



Comments of the World Privacy Forum regarding the Proposed FTC Facebook Settlement, Facebook File No. 092 3184

Via <https://ftcpublic.commentworks.com/ftc/facebookconsent>

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex D)
600 Pennsylvania Avenue NW
Washington, DC 20580

December 30, 2011

Dear Secretary and Commissioners,

Thank you for your hard and persistent work on the Facebook case, and congratulations for bringing this case to a proposed settlement.¹ The World Privacy Forum² recognizes the effort this settlement took, as well as its thoughtfulness and supports your work. We find many good things about the proposed settlement. Our comments below bring forward points of support and several substantive concerns with the settlement, which we submit with great respect, knowing how hard the FTC has worked on this case.

Our comments center on the following issues:

1. The definition of *covered information* needs to include financial information with particularity.
2. The final settlement needs to require that Facebook host a dedicated, formal and prominent consumer privacy complaint mechanism for users at the Facebook site.
3. The length of time for the retention and transmission of consumer complaints to the FTC regarding privacy complaints at Facebook needs to be expanded in the proposal from 6 months to 2 years.
4. The FTC's decision in the 2004 Gateway Learning Corp. case set a precedent for disgorgement of funds in cases where acts regarding privacy policies were found to be unfair. The Facebook settlement needs to follow this important precedent and require disgorgement of funds from Facebook pursuant to the income Facebook gained by violating its privacy promises.
5. In order to address consumer harm in this case, the settlement must require Facebook

¹ <<http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf>>.

² The World Privacy Forum is a non-profit public interest consumer education and research group based in San Diego, CA. We focus on a range of privacy issues, including Internet privacy. See <<http://www.worldprivacyforum.org>>.

to return its users' profile settings to what they were prior to the 2009 reduction of the privacy settings.

6. The proposed settlement lacks any mention of Facebook Payment, an important Facebook subsidiary, and by default the settlement omits any controls on the workings and interminglings of consumer financial data resulting from the interaction of Facebook's payment system with its social networking site and third parties. This is a substantial oversight.

7. The audits required in the proposed settlement need to be made affirmatively public without undue redaction, not just available via FOIA requests which are subject to numerous exceptions.

A discussion of each of these points follows.

1. The Definition of PII needs to include financial information with particularity.

In the proposed settlement, the FTC has proposed that "covered information" be defined as:

"Covered information" shall mean information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above."

We support the items that are included in the definition. We see some holes, though.

We request and indeed urge the Commission to include financial information very specifically in this definition, including numbers such as credit card numbers, debit card numbers, and/or numbers linked to financial accounts such as PayPal, bank accounts, and so forth. The Commission has omitted from this definition Social Security Numbers. SSNs were included in the covered language in the FTC's 2004 Gateway Learning Corp. decision, and we agree with the inclusion of SSNs in that case and think it is a necessary inclusion in this case as well.³

In the Facebook case there is a need to include both financial information and SSNs in the "covered information" definition due to the workings and interactions of Facebook Payment with Facebook's social networking site. The two are increasingly intermingled, thus giving rise to a great deal of financial information being transacted in direct connection with a user's social graph. See section #6 for further discussion of Facebook

³ In re Gateway Learning Corp, 138 F.T.C. 443, File No. 042-3047 (2004).
<<http://www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf>>.

Payment interactions with Facebook social graphs. Inclusion of financial information will go far in putting Facebook on clear notice regarding this area of data responsibility.

2. The final settlement needs to require that Facebook host a dedicated, formal and prominent consumer privacy complaint mechanism for users at the Facebook site.

Facebook’s current privacy feedback mechanisms are not conducive to gathering consumer complaints about Facebook’s privacy problems. We request that as part of the settlement that Facebook be required to set up a prominent consumer privacy complaint page that has unambiguous wording regarding collection of complaints, adequate publicity, staff support, and meaningful response from the company. The proposed settlement does not currently include a specific requirement for Facebook to institute a dedicated, formal consumer feedback mechanism to voice privacy complaints. This needs to be included.

Currently, Facebook’s privacy feedback mechanism is insufficient.

First, users click a link available near the end of the Facebook Help Center page, “Send a Suggestion about Privacy” (*Figure 1*).

