Trans Atlantic Consumer Dialogue

Chairwoman Edith Ramirez
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
c/o **Commissioners Julie Brill,**
Terrell McSweeny, Maureen K. Ohlhausen,
Joshua D. Wright

Commissioner Billy Hawkes
Office of the Data Protection Commissioner,
Canal House
Station Road
Portarlington
Co. Laois, Ireland.

Tuesday, 29th July 2014

Dear Chairman Ramirez and Commissioners Brill, McSweeney, Olhausen, and Wright, and Commissioner Billy Hawkes:

We are writing to express deep alarm about the announcement on June 12, 2014, that Facebook is planning to collect the web browsing activities of Internet users for targeted advertising.[1] Facebook already installs cookies and pixel tags on users' computers to track browsing activity on Facebook.com and Facebook apps.[2] If Facebook is permitted to expand its data collection practices, those cookies and pixel tags will also track users' browsing activity on any website that includes a few lines of Facebook code.

The Transatlantic Consumer Dialogue (TACD), whose members include leading consumer NGOs from both the EU and U.S., has long advocated for the privacy of consumers on both sides of the Atlantic to be respected and safeguarded. A TACD resolution on behavioral advertising, adopted in 2011, specifically calls on regulators from both the EU and U.S. to protect consumer privacy, including "Investigate and take regulatory action … to address new threats to consumer privacy from the growth of real-time tracking and sales of information about individuals online activities … ."[3]

---

[1] Facebook, *Making Ads Better and Giving People More Control Over the Ads They See*, Jun. 12, 2014, http://newsroom.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see.
[2] Facebook, *Your Information and Facebook Ads*, https://www.facebook.com/help/769828729705201.
[3] Trans Atlantic Consumer Dialogue, "Resolution of behavioral Advertising," June 2011, https://www.surfer-haben-rechte.de/cps/rde/xbcr/digitalrechte/TACD_Resolution_on_Behavioral_advertising_-_FINAL.pdf.

We urge you to act immediately to notify the company that it must suspend its proposed change in business practices to determine whether it complies with current U.S. and EU law. Moreover, we ask you to publish your findings so that your investigations can be subject to a public assessment and review. Facebook has previously stated explicitly that it does not track user behavior around the Internet. When a forensic researcher discovered in 2011 that one of Facebook's cookies was transmitting his web browsing information to Facebook, the company issued a series of statements regarding user tracking. Facebook stated, "Facebook does not track users across the web. Instead, we use cookies on social plugins to personalize content (e.g. Show you what your friends liked), to help maintain and improve what we do (e.g. Measure click-through rate), or for safety and security (e.g. Keeping underage kids from trying to signup with a different age). No information we receive when you see a social plugin is used to target ads, we delete or anonymize this information within 90 days, and we never sell your information."[4]

Facebook's proposed data collection expansion directly contradicts its previous statements. Facebook's proposed use of pixel tags to track users offline is almost identical to its 2007 Beacon program.[5] Beacon similarly used 1x1 pixel GIF tags to track and transmit users' browsing history—on non-Facebook websites—to Facebook's own servers. Facebook users objected so strongly to Beacon that over 50,000 users signed a petition against the program within its first 10 days. Other users filed a class-action lawsuit against Facebook for privacy violations. Facebook abandoned the program during the course of the lawsuit and publicly apologized, admitting that the program had been a mistake.[6]

Facebook has now completely reversed its stance to the detriment of users of the service. Contrary to its prior representations, upon which users may have relied, the company will now routinely monitor the web browsing activities of its users and exploit that information for advertising purposes. The FTC should examine whether Facebook's change in business practices violates the consent order between Facebook and the FTC.[7]

Count I of the Order requires that Facebook "shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including…the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls."[8] However, Facebook has

---

[4] Emil Protalinski, *Facebook denies cookie tracking allegations*, ZDNET (Sept. 25, 2011), http://www.zdnet.com/blog/facebook/facebook-denies-cookie-tracking-allegations/4044.
[5] Louise Story and Brad Stone, *Facebook Retreats on Online Tracking*, NEW YORK TIMES (NOV. 30, 2007), http://www.nytimes.com/2007/11/30/technology/30face.html?_r=0.
[6] Barbara Ortutay, *Facebook to end Beacon tracking tool in settlement*, USA TODAY (Sept. 21, 2009), http://usatoday30.usatoday.com/tech/hotsites/2009-09-21-facebook-beacon_N.htm?csp=34.
[7] *See Facebook, Inc.*, FTC Docket No. C-4365 (2012) (Decision and Order), http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf [hereinafter FTC Facebook Consent Order].
[8] FTC Facebook Consent Order, § I.

misrepresented the amount of control users will be able to exert over their privacy settings. Facebook has stated that it will collect user data from third-party sites, but users will be able to "control which ads" they see.[9] This is misleading; the new data collection policy is unrelated to users' control over Facebook's ability to collect browsing information. In fact, the extent to which users can "control the privacy of any covered information maintained by" Facebook is determined by their third-party opt-out cookie. Users cannot control the data collection that results in targeted advertising; users can only control how much targeted advertising they must look at.

Facebook's data collection practices involve a closely woven relationship among Facebook, its advertising partners, data-broker companies, and various marketing applications services. The extent of this complex network of data collection practices is not immediately obvious to consumers; in fact, users must click through several different parts of the Facebook website to discover the existence of many of Facebook's data partners.

