Fact Sheet on 2019 FTC Order with Facebook

- Facebook will pay an unprecedented $5 billion in civil penalties for violating its 2012 order with the FTC.

- The new order approved by the Commission requires Facebook to restructure its approach to privacy from the corporate board-level down, establishing strong new mechanisms to ensure that Facebook executives are accountable for the decisions they make about privacy, and that those decisions are subject to meaningful oversight.

- The settlement order imposes unprecedented new restrictions on Facebook's business operations and creates multiple channels of compliance.

- The order requires Facebook to create an independent privacy committee created within the company's board of directors that will have the sole focus of overseeing privacy at Facebook.
    - The privacy committee will review all material privacy issues and decisions.
    - It can remove privacy compliance officers (and, subject to FTC approval, the assessor).
    - It must be independent (Facebook management cannot be members of the privacy committee).
    - Members must be appointed by an independent nominating committee and can only be removed without cause by supermajority of voting shares, not by the CEO or other employees.
    - It must meet with the independent assessor quarterly, without management present, to be briefed about any new or continuing material privacy risk.

- Under the order, designated compliance officers and other high-level Facebook staff have new responsibilities to carry out Facebook's privacy program. This includes:
    - Conducting privacy reviews and documenting all privacy decisions;
    - Certifying compliance with the FTC order; and
    - Giving reports to the independent assessor, Facebook CEO, and the FTC.

- CEO Mark Zuckerberg is made more accountable for Facebook's privacy program.
    - He must certify Facebook's compliance with FTC order—exposing him, personally, to civil and criminal penalties.
    - He must review material privacy risks and decisions each quarter.
    - He does not control the independent privacy committee or assessor.

- Facebook must create an enhanced privacy program with greater oversight and transparency. It must:

    - Conduct and document privacy reviews of each new or modified product, service, or practice;
    - Share written privacy reviews with the assessor, Facebook CEO, and (upon request) the FTC;
    - Carry out closer oversight of third-party developers and terminate them as appropriate;
    - Expand the program to cover other services that share Facebook covered information, including WhatsApp and Instagram; and
    - Submit incident reports to the assessor and the FTC.

- Facebook must have a stronger and more independent assessor.
    - The assessor can be approved or removed only by the independent privacy committee and the FTC.
    - Facebook must give the assessor all relevant privacy information.
    - The assessor must "look under the hood" to judge the effectiveness of Facebook's privacy program—not rely solely on what management says.
    - It must meet regularly and in private with the board committee and send reports to the FTC.

- Facebook must create a comprehensive data security program and must encrypt user passwords.

- Facebook cannot use phone numbers it received specifically for security purposes for advertising.

- Facebook cannot ask for passwords to other third-party accounts when people sign up for Facebook accounts.

- Facebook must not create, or delete any existing, facial recognition templates for new and existing users who have its "Tag Suggestions" setting, unless it obtains the user's affirmative express consent. It also must obtain affirmative consent before using facial recognition technology in a manner that materially exceeds prior disclosures to users.

- Facebook must delete from its servers personal information deleted by users.

- Facebook must implement strict employee-access controls to user information.

- In addition to prohibiting misrepresentations about the collection or disclosure of information, the order prohibits Facebook from misrepresenting how it ***uses*** personal information.