

June 21st, 2021

To: Michel Protti Chief Privacy Officer - Product and Designated Compliance Officer, Facebook Inc.

Cc: Facebook Independent Privacy Committee

As required by Part VIII of the Consent Order (the Order) between Facebook and the Federal Trade Commission (FTC) and (DOJ) issued April 27, 2020, Protiviti was engaged to perform an independent Privacy Program Assessment (Assessment). Attached within is Protiviti's report on its initial assessment of Facebook's Privacy Program, pursuant to obligations in Part VII of the Order. This report includes the results of our review, included in the following sections of the report:

- I. Executive Summary
- II. Our Assessment Scope and Methodology
- III. Our Assessment Results which include the details of our testing approach and our noted findings related to gaps and weaknesses organized by Facebook's (b)(3):HSR; (b)(4)
- IV. Appendices supporting certain details of our Assessment

As required by Part VIII.G of the Order, in conducting our independent review, Protiviti did not primarily rely on assertions or attestations by Facebook management.

Refer to the remainder of this document for the details of our report.

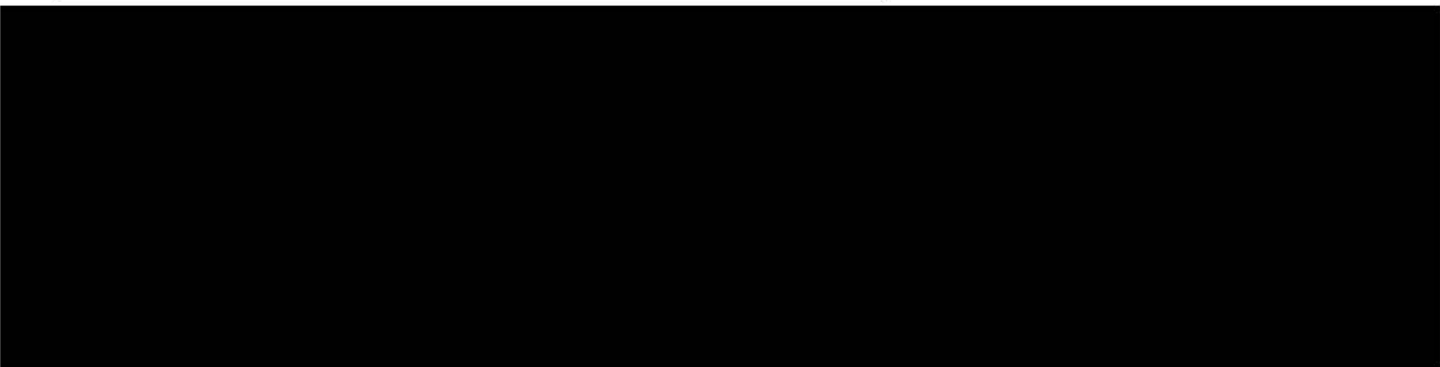
Sincerely,

(b)(4)

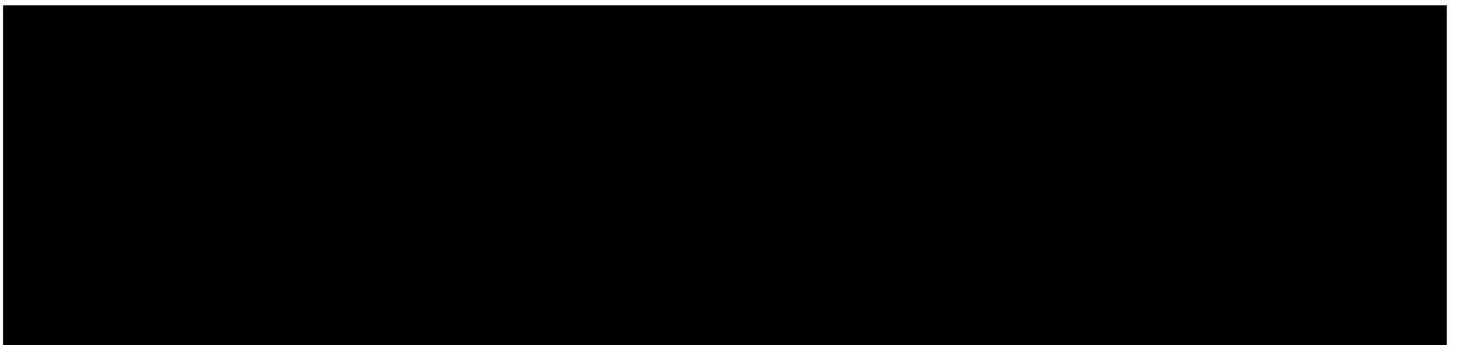
(b)(4); (b)(3):6(f)