Users are then deposited at a long page about general Suggestions and Feedback (*Figure 2*). There is still no mention of lodging a privacy *complaint*. There is a link that states: “share a suggestion about privacy settings, privacy options, and privacy policies here.” The choice of words here is unhelpful to consumers who are attempting to find a place to specifically complain.

Finally, users clicking on this link arrive at a form that does not have the word “complaint” anywhere on it (*Figure 3*). The Facebook privacy suggestion form also states there will not be a direct response. This is not sufficient for collecting *consumer complaints* about privacy, and in fact, we believe this three-click-minimum process and “suggestion” language deliberately discourages consumers from lodging a complaint. We reiterate that the word *complaint* never shows up on any of these forms or links.

Here is what the process looks like for consumers:

Click one:

Your Feedback

- [Post a question in the privacy forum](#)
- [Something is not working](#)
- [Send a suggestion about privacy](#)

Was this information helpful?

*Figure 1 Facebook's Privacy "send a suggestion" link at Facebook's Help Center
<https://www.facebook.com/help/?page=183300361718935>.*

Click two:

Submit feedback on privacy and safety

 [Privacy](#)

Share suggestions about privacy settings, privacy options and privacy policies here. If you are experiencing a security problem or abuse, visit the [Security](#) section for more information and to resolve your problem.

*Figure 2: Facebook's Suggestion Page
<https://www.facebook.com/help/?page=183300361718935>*

Click three:

Your Privacy Suggestion

This form is for suggestions about Facebook's privacy settings and policies.

If you think your account was hacked, [get help](#).
If you want to report abuse on Facebook, [learn more](#).

Subject:

More Details:

Note: While Facebook welcomes suggestions you submit using this form, we are unable to respond to them directly. Keep in mind that all submitted suggestions are governed by our [terms](#) (see section 2.5).

For more privacy and security information, check out our [Privacy Guide and Safety Center](#).

Figure 2 Facebook's privacy suggestion form at https://www.facebook.com/help/contact.php?show_form=ui-privacy2.

We note that in the proposed settlement, the FTC has already required Facebook to “clearly and prominently disclose to the user, separate and apart from any “privacy policy,” “data use policy,” “statement of rights and responsibilities” page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user” prior to any sharing of a user’s nonpublic user information with any third party which materially exceeds the restrictions imposed by a user’s privacy settings.

We support the clear language the FTC used here. Wherever this “clear and prominent disclosure” is going to occur would be a very good location to *also* clearly and prominently disclose to the user in the same manner a consumer complaint form and procedure to address privacy problems. We believe the word *complaint* should be used on the Facebook form to facilitate consumer feedbacks regarding complaints, not just suggestions.

Consumers have consistently voiced frustration in their inability to provide feedback to

Facebook over privacy complaints, most recently in the comments posted to the FTC in response to the proposed settlement. This issue needs to be much more specifically addressed in this settlement, or the risk is that current mechanisms will stay in place with the same wording.

3. The length of time for the retention and transmission of consumer complaints to the FTC regarding privacy complaints at Facebook needs to be expanded in the proposal from 6 months to 2 years.

The proposed settlement states:

IT IS FURTHER ORDERED that Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

....

B. for a period of six (6) months from the date received, all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;

We support this provision in the proposal. But we also argue that six months is not nearly a sufficient amount of time for a site of the magnitude of Facebook to institute changes, publicize those changes, then get feedback from consumers and corral consumer complaints. Two years is a much more realistic time frame. Currently, Facebook does not even have a clear consumer complaint form. (See Figures 1-3 in the previous section.) We urge and request the FTC to expand the mandates regarding Facebook consumer complaints for a period of two years. Please also generally see our earlier request in #2, that Facebook needs to be required to provide a dedicated consumer complaint mechanism via its site.

4. The FTC's decision in the 2004 Gateway Learning Corp. case set a precedent for disgorgement of funds in cases where acts regarding privacy policies were found to be unfair. The Facebook settlement needs to follow this important precedent and require disgorgement of funds from Facebook pursuant to the income Facebook gained by violating its privacy promises.

