ConsumersUnion®

THE ADVOCACY DIVISION OF CONSUMER REPORTS

June 27, 2018

Maneesha Mithal, Associate Director
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Dear Ms. Mithal,

We, Consumers Union, the advocacy division of Consumer Reports,[1] write to draw your attention to a report by the Norwegian Consumer Council (NCC)[2] released today that examines the information and consent dialogs that Microsoft, Google, and Facebook presented to their users as part of recent updates to respond to the General Data Protection Regulation (GDPR). The report, entitled *Deceived by Design*, concluded that while these dialogs did present users with more granular choices for consenting to uses of their personal data, the companies at times employed various tactics to nudge or push consumers towards giving consent to sharing as much data for as many purposes as possible. These tactics included privacy-intrusive default settings, giving users an illusion of control; "dark patterns"[3] such as hiding privacy-friendly choices; and presenting the user with take-it-or-leave-it choices. We believe these findings will be of interest to you as you evaluate how the Federal Trade Commission (FTC) can best safeguard consumer privacy interests in the U.S., and the proper role that consent should play in data protection. Further, we request that the FTC analyze whether these practices conform with the obligations these companies have voluntarily undertaken by certifying compliance with the E.U.-U.S.

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its advocacy work in the areas of privacy, telecommunications, financial services, food and product safety, health care, among other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million members and publishes its magazine, website, and other publications.

[2] *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMERS COUNCIL (June 27, 2018), *available at* https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/.

[3] Dark patterns are "…features of interface design crafted to trick users into doing things that they might not want to do, but which benefit the business in question." Nerdwriter1, *How Dark Patterns Trick You Online*, YouTube (Mar. 28, 2018), https://www.youtube.com/watch?v=kxkrdLI6e6M; *see, also*, Dan Schlosser, *LinkedIn Dark Patterns*, MEDIUM (June 5, 2015), https://medium.com/@danrschlosser/linkedin-dark-patterns-3ae726fe1462.

Privacy Shield Framework.[4]

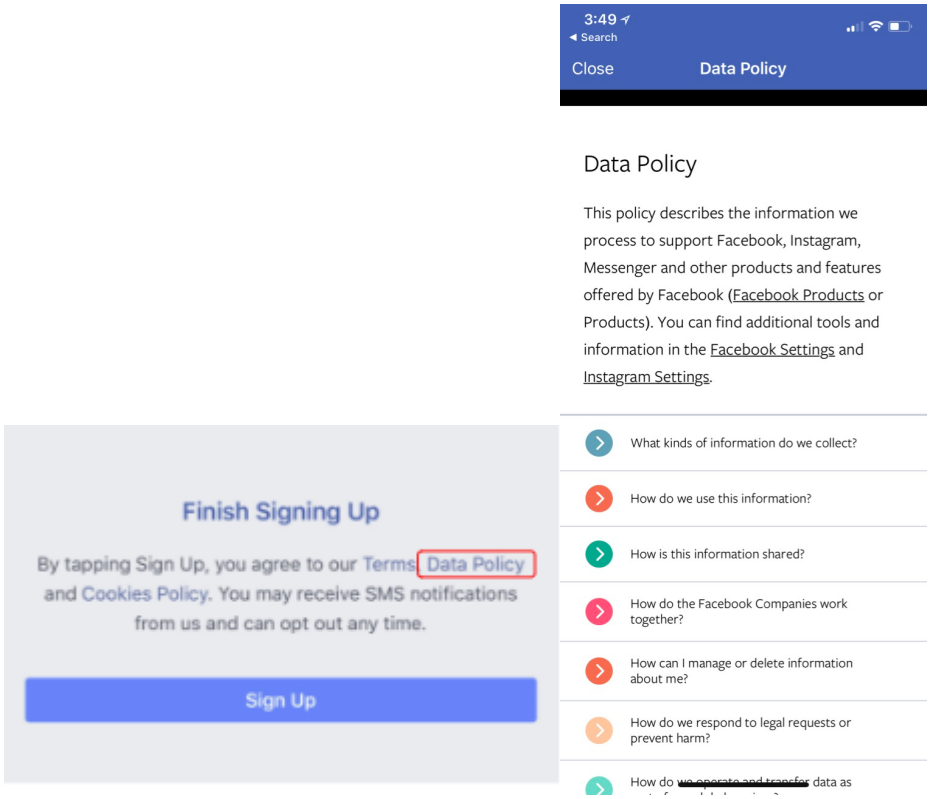
Based on the research completed by the NCC for its *Deceived by Design* report, Consumers Union conducted its own research to examine what U.S.-based users were presented with when they signed up for certain accounts. Our research found that Facebook uses similar interfaces to steer users to the least private options when creating a Facebook account, despite proclaiming that users are "in control of their data." Further, we uncovered a defective and potentially misleading setting on the Facebook iOS App, displaying an advertising setting as "Not Allowed" when our research showed that it is actually "Allowed."