Count II of the Order requires that, "prior to any sharing of a user's nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s)," Facebook must make a "clear and prominent" disclosure, "specifically identify" the third parties, and obtain the "affirmative express consent" of the user.[10] Users' web browsing history is far outside the scope of the information users expect Facebook to collect. By giving third-party websites the means to track users' movements across the Internet, Facebook is able to associate users' Facebook activity with users' activity on third-party sites. The information that Facebook is able to collect from third parties creates the effect of a combined data profile of the user that "exceeds the restrictions imposed by a user's privacy settings." In fact, users must provide information to a third-party website in order to prevent Facebook from collecting third-party browsing information.

Users have not given "affirmative express consent" to a program when they must go to a separate website in order to opt out of the program. Once users arrive at the separate website, they must download an opt-out cookie to override the Facebook collection cookie. This has the effect of punishing the users who are most diligent about their privacy: the minute users clear their cookies, they also delete the opt-out preference. Thus, even consumers who work to exercise their ability to opt out must remain vigilant, even after taking the appropriate privacy precautions.[11] Moreover, as we have explained in our previous work, "Consumers should not be expected to

[9] FTC Facebook Consent Order, § I.
[10] FTC Facebook Consent Order, § II.
[11] As consumer advocate Jeff Fox has said, this process "puts the onus an every consumer to defend their own privacy." Jeff Fox, *What kind of privacy pipe is Facebook smoking? Consumers DON'T want targeted ads*, STATE OF THE NET (Jun. 17, 2014), http://stateofthenet.net/2014/06/what-kind-of-privacy-pipe-is-facebook-smoking-consumers-dont-want-targeted-ads.

understand the privacy dimensions of a 'custom targeting' system that uses wide-ranging data sets to determine 'the absolute value of each impression' for an advertiser. And even if they did, it is currently impossible for consumers to exercise control over how their data is collected and used."[12]

We also question whether Facebook is abiding by its commitment to "maintain a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers." In Count IV of the Order, Facebook also agreed to address the privacy risks associated with "the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks." However, Facebook has failed to address any of the risks associated with its collection of browser history information or the safeguards put in place to control the risks. Facebook has only provided users with an imperfect opt-out method, without addressing the potential failures of the third-party cookie to prevent Facebook's tracking activities.

Whatever determination the FTC made regarding the company's proposed change in business practices, the Commission should have made its review process public. In the past, the Commission has stated that privacy assessments by companies would be available to the public, subject to applicable laws. For example, after finalizing a consent order with Google that required similar independent assessments, the Commission wrote to EPIC and stated that "[t]o the extent permissible under law, the public may have access to the submissions required pursuant to the order."[13] Indeed, Google's initial compliance report was released without redactions.[14]

Furthermore, the experience of the international community provides evidence of the feasibility of such transparency. In 2009, the Canadian Privacy Commissioner conducted an investigation of Facebook's privacy policies and released a 113-page report that described in detail the findings of the investigation and the office's recommendations.[15] More recently, the Irish Data Protection Commissioner's investigation into Facebook produced a 150-page report and 77 pages of "technical

---

[12] Transatlantic Consumer Dialogue, Resolution on Behavioral Advertising, Doc. No. INFOSOC 45-11 (Jun. 2011), *available at* http://test.tacd.org/wp-content/uploads/2013/09/TACD-INFOSOC-45-11-Behavioral-advertising.pdf.

[13] Letter from Donald S. Clark, Secretary, Fed. Trade Comm'n, to Marc Rotenberg et. al (Oct. 13, 2011), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzepic.pdf.

[14] Letter from Sarah Mathias, Associate General Counsel, Fed. Trade Comm'n, to Ginger McCall, Director, EPIC Open Gov't Program (Feb. 15, 2012), *available at* https://epic.org/privacy/ftc/google/EPIC-FTC-Google-Compliance-Reply-02-17-12.pdf .

[15] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. (2009), http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm#complaint.

analysis" that were made publicly available.[16] The Irish DPA's report on the audit promised EU consumers that Facebook was in compliance with better privacy practices, and the company made a series of commitments to the DPA. In light of that, we question how this new vast expansion of the social network's data collection and user profiling could have been allowed to go forward.

The lack of adequate review of Facebook's proposed changes also calls into question the effective use of the FTC's Section 5 authority and its commitment to enforcing Safe Harbor. A 2010 WPF report analyzed the US-EU Safe Harbor Framework, finding that "[u]nlike most other privacy self-regulatory efforts the Safe Harbor Framework continues to exist, largely because of the government role."[17] Lack of genuine enforcement mechanisms has decreased industry compliance, and "evidence [now] suggests that the number of companies not in compliance [with the Framework] has increased over time."[18]

We respectfully call on you to take the appropriate action, order Facebook to reverse its new data collection practice, and develop public accountability mechanisms for the company to ensure it is complying with required privacy practices.

Cordially,

Kostas Rossoglou
Senior Legal Officer, BEUC (The European Consumer Organisation)
EU Co-Chair of the TACD Information Society Policy Committee

Jeffrey Chester
Executive Director, Center for Digital Democracy
U.S. Co-Chair of the TACD Information Society Policy Committee

On behalf of the TACD Information Society Policy Committee.

[16] *See* DATA PROTECTION COMM'R, REPORT OF AUDIT (2011), http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf .
[17] *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, 4.
[18] *Id.* at 21.