In the 2004 Gateway Learning Corp. case, the FTC set a clear precedent for disgorgement where a company has retroactively applied privacy policy changes.⁴ In the Gateway case, the FTC settlement required Gateway to divulge its gains made pursuant to breaking its

⁴ FTC File No. 042-3047.

privacy promises.⁵ In the case of Facebook, no such disgorgement has been required, despite the clear precedent the Gateway Learning case set. Facebook affects more individuals and affects them more acutely in areas with the potential for direct harm such as finance and employment. The lack of disgorgement is an error and needs to be reversed. Companies get a message that if they commit privacy misdeeds, they may not face the fiscal consequences of substantial disgorgement of revenue.

In 2004, the FTC charged in its Gateway Learning complaint:

13. As described in Paragraphs 7 - 9, Respondent posted a revised privacy policy containing material changes to its practices that were inconsistent with Respondent's original promise to consumers. Respondent retroactively applied such changes to personal information it had previously collected from consumers. Respondent's retroactive application of its revised privacy policy caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. The practice was, and is, an unfair act or practice.

The Facebook case in question follows clearly in the precedent this case set. In its current discussion of the Facebook settlement for consumers, the FTC wrote:

Privacy changes – unfair practices. Furthermore, according to the FTC, by designating certain user profile info as public when it had previously been subject to more restrictive privacy settings, **Facebook overrode users' existing privacy choices. In doing that, the company materially changed the privacy of users' information and retroactively applied these changes to information that it previously collected.** The FTC said that doing that without users' informed consent was an unfair practice, in violation of the FTC Act. (*emphasis added*) <http://onguardonline.gov/blog/ftc's-settlement-facebook-where-facebook-went-wrong>

This paragraph above is a clear, concise description of count 3 of the FTC's complaint, which reads:

Count 3

29. As described in Paragraphs 19-26, by designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information

⁵ In the 2004 Gateway case, the FTC found that Gateway had made "false and misleading representations" in its privacy policy regarding users personally identifiable information. The FTC ordered Gateway to pay \$4,608 to the United States Treasury.

private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent, in a manner that has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers. This practice constitutes an unfair act or practice.

It is exceptionally clear that The Facebook case follows on the precedent set in the 2004 Gateway Learning case. The language in the two counts in the two cases could not be clearer as to this fact.

We urge the FTC to reopen this issue and to reconsider the consumer harms from Facebook's bad actions.

First, there is the fact of the magnitude of the sheer numbers of individuals affected: hundreds of millions of users who posted their information privately had it made public retroactively and without their consent.

Second, consider the magnitude of the further harms that ensued as a result of this action. After the opening of the consumer profiles, companies such as Rampleaf⁶ and Social Intelligence scraped that information and used it for a variety of purposes, including in Social Intelligence's case, employment decisions about the users. The FTC is well aware of Social Intelligence; the Commission sent an important and thoughtful letter⁷ to Social Intelligence in May 2011 noting that the information Social Intelligence collected from Facebook⁸ was subject to the Fair Credit Reporting Act:

“As you know, the staff of the Federal Trade Commission's Division of Privacy and Identity Protection has been investigating Social Intelligence Corporation ("Social Intelligence"), an Internet and social media background screening service used by employers in pre-employment background screening. The reports sold by Social Intelligence include public information gathered from social networking sites. Our investigation aimed to determine the company's compliance with the Fair Credit

⁶ Rampleaf sold consumer information culled from Facebook and other sources to financial institutions which then used the data for “marketing purposes,” for example, to target promotional offers on credit cards. See Ginny Miles, *Can Your Online Life Ruin your Credit?* PC World, March 23, 2010.

<http://www.pcworld.com/article/192207/skeptical_shopper_can_your_online_life_ruin_your_credit.html>. See also David Goldman, *Rampleaf is selling your identity*, Oct. 21, 2010. <<http://money.cnn.com/2010/10/21/technology/rampleaf/index.htm>>.

⁷ Federal Trade Commission Letter to Social Intelligence, May 9, 2011. <<http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf>>.

⁸ See for example, Kashmir Hill, *Social Media Background Check Company Ensures that Job-Threatening Facebook Photos are Part of your Application*, Forbes, June 20, 2011. <<http://www.forbes.com/sites/kashmirhill/2011/06/20/now-your-embarrassingjob-threatening-facebook-photos-will-haunt-you-for-seven-years/>>. See also: <http://www.pcmag.com/article2/0,2817,2387315,00.asp>.

Reporting Act ("FCRA").