These findings, along with the NCC's, show that Facebook is using coercive patterns involving the default settings, ease of use, and framing of options when a user tries to manage their privacy settings on the platform. First, and as illustrated further below, Facebook uses tactics that nudge the user to agree to default settings that permit the use of the user's personal information. These tactics include: (1) barring a user from making changes to their privacy settings before signing up for an account, (2) directing the user through a confusing dashboard of policies to learn how to change their settings, and (3) requiring the user clicks and/or swipes multiple times to alter their advertising preferences. Second, Facebook makes the privacy-protective option more cumbersome by requiring many more clicks and/or swipes for a user to limit the collection of their personal information. Third, Facebook frames various privacy settings to only focus on the benefits—and not the disadvantages—of turning on or allowing settings that collect and disseminate personal information.

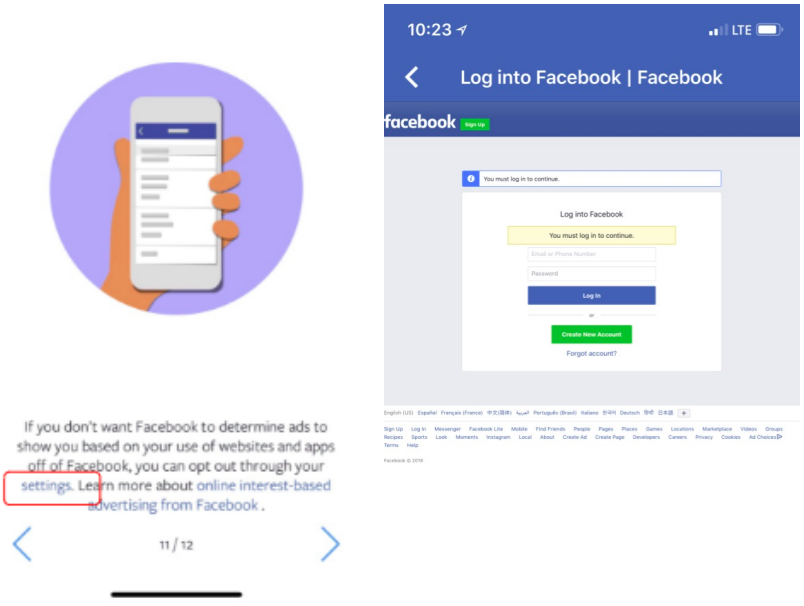
Here is a more detailed description of the practices we found: When a user signs up for a Facebook account, the user must agree to the platform's default advertising settings before creating an account. Facebook's default advertising settings are enabled to allow advertisers to access a user's personal information. If the user attempts to change settings via the Facebook mobile application before completing the sign-up process, they are redirected to a confusing array of policies which ultimately leads the user back to an interface that requires them to sign-up before making changes.

[4] *Privacy Shield Framework*, U.S. DEPT. OF COMMERCE, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg (last visited June 25, 2018).

The "Data Policy" screen a user is directed to when trying to change their settings before signing up for Facebook