Table of Contents

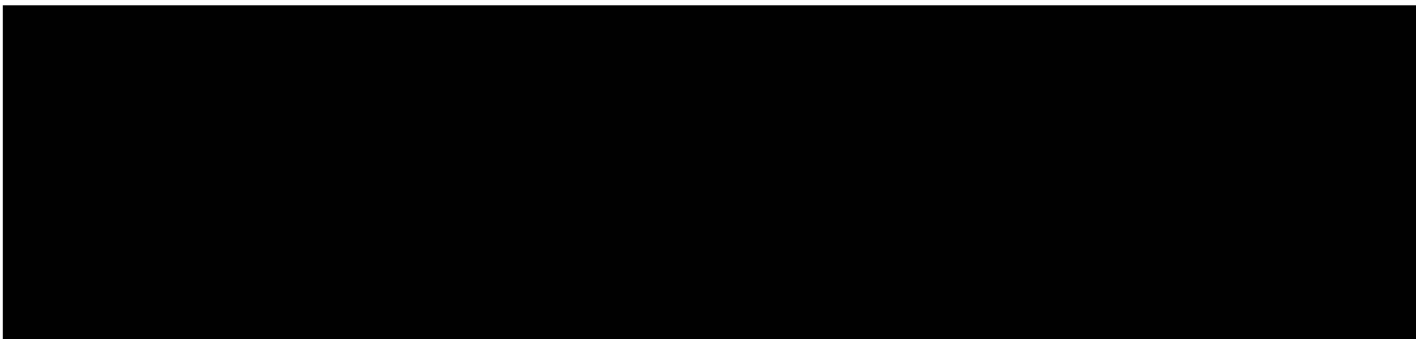
I. Executive Summary.....	1
II. Assessment Methodology	7
A. Assessment Scope	7
B. Methodology Framework.....	9
III. Order Mandated Assessment (b)(4); (b)(3);6(f)	15
A. (b)(4); (b)(3);6(f)	15
(b)(4); (b)(3);6(f)	15
.....	15
.....	16
.....	18
B. (b)(4); (b)(3);6(f)	20
(b)(4); (b)(3);6(f)	20
.....	20
.....	22
.....	23
C. (b)(4); (b)(3);6(f)	26
(b)(4); (b)(3);6(f)	26
.....	26
.....	27
.....	28
D. (b)(4); (b)(3);6(f)	31
(b)(4); (b)(3);6(f)	31
.....	31
.....	34
.....	36
E. (b)(4); (b)(3);6(f)	40
(b)(4); (b)(3);6(f)	40
.....	40
.....	41



(b)(4); (b)(3):6(f)	43
F. (b)(4); (b)(3):6(f)	51
(b)(4); (b)(3):6(f)	51
	52
	56
	59
G. (b)(4); (b)(3):6(f)	64
(b)(4); (b)(3):6(f)	64
	66
	71
	73
H. (b)(4); (b)(3):6(f)	90
(b)(4); (b)(3):6(f)	90
	90
	92
	93
I. (b)(4); (b)(3):6(f)	101
(b)(4); (b)(3):6(f)	101
	101
	107
	109
J. (b)(4); (b)(3):6(f)	114
(b)(4); (b)(3):6(f)	114
	114
	118
	120
K. (b)(4); (b)(3):6(f)	123
(b)(4); (b)(3):6(f)	123
	124
	126



(b)(4); (b)(3);6(f)	128
L. (b)(4); (b)(3);6(f)	134
(b)(4); (b)(3);6(f)	134
	134
	145
	150
IV. Appendices.....	163
A. Safeguard Listing	163
B. Assessment Glossary.....	225
C. (b)(4); (b)(3);6(f)	236



I. Executive Summary

Consent Order Background

On April 28, 2020, Facebook Inc. (Facebook) entered into a Consent Order (the Order) with the US Department of Justice (DoJ) and Federal Trade Commission (FTC) concerning Facebook's privacy program and practices. The Order resolved a pending investigation into whether Facebook had violated the terms of an earlier privacy-related Consent Order dated July 27, 2012.