Social Intelligence is a consumer reporting agency because it assembles or evaluates consumer report information that is furnished to third parties that use such information as a factor in establishing a consumer's eligibility for employment. Consumer reporting agencies must comply with several different FCRA provisions, and *these compliance obligations apply equally in the social networking context.*" (emphasis ours.)

That Facebook's bad actions made public the user data that Social Intelligence was then able to collect and use for pre-employment background checks speaks to the very substantial and consequential privacy concerns users have in this matter. How many people did not receive an offer of employment because of Facebook's bad act? The consumer harm in this case is substantial as to the number of consumers affected and as to the nature of the harm.

We also urge the FTC to consider Facebook's willfulness in this bad behavior. It is silly to postulate that Facebook was not apprised of nor aware of the privacy policy issues and the Gateway Learning precedent. Facebook has exceptional and deep legal staffing, and has employed or contracted with some of the best legal experts in the country. This was as true in 2009 as it is today. Retroactively altering a privacy policy toward more information sharing is a Privacy 101 no-no.

We request that the FTC consider the impact of the *new* precedent that the FTC sets by not following the Gateway Learning precedent in the Facebook case. The lack of disgorgement (and the lack of real consumer redress by way of returning the privacy settings to their original state prior to the bad act) sends a deleterious message to contemporary and future data-rich companies: do as you please, then apologize later.

Commissioners, much burden is being placed on the FTC for enforcement in the digital world. Many new self-regulatory schemes and codes of conduct programs have as their primary enforcement mechanism FTC enforcement of Section 5 of the FTC Act. In this clearly-argued case that the FTC has brought against Facebook, disgorgement is warranted and indeed required to address consumer harm. We also believe that following the 2004 Gateway Learning precedent is an extremely important aspect of retaining the "big stick" power the FTC has in Section 5 enforcement actions. Please see also the next section discussing the need to return users' profile settings to the state prior to the bad act.

5. In order to address consumer harm in this case, the settlement must require Facebook to return its users' profile settings to what they were prior to the 2009 reduction of the privacy settings.

The proposed settlement does not require Facebook to roll its privacy controls back to users' previous levels prior to Facebook's bad acts. When Facebook broke the law in retroactively altering users' privacy settings, it opened user profiles and additional user

data to numerous third parties, including Rapleaf and Social Intelligence. This inappropriate retroactive change broke the law and it harmed consumers. The retroactive changes need to be specifically addressed as part of this settlement.

We urge the FTC to **require Facebook to return users' settings to their original defaults prior to Facebook's bad acts**. Otherwise, Facebook still gets to have its way and keep the diminished privacy settings. This is not a correct outcome. It fundamentally encourages information-rich companies to behave badly and ask for public forgiveness later (while meanwhile making no changes that restore or repair the consumer harm.)

Commissioners, we view this roll-back as the key to a fair settlement. The company should not be allowed to move forward with its new privacy settings just because several years have passed since the changes. The decision to rollback the privacy settings to prior user defaults needs to be made in order to address the consumer harm and to address the correction of Facebook's bad acts. The proposed settlement does address some of the issues, but indirectly. Rolling back the settings to prior levels directly addresses the harm issue for consumers.

6. The proposed settlement lacks any mention of Facebook Payment, and by default the settlement omits any controls on the workings and interminglings of the financial PII resulting from the interaction of Facebook's Payment system with its social networking site.

No specific mention of information relating to consumers' financial transactions or consumers' financial information has been made in the proposed settlement. This is a significant oversight, and we urge the Commission to add consumer-protective language in this area to the settlement.

Facebook has become an important player in the payments space.⁹ Since 2009, analysts have been tracking the growth of Facebook credits from merely being used as a quaint credit to pay for materials on, for example, Farmville, to now a full vehicle for financial transactions.¹⁰

⁹ "Facebook and Google are poised to challenge the banking industry in online payments. Both Internet giants have developed alternative payment networks that observers say could come to undermine the likes of MasterCard and Visa," See: Jeremy Quittner, *Facebook and Google encroach on Banks Turf*, American Banker, May 1, 2011. <http://www.americanbanker.com/magazine/121_5/facebook-and-google-encroach-on-banks-turf-1036012-1.html?zkPrintable=true>.