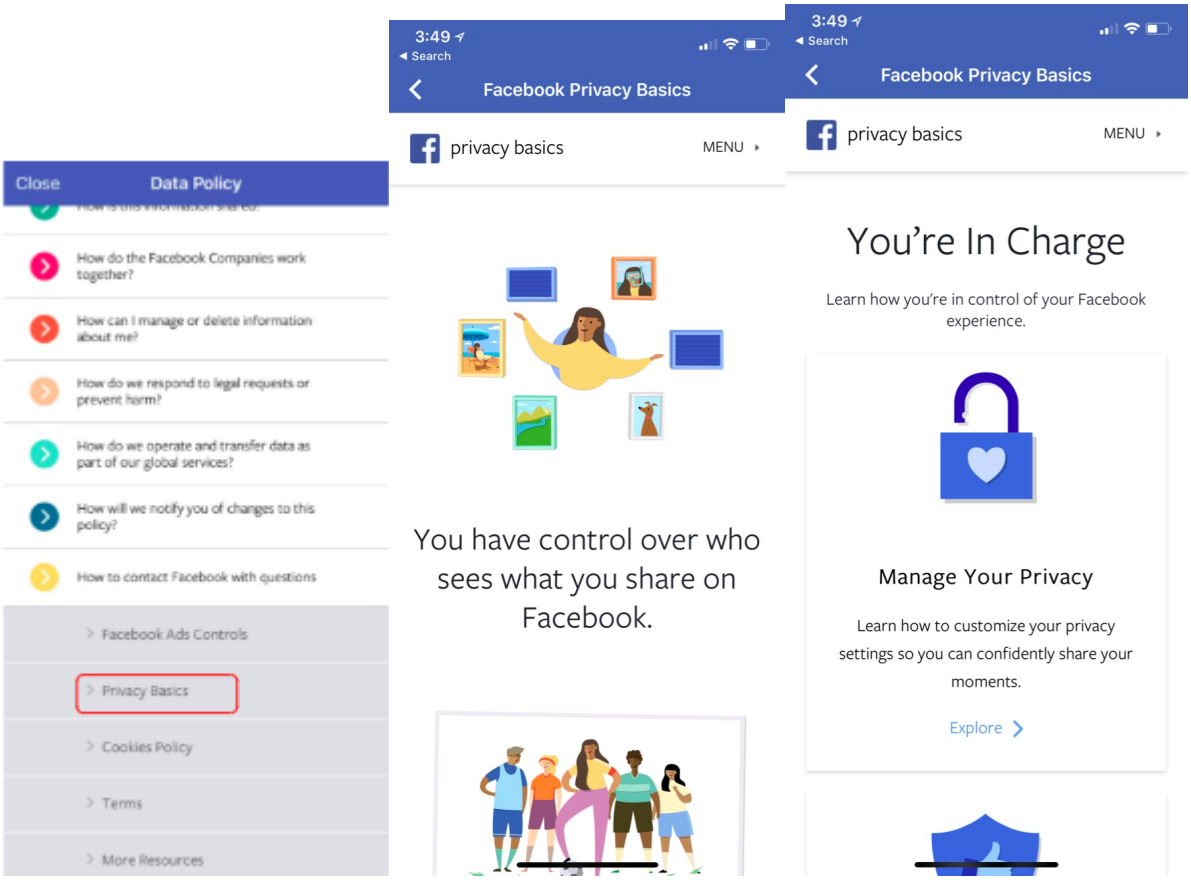


Display after a user clicks/swipes through 16 screens on Facebook's Data Policy trying to change their ad preferences (left) and the next screen requiring they create an account (right)



Furthermore, when the user is navigating through this "Data Policy," Facebook advertises that the user has "control over who sees what [they] share on Facebook]," and is "in charge…of [their] Facebook experience."

Screencaptures within the Data Policy demonstrating that Facebook tells users they are "in charge" of their privacy before signing up for Facebook