Among numerous other provisions, the Order required Facebook to pay a record \$5 billion judgment, barred Facebook from misrepresenting its user data practices, gave users additional rights over the sharing and deletion of their data broadly, and further restricted use of specific types of data such as telephone numbers provided for security verification purposes, account passwords, and facial recognition information. The Order also required Facebook to establish a Mandated Privacy Program (MPP) addressing approximately ten specific categories of privacy Safeguards set forth in Part VII(A-J) of the Order, and imposed significant self-assessment, management and Board of Director reporting, and other governance requirements. Finally, the Order required Facebook to obtain initial and biennial independent privacy Assessments, the role of which Protiviti (hereafter also referred to as "Assessor" or "we") was engaged to perform. Most of the significant requirements of the Order were subject to an initial compliance due date of October 24, 2020, which was 180 days after the entry of the Order. Protiviti's Assessment Period began immediately thereafter on October 25, 2020 and concluded on April 22, 2021.

Protiviti's Assessment Approach

Protiviti designed and implemented a comprehensive and fully independent approach for the initial six-month Assessment required under the Order. Our Assessment plan incorporated relevant elements of the National Institute of Standards and Technology (NIST) and Generally Accepted Privacy Principles (GAPP) framework and criteria, as well as our collective professional experience on privacy program standards, and was tailored to Facebook's unique size and complexity. More than (b)(4) Protiviti professionals contributed over (b)(4) hours to the Assessment, including specialists in the technology and social media industries, as well as data analytics, privacy regulation, and compliance program governance leading practices.

Consistent with the terms of the Order, Protiviti did not rely primarily on Facebook management assertions or attestations in conducting the Assessment. Instead, we submitted more than (b)(4) requests to independently obtain and review evidence regarding Facebook's compliance activities. This information included more than (b)(4) policies, procedures, management reports, training materials, and other key documents. We also conducted more than (b)(4) interviews and process walkthroughs with management to evaluate Safeguard design effectiveness and observe Facebook's compliance controls in practice. Finally, we developed tailored testing plans for each Safeguard and conducted independent testing using audit-industry standard sampling methodologies, ultimately performing approximately (b)(4) sample tests (testing of a unique Safeguard multiplied by the number of samples evaluated), to assess the operating effectiveness of Facebook's Safeguards. Protiviti met with members of Facebook's Independent Privacy Committee (IPC) of the Board of Directors (b)(4); (b)(3);6(f)

(b)(4); (b)(3);6(f)

(b)(4); (b)(3);6(f)

We also met with the FTC four times, and regularly met with members of Facebook's management team and outside legal advisors, to inform them of the progress of the Assessment and of the gaps and weaknesses that were noted as a result.

It should be noted that the MPP and the Safeguards surrounding it remained subject to a significant degree of change throughout our Assessment Period. This required flexibility and close coordination on both Protiviti and

Facebook's parts to understand implementation timelines and align our evaluation schedule accordingly, and employ alternative assessment techniques for newly-implemented Safeguards for which there was little to no historical performance evidence available to review. We acknowledge and appreciate the extensive access to, and cooperation provided by Facebook leadership throughout our Assessment.

Facebook's Compliance Strategy

In the FTC's own words, the Order "impose(d) unprecedented new restrictions on Facebook's business operations," and provided for "sweeping conduct relief...unprecedented in the history of the FTC" with the intent of "chang(ing) Facebook's entire privacy culture to decrease the likelihood of future violations."¹ As the company had been operating under an existing privacy Consent Order since 2012, it had the option of renovating its existing program and Safeguards to conform to the new requirements imposed by the 2020 Order. Alternatively, and in recognition of the significant degree of change expected by the Order, an entirely new program could be created. Ultimately, Facebook management elected the latter option and made the decision to comprehensively redesign the privacy organizational structure, program materials, and Safeguards (b)(4); (b)(3);6(f)

(b)(4); (b)(3);6(f) A few of the key examples of the changes made to address the Order include:

- Established dedicated privacy oversight and governance functions at both the Board of Directors and senior management committee levels;
- Redesigned privacy program management (b)(4); (b)(3);6(f) (b)(4); (b)(3);6(f) based on input from multiple outside experts (b)(4); (b)(3);6(f)
- Grew privacy-dedicated headcount from approximately (b)(4) employees as of mid-2019 to more than (b)(4); (b)(3);6(f) employees as of the date of our Assessment, with budget-approved plans to add an additional (b)(4); resources by 2021 year-end;
- Created a dedicated Privacy Review function staffed by more than (b)(4) privacy subject matter specialists and supporting technology infrastructure to conduct independent assessments of the privacy risks posed by new or modified products, services, or practices;
- Expanded the universe of privacy Safeguards from (b)(4) as of February 2019 to over (b)(4) by February 2021;
- Significantly expanded the privacy training program content and delivered enhanced training to more than (b)(4); (b)(3);6(f) employees and associates by the date of our Assessment; and
- Published more than (b)(4) privacy governing documents and approximately (b)(4) additional privacy-focused procedures.

(b)(4); (b)(3);6(f)

(b)(4); (b)(3);6(f)

We will continue to

¹ <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>

monitor closely Facebook's implementation within its new program of all the measures required by the Order throughout the upcoming two year assessment cycle.

Summary of Assessment Findings

Across many different areas, Facebook has made extensive investments in its privacy program since the effective date of the Order, and meaningful progress has been made. We believe the overall scope of the program and structure (b)(4); (b)(3):6(f) into which the program is organized is logical and appropriately comprehensive. As a result, the key foundational elements necessary for an effective program are now in place, although their maturity and completeness vary (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

That said – and as Facebook management itself anticipated in the Company's Day 180 Compliance Report submitted to the FTC – the gaps and weaknesses noted within our review demonstrate that substantial additional work is required, and additional investments must be made, in order for the program to mature (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) In total, our initial Assessment notes (b)(4); (b)(3):6(f) gaps and weaknesses (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

Our

key thematic observations include the following:

Need to Fully Establish and Mature an Independent Standard Setting and Oversight Function

In our experience, nearly all effective privacy programs operate according to a model where front-line product teams are responsible for performing day to day control activities that are designed to manage the risk associated with those products. (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

Establishing a Risk and Controls Mindset and “Showing Your Work”

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

Applying Core Strengths in Automation and Analytics to the Privacy Program

Few would dispute that Facebook stands among the most technologically sophisticated companies in the world. The company employs large numbers of highly specialized resources who use process automation techniques, artificial intelligence and machine learning, and other forms of data analytics (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

we believe there are significant further


opportunities in this area that should be prioritized and accelerated. (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)


(b)(4); (b)(3):6(f)

(b)(4); (b)(3);6(f)




Summary Conclusions

(b)(4); (b)(3);6(f)




(b)(4); (b)(3);6(f)

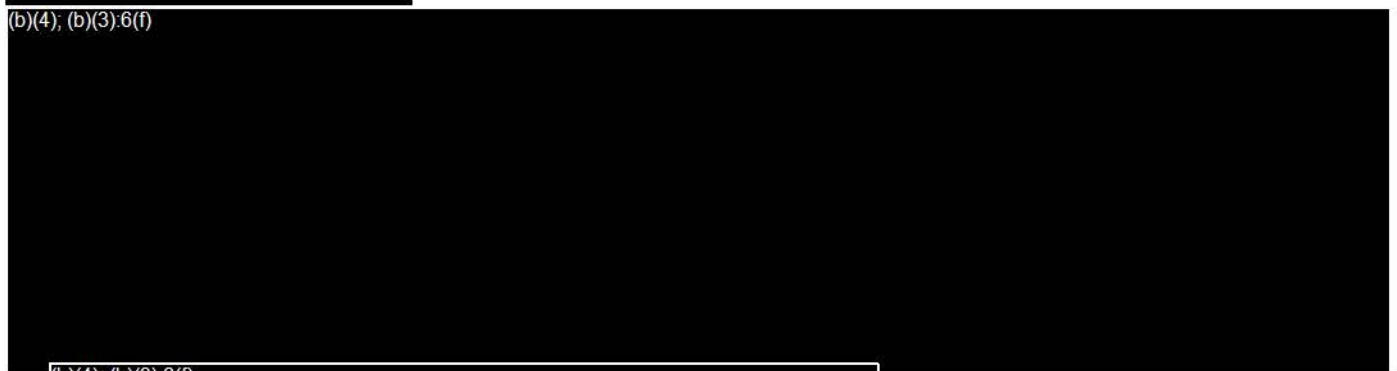
(b)(4); (b)(3);6(f)




(b)(4); (b)(3);6(f)



(b)(4); (b)(3);6(f)



(b)(4); (b)(3);6(f)



II. Assessment Methodology

A. Assessment Scope

Pursuant to the Order and its requirements under Part VIII.D, the purpose of Assessor's initial Assessment was to:

- Determine whether Facebook has implemented and maintained the MPP required by Part VII.A-J of the Order;
- Assess the effectiveness of the MPP, as implemented, to address each subpart in Part VII of the Order;
- Identify any gaps or weaknesses in the MPP; and
- Assess the effectiveness of any revised, updated, or added Safeguard(s) implemented during the Assessment Period for the period in which it was in effect.

The scope of the Assessment of information security was limited to security at the application and data layers as these have a direct connection between privacy and security. Although Part V of the Order mandates that Facebook maintains a comprehensive security program, this Assessment is limited (as described below) to Part VII of the Order. So, while it could be argued that security across many layers of Facebook's infrastructure ultimately help to protect Covered Information, under the Order, our scope was limited to privacy risks required under Part VII. We presented and received confirmation on this approach from the FTC representatives during our Assessment.

From a Facebook, business line perspective, 'Respondent' (for purposes of Parts VII-VIII, including the Mandated Privacy Program (MPP)) is defined in the Order as Facebook, Inc. and WhatsApp, Inc. (and successors/assigns). The MPP is operationalized through Facebook's products, services, and business areas, which tend to be centralized and operate across Legal entities in terms of their systems and practices. The Assessment therefore encompasses the vast majority of Facebook, Inc.'s Legal subsidiaries (and any corresponding products and services) to the extent they collect, use, or share Covered Information including Facebook, Instagram, WhatsApp, Messenger, Portal, and Oculus as well as other smaller internal organizations and business areas such as: Facebook Open Research and Transparency (FORT), CrowdTangle, UX Research Org (UXR), New Product Experiment (NPE), ABP Engineering, The Production Group (TPG), and Facebook Artificial Intelligence Research (FAIR). The Assessment did not cover a small number of independently operated affiliates. (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

Our scope was focused on U.S. users and functionality. In some cases, Facebook may present different options to non-U.S. users, these were not included in our Assessment. Additionally, business units that have no impact on U.S. users were not included in the Assessment. We also did not assess compliance to specific laws. While in-scope risks and Safeguards may address specific laws, legislative requirements for how these risks are addressed were not evaluated.

In its intent to address all requirements of the Order, Facebook designed and implemented (b)(4); (b)(3):6(f) the MPP. (b)(4); (b)(3):6(f) that relate to requirements within Part VII of the Order address expected elements of a comprehensive privacy program and are within the scope of Protiviti's Assessment. Pursuant to subpart VIII.C of the Order, the Assessment Period consisted of the first 180 days of the MPP's operation (October 25, 2020 – April 22, 2021). Only Safeguards for which the Safeguard activity was performed within the Assessment Period were in scope and evaluated.

Further, as the Order indicates that our Assessment is specific to Part VII, there were some elements of the MPP which did not address either relevant privacy risks nor other requirements from VII.A – VII.J. The Safeguards that are not included in our Assessment are related to Legal or administrative Order requirements and did not relate to a requirement in Part VII. These elements of the MPP were considered out of scope for our Assessment. In other cases, requirements in other Parts of the Order did translate to risks identified in Part VII and were therefore included in the Assessment. For example, while Part I of the Order prohibits misrepresentations, and therefore was not directly assessed, Facebook identified risks and Safeguards that are intended to prevent privacy related misrepresentations. In this example, we did assess these Safeguards.