¹⁰ In March 2011, Facebook opened a new payment unit, Facebook Payments. It has been growing rapidly and expanding in unforeseen ways. Many announcements clustering from October 2011 to December 2011 have been coming forward surrounding the financial integration of Facebook Payments to Facebook's social media site – and users' data and social graphs. See *Facebook payments: think virtual*, CNN Tech, May 26, 2009 <http://articles.cnn.com/2009-05-26/tech/cnet.facebook.payments_1_facebook-platform-paypal-virtual?_s=PM:TECH> for details

Facebook now has PayPal integration¹¹ that allows users to make person-to-person payments over Facebook. Facebook also now has integration with Dwolla.¹² Dwolla allows users to link their checking or savings account to Dwolla, and then their Facebook social networking contacts are imported, allowing users to send money to their Facebook friends.¹³ Facebook is also facilitating point-of-sale transactions.¹⁴ For example, Warner Brothers Digital Distribution now accepts Facebook Credits for movie purchases and rentals. Users can receive streaming movies without ever leaving Warner Brother's Facebook page.¹⁵ This is already happening, yet when Facebook recently changed its payment terms in October 2011, it did not make an effective or complete discussion or disclosure of integration of user payment information with profile information, nor how that information will be used. *See* https://www.facebook.com/payments_terms.

We predict that social commerce as mediated through Facebook is going to be a whole issue going forward; it already is. But it will get bigger. This particular area has the flavor of the Wild West; for example, we note that Dwolla apparently does not have a privacy policy as of yet, and we note that Facebook is apparently allowing Dwolla to move forward with integration. There is a pronounced lack of oversight over the integration of consumers' financial data with social graph data. Someone, somewhere has to take responsibility.

The proposed Facebook settlement needs to address the financial information of consumers with particularity in order to prevent future bad acts by Facebook regarding consumers' financial information. If Facebook were to retroactively open up or share consumers' financial information in a way that was different than it promised, the effects would be notable. We believe this is an area that warrants further review by the Commission prior to making the settlement final. We reiterate our request that the Commission include financial information in the definition of covered information in the settlement.

7. The audits required in the proposed settlement need to be made public affirmatively, not just available via FOIA requests which are subject to exemptions.

emerging in 2009. *See also Facebook Creates Payments Subsidiary*, All Facebook, March 22, 2011 < <http://www.allfacebook.com/facebook-creates-payments-subsidiary-2011-03>>.

¹¹ Daniel Wolfe, *PayPal adds Facebook Payment App*, American Banker, Nov. 18, 2011. <http://www.americanbanker.com/issues/176_225/paypal-facebook-gift-1044193-1.html>.

¹² Dwolla home page, <<https://www.dwolla.com/>>.

¹³ Sarah Kessler, *Dwolla Loans Users \$500 to Make Instant Payments Through Facebook and Twitter*. Mashable, December 15, 2011. <<http://mashable.com/2011/12/15/dwolla-loans-users-500-to-make-instant-payments-through-facebook-and-twitter/>>. *See also* <<http://mashable.com/2010/12/22/dwolla/>>.

¹⁴ Lauren Fisher, *Facebook To Change Social Commerce As They Roll Out Credits To Websites*, October 24, 2011.

¹⁵ *Signaling Possible Plans Beyond Credits, Facebook Sets up a Payments Unit*, Mar. 10, 2011 <digital transactions, <http://digitaltransactions.net/news/story/2965>>

The World Privacy Forum supports the requirement for audits. The audits need to be made public affirmatively without undue redaction to ensure transparency to the public. We are aware that the audits can be requested via Freedom of Information Act (FOIA) requests made to the Commission. However, audits received through FOIA requests are likely be heavily redacted as allowable via FOIA Exemption 4, which covers trade secrets and commercial or financial information, among other information.¹⁶ This is a tricky area to find balance, and we recognize that. We believe that the public is better served by more transparency in this situation given the magnitude of the impact of Facebook and the privacy interests of consumers regarding their personally identifiable information and social graph data. We note that the VZBW has also made a similar request, and we expect more requests for this at the end of the public comment process.¹⁷

Thank you for the opportunity to comment on this important settlement.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org

¹⁶ Freedom of Information Act Guide, US Department of Justice, Exemption 4. May 2004. <<http://www.justice.gov/oip/exemption4.htm>>.

¹⁷ <<http://www.ftc.gov/os/comments/facebookconsent/00041.html>>.