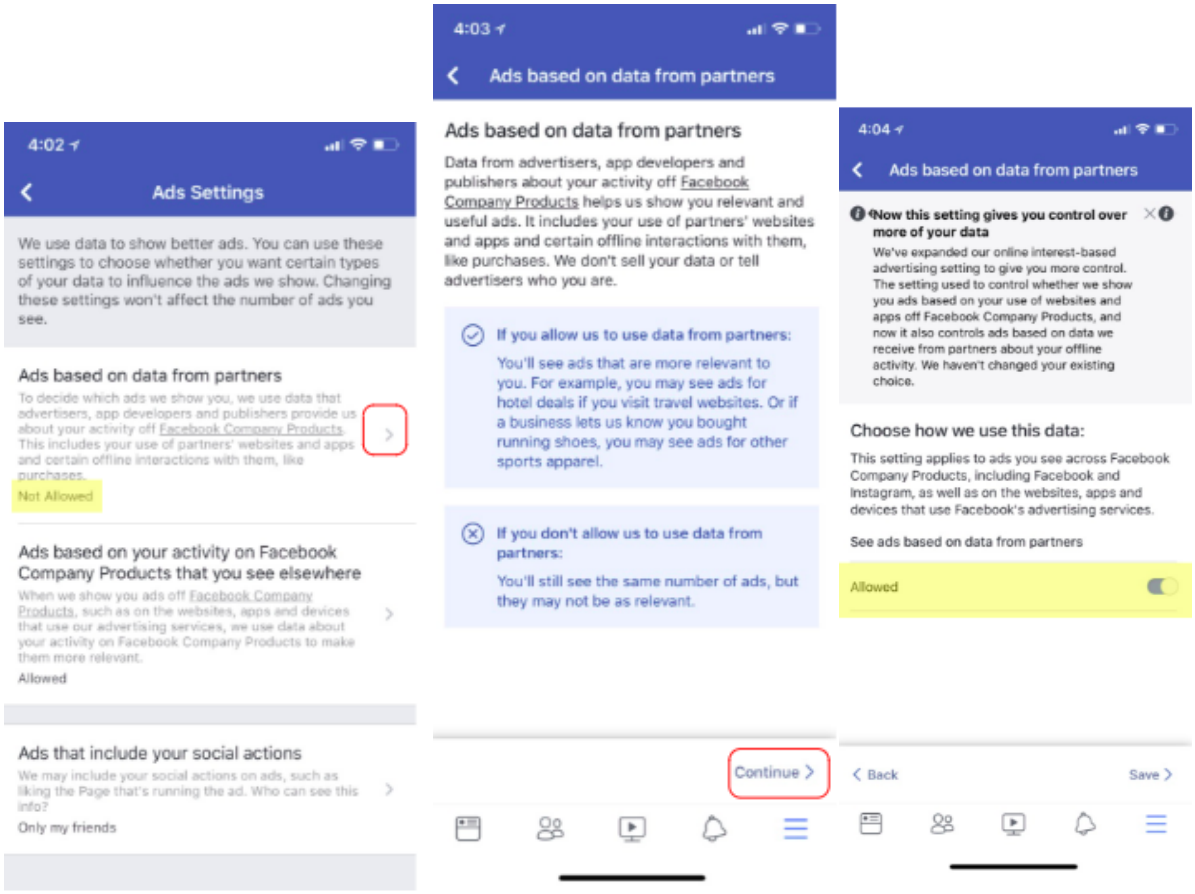


This gives the user an illusion of control over their information while Facebook employs interface and design tactics that lead users to agree to default settings and surrender their personal information. Ultimately, it takes the user who tries to change the default ad settings before signing up 21 clicks and/or swipes to navigate to a page where they can do so, and they only can get there after creating an account.

When the user does complete the sign-up process, Facebook immediately encourages them to build a profile and release more of their personal information before navigating to their settings to change preferences. Facebook makes it difficult to bypass or skip many of these steps. These practices are a direct contrast to those of other major digital services, such as Google, which allow users to change many of their privacy settings before creating an account.

