR 622, 7/14/04).

From the FTC's perspective the problem in the Gateway proceeding was not that the company changed its policies. The unfairness resulted from applying the new policy to previously collected information without affirmative, express consent.

Facebook Notified Users About Changes. On Dec. 1, Facebook founder Mark Zuckerberg posted a letter on a Facebook blog in which he said the service was working on ''a simpler model for privacy control where you can set content to be available to only your friends, friends of your friends, or everyone.''

On Dec. 9, the privacy changes went into effect. ''Facebook will be rolling out easy-to-use tools to empower people to personalize control over their information—based on what the content is, why they are sharing it, when, and the audience they seek to reach,'' the company announced.

When users logged in they were presented with a pop-up notice about changes to the privacy policy. Facebook walked users through a series of screens containing privacy choices it said would help ease the transition to the new privacy protocols.

Through the transition tool, Facebook gave users the choice to either preserve current settings or accept new suggested privacy defaults.

Advocates Say Defaults Compromise Privacy. The changes—especially the defaults—did more to compromise users' privacy than they did to protect it, some groups said.

Kevin Bankston, senior staff attorney with the Electronic Frontier Foundation, both praised and criticized the changes on the group's website. ''We're glad to see Facebook is attempting to respond to [ ] privacy criticisms with these changes, which are going live this evening[,]'' he wrote. ''Unfortunately, several of the claimed privacy 'improvements' have created new and serious privacy problems for users of the popular social network service.''

One area of particular concern is Facebook's new categorization of ''publicly available information,'' Bankston told BNA. The phrase was not contained in prior policies, but now applies to user information such as names, profile photographs, current city, gender, networks, and ''fan pages.''

Under the new policy, that information is not controlled by users' privacy settings and can be freely accessed by ''everyone,'' including third party applications. However, users can prevent that information from being obtained through searches both within the network and on search engines by modifying that setting using a menu linked to its ''privacy settings'' page.

The negative effects on users' privacy may be felt immediately, critics said, noting recent market developments. Google announced Dec. 7 partnerships with Facebook, as well as MySpace and several other social networks. Through the deals, ''publicly available'' information from those sites, including updates and blogs, will now be indexed and displayed in search results.

The Facebook ''privacy settings'' page, which is linked to the bottom of all Facebook pages and presented separately from users' ''account settings,'' contains options for users to restrict search engines' access to their account information.

When announcing the new policies, Facebook staff should have said more about those changes, Bankston said.

EPIC: Facebook Unfairly Changed Policies. In the complaint filed with the FTC, EPIC—joined by the Center for Digital Democracy, Consumer Federation of America, and seven other privacy groups—asserted that the changes are unfair and deceptive in violation of Section 5 of the FTC Act.

Despite Facebook's representations that it was offering users more control over their information, the company disabled privacy controls for some categories of information altogether and led users towards default options that were designed to make more information publicly available, the groups argued.

Incremental changes to Facebook policies over time have created new categories of public information that are available to developers of hundreds of thousands of third-party applications, as well as to search engines. Users who signed up under previous policies were not given meaningful notice or effective options to prevent sharing, the groups asserted.

   ISSN 1098-5190

Searching Facebook's application directory and opting out of each of over 350,000 applications—which is what users now have to do to prevent their newly defined ''publicly available'' information from being shared with applications—is not a meaningful choice, the groups argued in their complaint.

The shift is likely to cause substantial injury to users' privacy and is thus unfair, the groups complained, looking to the Gateway proceeding for support. It was also deceptive, they said, because Facebook told users it was simplifying its privacy practices, while it set up roadblocks impeding the process.

In their complaint, the groups asked the FTC to:

- compel Facebook to restore its previous privacy settings to allow users to choose whether their information is publicly available;
- compel Facebook to allow users to fully opt out of revealing information to third party developers;
- compel Facebook to make its data collection practices clearer and more comprehensible, and to give users meaningful control over personal information provided by Facebook to advertisers and developers; and
- enjoin what the complaints called unfair and deceptive business practices.

The complaints have the potential to focus the Commission's attention on issues related to changing privacy practices. ''EPIC frequently files complaints with the FTC regarding privacy issues,'' Sotto said. ''This will likely ensure increased scrutiny by the FTC on the changes made by Facebook to users' privacy settings.''

BY AMY E. BIVINS

Full text of the complaint filed with the FTC at http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf