



ELECTRONIC COMMERCE & LAW



REPORT

Reproduced with permission from Electronic Commerce & Law Report, 16 ECLR 566, 4/6/11, 04/06/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Privacy

FTC-Google Pact: First Major Safe Harbor Action, First ‘Privacy by Design’ Requirement

The Federal Trade Commission’s proposed administrative consent agreement with Google Inc. over the internet giant’s alleged misuse of user data during the launch of its now-abandoned Buzz social network yielded a number of firsts—including the FTC’s first action against a firm for failing to live up to privacy promises under the U.S.-EU Safe Harbor Program, which launched in 2000 (*In re Google Inc.*, FTC, File No. 102 3136, *proposed consent agreement* 3/30/11).

Privacy and e-commerce attorneys told BNA that the enforcement action also serves notice that the FTC considers privacy by design to be more of a compliance requirement than a guiding principle. Privacy by design is aimed at building privacy into the front end of the design and implementation of new information systems and technology.

According to the FTC, “this is the first time an FTC settlement order has required a company to implement a comprehensive privacy program to protect the privacy of consumers’ information.” The agreement will, in essence, require Google to embed privacy by design in its operations, attorneys said March 30.

Privacy by Design Now Legal Requirement? “This enforcement action and settlement marks a significant step toward moving privacy by design from ‘best practice’ to ‘compliance requirement’ since the regulated community is now effectively on notice that failure to fully integrate privacy into product and service developments could constitute a violation of the FTC Act,” Elizabeth Johnson, a partner and privacy and information security practice leader at Poyner Spruill LLP, in Raleigh, N.C., told BNA.

The FTC’s online privacy preliminary staff report, released in December 2010 (15 ECLR 1815, 12/8/10), made privacy by design one of its core principles.

Privacy by design has been championed as an alternative to after-the-fact enforcement action (16 ECLR 481, 3/23/11). But the FTC action against Google takes the concept beyond promotion of a self-regulatory scheme into the enforcement arena, perhaps serving as the commission’s notice to businesses that it may view privacy by design as a requirement under Section 5, attorneys told BNA.

The proposed consent agreement sends a clear message to businesses—“You better very closely review how your new products or services will use the personal data you previously collected from your customers or users, and take account of the corresponding privacy implications for those uses, before you roll out the new products or services to the public,” Alan Charles Raul, with Sidley Austin LLP, in Washington, told BNA March 30.

“The FTC continues to make new privacy law through its ‘common law of consent decrees’ as its final Staff Report is pending and legislative ideas get batted about,” Christopher Wolf, Hogan Lovells LLP, Washington, D.C., remarked.

The bottom line, Wolf said, is that online privacy standards are becoming more stringent even without new laws or regulations, even though the FTC lacks rulemaking authority.

“The launch of Google Buzz fell short of our usual standards for transparency and user control—letting our users and Google down,” Google Director of Privacy, Product & Engineering Alma Whitten said in a March 30 post on the official Google blog.

FTC: Buzz Privacy Promises Deceived Gmail Users. In a draft administrative complaint released concurrently with the proposed consent agreement, the FTC alleged that Google violated Section 5 of the FTC Act by engaging in false and misleading promises to users about how it would use the information of those who signed up for Gmail accounts.

The FTC contended that Google led Gmail users to believe that they had a choice about whether they wanted to enroll in the Buzz networking feature, but

that at least some opt out attempts were ignored. For those that stayed in the program, Google did not inform them adequately that their most frequent e-mail contacts would be made public by default.

Despite a privacy policy that said Google would notify users if data was used for a purpose different than that for which it was collected, user data ended up posted on third party websites, FTC said.

Safe Harbor Notice, Choice Principles at Issue. Despite Google assurances to users that it complied with the requirements of the Safe Harbor Program—a data protection certification registry that allows U.S. companies and organizations to transfer personal information outside of the European Union without running afoul of the EU Data Protection Directive (95/46/EC) if they voluntarily commit to comply with EU privacy requirements—it “did not adhere to the US Safe Harbor Privacy Principles of Notice and Choice,” the FTC complaint said.

Google’s statements to users asserting that it complied with Safe Harbor requirements and its own separate privacy policies and claims that it would only collect user data to set up Gmail accounts amounted to prohibited deceptive acts or practices under the FTC Act, the complaint said.

The proposed consent order would bar Google from misrepresenting the privacy or confidentiality of individuals’ information or misrepresenting compliance with the U.S.-EU Safe Harbor or other privacy, security, or compliance programs.

The Department of Commerce administers the Safe Harbor Program registry but program enforcement is the FTC’s responsibility. Some EU officials, particularly German data protection authorities, have questioned whether Safe Harbor Program compliance has been adequately enforced.

Prior to the current case, the only FTC enforcement actions made public involved a company that claimed it was registered in the Safe Harbor Program when it was not and six firms that continued to tell users they were part of the program but had let their registrations lapse.

Commerce officials have pointed out more than 4,000 complaints by individuals regarding their personal information that have been resolved through the third party dispute resolution process established as part of the Safe Harbor Program.

Google’s launch of Buzz and its hasty retreat when consumers and regulators complained quickly became the go-to case study to demonstrate the need for companies to embrace a privacy by design approach to privacy protection.

Requirements for Google. Under the agreement, Google must establish and maintain a comprehensive privacy program. Google must submit to independent data protection audits every two years for the next 20 years. The 20-year compulsory independent oversight requirement has been a frequent fixture of FTC privacy and security consent agreements dating back to its pact with Eli Lilly and Co. in January 2002 (7 ECLR 76, 1/23/02). (See a summary of other recent FTC settlements at Buzz at “Google Buzz One of Many Recent FTC Targets”).

Google would also be required to obtain the assent of users before sharing their information with third parties if Google changes its products or services in a way that results in information sharing that is contrary to

any privacy promises made when the user’s information was collected.

If finalized, the settlement will require Google to perform a privacy risk assessment during “product design, development and research,” Johnson noted.

“That language, in essence, requires a privacy impact assessment, something privacy professionals have widely tried to integrate into their organizations with varying degrees of success,” she added. “Privacy impact assessments are a key step toward a ‘privacy by design’ approach to privacy implementation, Johnson said.

In a March 30 statement, the Electronic Privacy Information Center—which filed a complaint against Google with the FTC within a week of Buzz’s launch (15 ECLR 273, 2/24/10)—called the proposed settlement “the most significant privacy decision by the Commission to date.”

The privacy requirements in the settlement itself are not particularly surprising, Daniel T. Rockey, of counsel with Bullivant Houser Bailey PC in San Francisco, remarked. “The proposed settlement itself imposes pretty modest requirements which I am confident Google had already intended to adopt, and which are consistent with industry best practices (aside from the compulsory audits),” he said.

Developer-Privacy Staff Disconnect? Google’s approach to the launch of Buzz was the antithesis of privacy by design, attorneys said. They told BNA that the case demonstrates the privacy hazards that can arise when risk and liability assessments take a backseat to the push to get new and innovative online services to the market.

The action also demonstrates the risk of a lack of communication between corporate product developers and privacy and legal staff, according to Gary Kibel, a partner with Davis & Gilbert LLP, in New York City. “In this case, there appears to be a disconnect between very creative developers and privacy advisors,” he said.

Buzz was “a very intentional disclosure, and no one stopped and asked, ‘Does our policy permit us to do this with this data?’,” Kibel said.

Kirk Nahra, a partner with Wiley Rein LLP, in Washington, expressed a similar view. “This action shows the importance of knowing what you’re going to do in advance, and that privacy by design has to be built in from the start.”

“Google really bungled the Buzz rollout, they know they bungled it, and the FTC had them dead-to-rites in failing to act in accordance with their stated privacy policy and the EU safe harbor,” Rockey added.

Leslie Harris, president of the Center for Democracy & Technology, predicted in a March 30 statement that the FTC settlement “will have a far-reaching effect on how industry develops and implements new technologies and services that make personal information public.” Harris added: “We expect industry to quickly adopt the new requirement for opt-in consent before launching any new service that will publicly disclose personal information.”

Rosch Cites Competition, Opt-In Consent Concerns. The Commission vote to accept the proposed consent order and seek public comment was 5-0, with Commissioner J. Thomas Rosch concurring. The FTC released an analysis of the agreement to assist members of the pub-

Google Buzz One of Many Recent FTC Targets

The Federal Trade Commission's Bureau of Consumer Protection has taken an increasingly active interest in companies' online privacy practices in recent years—demonstrated by both its comprehensive review of its privacy policymaking strategy and publicized investigations into companies' privacy and data security efforts, or lack thereof.

Other recent FTC investigations against online companies that have resulted in settlements include:

In re Chitika Inc., (March 14, 2011)(16 ECLR 414, 3/16/11). Settlement prohibits company from misrepresenting the extent of its data collection and consumers' controls; requires it to improve transparency about data collection via a mandated website notice, and provide a five-year opt-out.

In re SettlementOne Credit Corp., In re AC-RAnet Inc., In re Fajilan and Associates Inc., (March 3, 2011)(16 ECLR 181, 2/9/11). Settlements require companies to establish and maintain a "comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information[.]" Companies are also ordered to comply with applicable data security laws and regulations.

FTC v. EchoMetrix Inc., (Nov. 30, 2010)(15 ECLR 1809, 12/8/10). Settlement prohibits company from sharing children's information obtained without proper disclosure and consent, and destroy information that was improperly shared with a marketing company.

In re Twitter, (June 24, 2010)(15 ECLR 1052, 6/30/10). Settlement requires Twitter to implement a comprehensive information security program that will reasonably protect nonpublic information.

In re Sears, (June 4, 2009)(14 ECLR 819, 6/10/09). Settlement requires company, prior to installing tracking applications, to provide detailed privacy notices on a separate screen and obtain express opt-in consent.

In each case other than the *Echometrix* action, the consent orders terminate 20 years from the date of issuance.

lic in reviewing the settlement. Comments are due by May 1.

In his concurrence, Rosch voiced skepticism over any settlement that may hurt rivals as much or more than Google. He warned against use of an FTC settlement "as 'leverage' in dealing with the practices of other competitors."

Rosch, who served as Director of the Bureau of Consumer Protection from 1973 to 1975, explained that Part II of the proposed order bars Google, without prior "express affirmative consent"—essentially, an "opt-in" requirement—from engaging in any "new or additional sharing" of previously collected personal information "with any third party" that results from "any change,

addition, or enhancement" to any product or service offered by Google.

The "opt-in" requirement, he cautioned, "is seemingly brand new" and could be used "as leverage in consent negotiations with other competitors." Rosch questioned the wisdom of the 20-year life of the settlement—especially in a market where internet business models and technology change so rapidly. Finally, he posited, the Part II restrictions would extend beyond Google's social networking services to all Google services and products.

Google was represented by Albert Gidari, of Perkins Coie, in Seattle, and Kent Walker, Google vice president and general counsel, in Mountain View, Calif. Kathryn D. Ratté and Katherine Race Brin of the FTC, in Washington, represented the commission.

Senators: Case Highlights Need for Federal Law. Sen. John D. Rockefeller IV (D-W.Va.), who chairs the Commerce, Science and Transportation Committee, said in a March 30 statement that he was pleased that the FTC "is taking this issue so seriously" and that the FTC action should be "a wake-up call for online businesses—both large and small—of the need to be clear and honest about how the personal information of consumers is collected and used."

Sen. John Kerry (D-Mass.), who chairs the Communications, Technology and the Internet Subcommittee of Rockefeller's committee, said in a separate March 30 statement that the FTC's enforcement action is "evidence of the need for a Commercial Privacy Bill of Rights," proposed by the Obama administration and embodied in draft legislation Kerry is working on.

"Baseline privacy protections in law remain common sense, and this case proves it," Kerry said. This "underscores that everyone will be better off with clear rules of the road rooted in a specific law."

Other Legal Fallout From Buzz. The FTC action is not the only legal scrutiny Google has faced as a result of its actions surrounding Buzz.

Although Google began dismantling Buzz's automatic data sharing features within two days after the service's Feb. 9, 2010, launch, the company was hit Feb. 17, 2010, with the first of several Gmail user class action complaints.

In October 2010, a federal court gave preliminary approval of Google's move to settle the now-consolidated class actions for some \$8.5 million, *In re Google Buzz User Privacy Litigation*, No. 10-672 (N.D. Cal. Oct. 7, 2010)(15 ECLR 1688, 11/10/10).

EPIC, on behalf of itself and other privacy groups—the Center for Digital Democracy, Consumer Action, Patient Privacy Right, Privacy Activism, the Privacy Rights Clearinghouse, U.S. PIRG, and the World Privacy Forum—filed an objection to the settlement March 30.

In the submission of class counsel, none of the groups were designated to receive cy pres awards, as they have in similar matters concerning internet privacy. "Class Counsel proposed instead to distribute the majority of cy pres funds to organizations that are paid by Google to lobby for or consult for the company, which is the defendant in this matter," the groups contended.

That would be contrary to the interests of the class, they added.

As of April 1, the court had not given final approval to the proposed consent judgment.

In April 2010, a coalition of data protection officials from ten countries outside the United States sent a letter to Google, denouncing the firm's rollout of Buzz without what they said were adequate privacy protections.

It is unclear in light of the FTC's enforcement action whether international data protection authorities will continue to investigate Google's handling of Buzz or initiate formal enforcement action.

BY AMY E. BIVINS

The draft complaint is available at <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf>.

The proposed consent order is available at <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf>.

The analysis of the proposed settlement is available at <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzanal.pdf>.

The concurring statement by Commissioner Rosch is available at <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzstatement.pdf>.

EPIC's opposition to the settlement of class litigation at <http://pub.bna.com/eclr/epic.objection.pdf>.