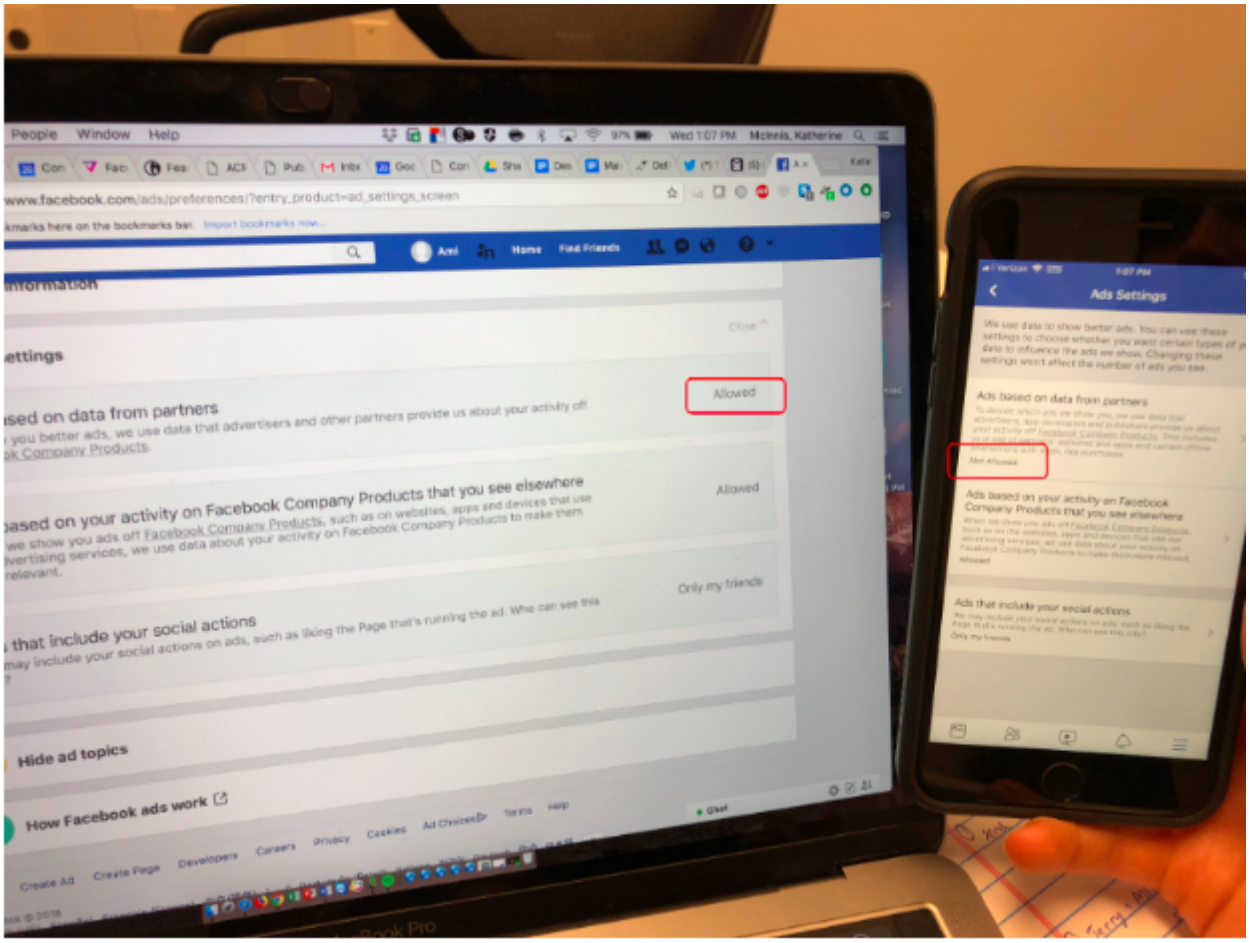
Additionally, a defective and misleading ad setting on the Facebook iOS App v177.0 initially displays to the user that one of their two ad settings, "Ads based on data from partners," is "Not Allowed" by default. However, when the user clicks into this setting for more information, the settings is switched on to "Allowed."

Facebook Ads Settings page after signing up for an account and not changing the defaults