(b)(4), (b)(3):6(f) Part VII.D which required Facebook to assess and document a Privacy Risk assessment and requirement VII.A and VII.E which required Facebook to document the Safeguards that mitigate for those risk identified in Part VII.D. (b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f) Our Assessment included these Safeguards in our scope. (b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f) (b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f)

B. Methodology Framework

Part VIII.A of the Order in part stipulates the Assessor:

“(1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Mandated Privacy Program; and (3) retains all documents relevant to each Assessment for five years after completion of such Assessment and furnishes such documents to the Commission within ten days of receipt of a written request from a representative of the Commission.”

Further, Part VIII.D of the Order stipulates:

“Each Assessment must “(1) determine whether Respondent has implemented and maintained the Privacy Program required by Part VII.A-J of this Order, titled Mandated Privacy Program; (2) assess the effectiveness of Respondent’s implementation and maintenance of each subpart in Part VII of this Order; (3) identify any gaps or weaknesses in the Privacy Program; and (4) identify specific evidence examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor’s findings.”

With these requirements established, among other stipulations set forth in Part VIII of the Order, the Assessor developed and executed an Assessment Methodology to:

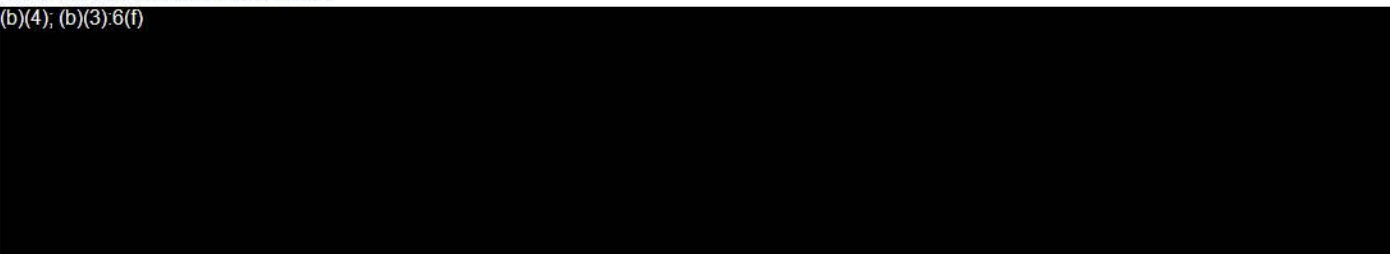
- Define a process to evaluate the Mandated Privacy Program (MPP) relative to the Order requirements and industry standards for privacy programs;
- Generate standards related to design and operational effectiveness testing;
- Establish protocols for escalation of potential gaps and weaknesses identified in the MPP; and
- Establish documentation requirements to maintain evidence of results related to the Assessment.

The remainder of this section outlines the components of the Assessment Methodology, including:

- Pre-Assessment Activities: an evaluation of the MPP in relation to the Order requirements and industry standards;
- Safeguard Impact Analysis: a process to establish a risk to Safeguard mapping, including an associated Safeguard impact rating;
- Design Effectiveness (DE) Assessment: an evaluation of whether the MPP and affiliated Safeguards would achieve the MPP’s objectives and the Order requirements;
- Operating Effectiveness (OE) Assessments: an evaluation of whether the Safeguards were operating to mitigate their intended associated risk or Control Objective;
- Gap and Weakness Disposition: a process to validate the observations raised throughout the course of DE and OE assessments; and
- Evidence of Assessment: storage and documentation standards to address the requirements set forth in the Order.

Pre-Assessment Activities

(b)(4), (b)(3);6(f)



(b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f)

we developed a framework to assess the effectiveness of the MPP by leveraging the National Institute of Standards and Technology (NIST)² and Generally Accepted Privacy Principles (GAPP)³ framework and criteria, as well as our collective professional experience on privacy program standards, and tailored an assessment approach to Facebook's unique size and complexity. The evaluation of standards, (b)(4), (b)(3):6(f), was used to inform the development of the Assessment Methodology in accordance with the requirements of the Order and in consideration of Facebook's MPP structure.

Safeguard Impact Analysis

(b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f)

(b)(4), (b)(3):6(f)

² Working in collaboration with private and public stakeholders NIST produced a framework for improving Privacy through Enterprise Risk Management, to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals' privacy, the NIST published a Privacy Framework on January 16, 2020, which helps organizations assess and manage:

- Privacy risks across the enterprise and the data processing ecosystem;
- Integration of privacy controls into the design and development of new systems, products, and services;
- Communication, awareness and public notice about organizational privacy practices; and
- Governance of privacy policies and processes inside the organization and across the data processing ecosystem.

³ GAPP is a framework intended to assist in creating an effective privacy program for managing and preventing privacy risks. GAPP is a component of System and Organization Controls – Type 2 reporting (SOC 2). The GAPP framework was developed through joint consultation between the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA)

Design Effectiveness Assessment

During the Design Effectiveness Assessment, the Assessor evaluated if the MPP, as designed, would achieve the MPP's objectives and the Order requirements, mitigate privacy risk, and allow for implementation of a comprehensive privacy program. (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

Operating Effectiveness Assessment

Operating effectiveness assessments were performed on (b)(4); Safeguards to determine if they achieved their (b)(4); (b)(3):6(f) Safeguards which were not implemented or not yet performed were not tested for operating effectiveness. Operating effectiveness included using procedures developed by the Assessor to determine whether high- and medium-impact Safeguards were fully implemented, executed, and operating as intended.

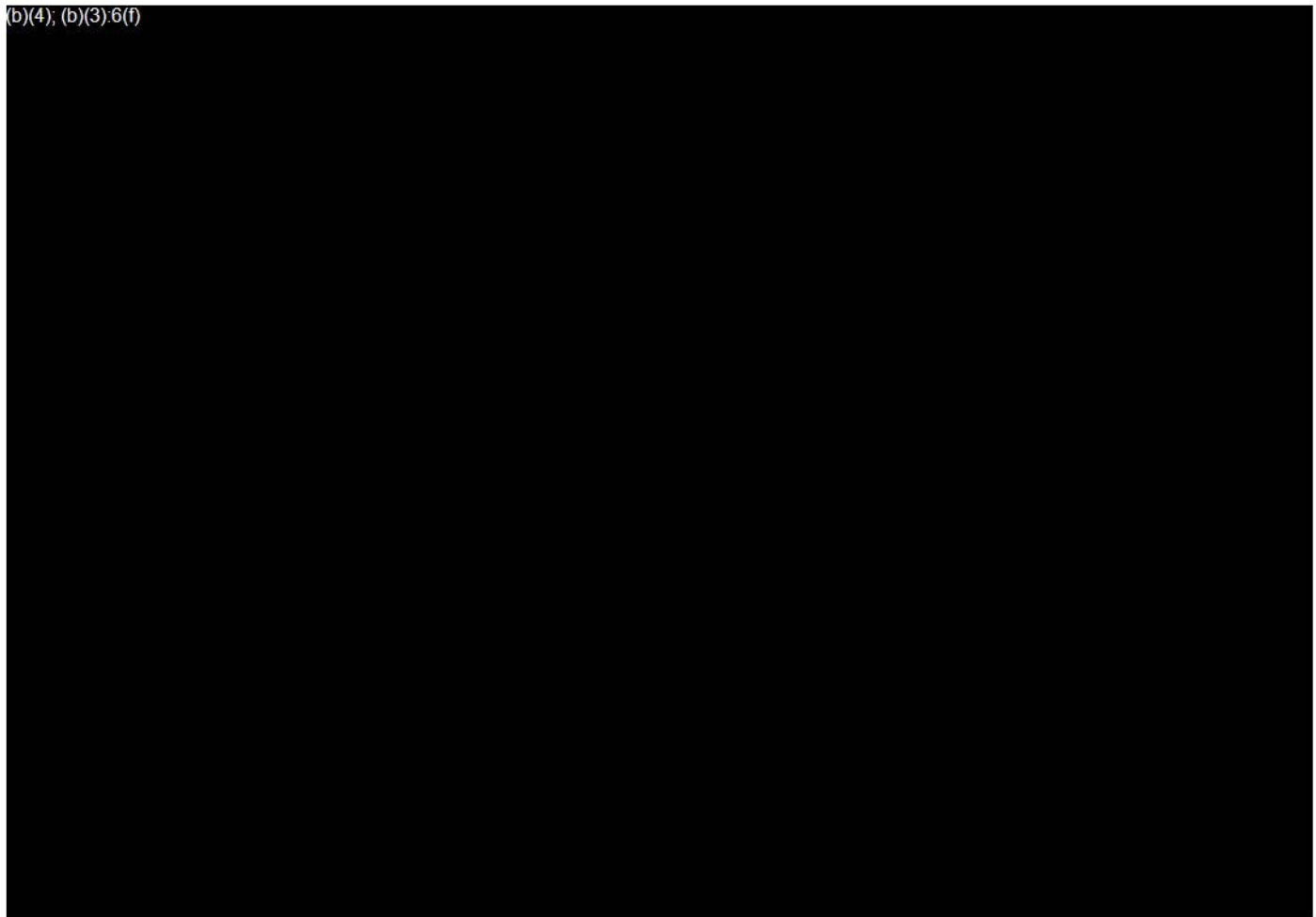
The testing procedures were designed to evaluate whether the Safeguards support an effective mitigation of the respective risk. (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

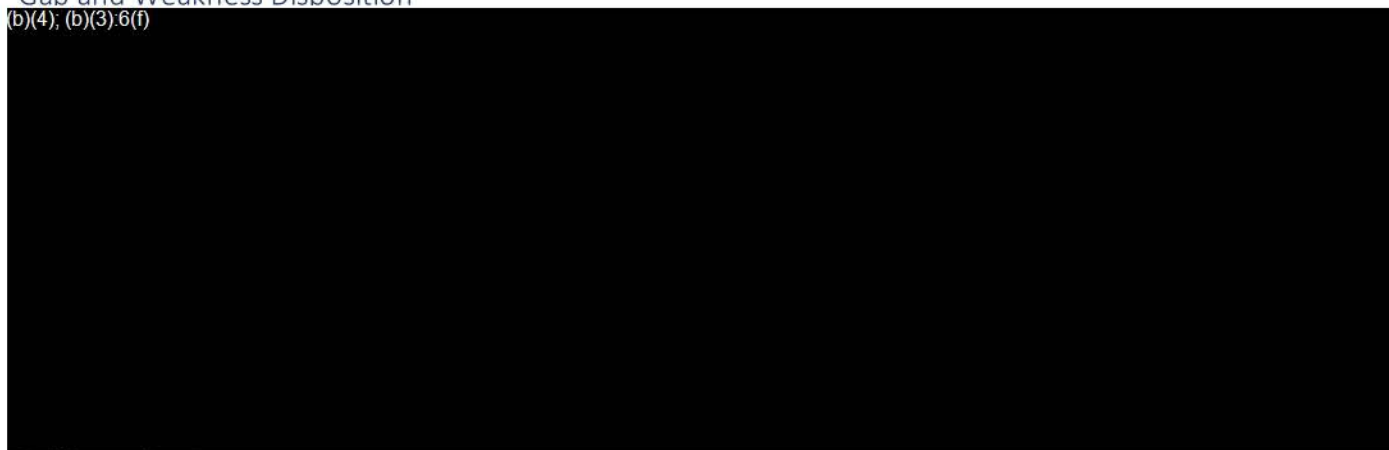
(b)(4); (b)(3):6(f)

(b)(4); (b)(3);6(f)




Gap and Weakness Disposition

(b)(4); (b)(3);6(f)



Evidence for Assessment

The Assessor utilized and examined various forms of evidence to conduct the Assessment and make observations and determinations. Specific evidence utilized varied based upon the Safeguard and the testing performed. All evidence reviewed was discussed and documented in the Assessor's work papers. Generally, the types of evidence examined are as follows:

- Interview Notes: Assessor notes detailing information gathered during walkthroughs and interviews conducted with (b)(4); (b)(3);6(f), as well as support staff;
 - Policies: Governing documents outlining high-level objectives of the Privacy Program;
- 

- Playbooks: Detailed supporting documentation that contain procedural steps for executing Safeguards and their underlying processes; and
- Samples: Individual pieces of evidence provided by Facebook based on requests from Assessor used to demonstrate the operation of Safeguards.

The Assessor maintained a log of all requests for information and data submitted to Facebook as well as the responses and documentation received. In accordance with part VIII.A of the Order, all documentation and evidence provided by Facebook for the Assessment will be retained for five years.