

June 27, 2018

Chairman Joseph Simons
Commissioner Maureen K. Ohlhausen
Commissioner Noah Joshua Phillips
Commissioner Rohit Chopra
Commissioner Rebecca Kelly Slaughter
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: How tech companies nudge users to choose less privacy-friendly options

Dear Chairman Simons and FTC Commissioners:

On behalf of leading consumer privacy organizations in the United States, we urge you to investigate the misleading and manipulative tactics of the dominant digital platforms in the United States, which steer users to “consent” to privacy-invasive default settings.

As the new General Data Protection Regulation (GDPR) is implemented across Europe, users of digital services have been asked to consent to new privacy settings through numerous “pop-up” messages. As illustrated by a report published today by the Norwegian Consumer Council, the pop-up messages used by Google and Facebook manipulate users into accepting settings that will disclose personal information far beyond what is needed to use the service.

The report, entitled “Deceived by Design,” details how companies employ numerous tricks and tactics to nudge consumers toward giving consent to disclosing as much data as possible for as many purposes as possible.* These tactics include:

- **Privacy-intrusive default settings.** Research has shown that users rarely change pre-selected settings. In many cases, both Facebook and Google have set the least privacy friendly choice as default.
- **Illusion of choice.** Companies employ take-it-or-leave-it privacy settings, obscuring the fact that users have very few actual choices and disclosure of personal information is a condition of using the service. The feeling of control may also persuade users to disclose more information.
- **Hiding privacy-friendly choices.** Privacy-friendly choices require significantly more clicks to reach and are often hidden away.

* Norwegian Consumer Council *Deceived by Design*, (June 27, 2018), available at <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design>

- **Deceptive design choices.** The disclosure of personal data and the use of targeted advertising is often presented as beneficial through wording and design, often in combination with threats of lost functionality if users decline.

A key aim of GDPR is to protect the personal data of individuals and to strengthen individuals' control and rights over their data. Many companies have recently pledged to extend GDPR-level protections to individuals in the U.S. As the findings of the report make clear, however, the approach of Facebook and Google takes away agency from individuals, nudging them towards the most privacy-invasive options.

The practices highlighted in this report raise significant issues, including whether these companies are upholding their promises to comply with the GDPR, and whether these tactics constitute unfair and deceptive trade practices under Section 5 of the FTC Act. We have documented similar practices for the FTC in the past, most notably in the way that Facebook altered users' privacy settings and Google opted users into Buzz. In both cases, the FTC took action and found that these were unfair and deceptive trade practices.

The new report of the Norwegian Consumer Council calls into question these companies' compliance with the following provisions of GDPR:

- (1) *The data protection principles of transparency, purpose limitation and data minimization (Article 5 GDPR).* Individuals are not being given the full picture – notifications have been designed in such a way as to hide important information from them and nudge them to consent to the collection and use of as much data as possible for a wide range of purposes.
- (2) *The lawful basis for processing (Articles 6 and 9), and consent (Article 7).* Many of the prompts covered in the report appear to rely on consent as a legal basis for processing. However, the practices employed by these companies raise questions as to whether consent in this case can be considered informed and freely given.
- (3) *Data protection by design and by default (Article 25).* Contrary to the requirements of this principle, the design and operation of the “pop-ups” as described in the report make it difficult for individuals to protect their personal data, nudging them towards more data sharing and with (hidden) default settings being set to options that are not the most privacy friendly ones.

We hope that you will share our concerns about the practices highlighted in this report and urge you to investigate these issues more in depth. The report analyzes the practices of three of the world's largest technology companies, which process billions of people's data. There is the added risk that where these companies lead (or in this case fail to lead), others will follow.

Sincerely,

Marc Rotenberg, President
Electronic Privacy Information Center

David Monahan, Campaign Manager
Campaign for a Commercial-Free Childhood

Katharina Kopp, Ph.D., Deputy Director, Director of Policy
Center for Digital Democracy

Ruth Susswein, Deputy Director, National Priorities
Consumer Action

Susan Grant, Director of Consumer Protection and Privacy,
Consumer Federation of America

John Simpson
Consumer Watchdog

Robert Weissman, President
Public Citizen

Ed Mierzwinski, Senior Director, Federal Consumer Program,
U.S. PIRG