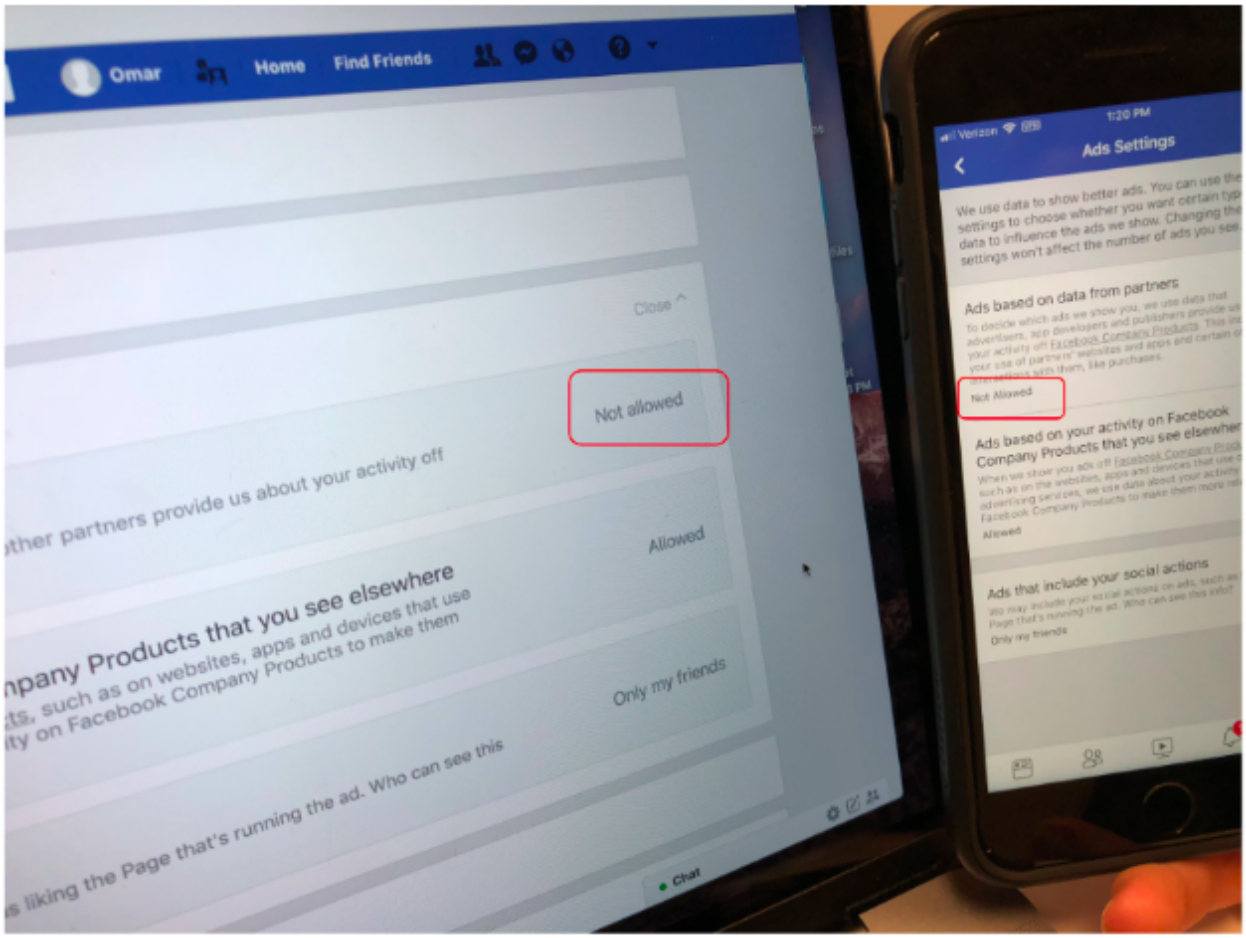


Our research demonstrated that this setting initially and directly displays as "Allowed" by default on Facebook's browser interface and Android App v177.0.0.57.105. Because of these discrepancies, Consumers Union is unsure as to what the default ad setting for this feature is. Most concerningly, iOS users who do not want this setting to be allowed would not attempt to switch this setting off if it is initially displayed as "Not Allowed." Lastly, we found that the "Ads based on data from partners" setting changes from "Allowed" to "Not Allowed" if the user, who made an account in a browser, simply logs into the iOS Facebook app.

The different default settings for "As based on data from partners" for browser (left) and mobile (right)



Settings change without a user updating them: Browser screen after refreshing the browser (right) and the same profile on the iOS app (right)



We conclude that, most likely, the default setting for this ad preferences control is "Allowed"/on, and that the indication in iOS apps that the setting is off by default is incorrect.

We are concerned that these ad setting discrepancies could mislead consumers into believing that certain privacy protections are "on" when they "off," and thus disable them from making informed choices about their data. If so, they could potentially constitute violations of the FTC Act and/or the FTC's 2011 consent decree.[5] We therefore urge the FTC to investigate these practices as it also examines Facebook's use of dark patterns discussed above and in the NCC report. Further, we urge the FTC to provide more guidance about the use of dark patterns to industry as a whole, to ensure that when consumers make privacy choices, such choices are fully

[5] *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, FED. TRADE COMM'N (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

informed and meaningful.

Thank you for your attention to this matter. If you have any questions, please do not hesitate to contact me at katie.mcinnis@consumer.org or 202.462.6262.

Sincerely,

Katie McInnis
Policy Counsel

Gabrielle Rothschild
Privacy Intern

Consumers Union
Suite 500
1101 17th Street NW
Washington, DC 20036

Cc: Andrew Smith, Director
Bureau of Consumer Protection