

### III. Order Mandated Assessment by

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

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

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

[Within this (b)(4); (b)(3):6(f) and throughout the remainder of the (b)(4); (b)(3):6(f) discussed in Section III – Order Mandated Assessment by (b)(4); (b)(3):6(f) we use affirmative terms such as “does,” “performs,” “executes,” etc. In those instances, the terms do not necessarily represent the results of our testing, but instead describe Facebook’s intent behind the associated processes and Safeguards.]

The (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) covers requirements to implement internal-facing written policies and procedures pertaining to the privacy and handling of Covered Information. (b)(4); (b)(3):6(f)

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

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

Part VII.A: Document in writing the content, implementation, and maintenance of the Privacy Program that includes: (1) the documented risk assessment required under Part VII.D. of the Order; and (2) the documented safeguards required under Part VII.E of the Order ... (4) a description of the procedures adopted for implementing and monitoring the Privacy Program, including procedures used for evaluating and adjusting the Privacy Program as required under Part VII.J of this Order.

Part VII.E: Design, implement, maintain, and document safeguards that control for the material Internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

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

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

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

In response to the Order, Facebook, in effect, created a new Privacy Program, including a foundational redesign of both its Safeguard environment and compliance documentation. As a result, as of October 25<sup>th</sup>, 2020, (b)(4); (b)(3):6(f)

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

published more than (b)(4); (b)(3):6(f) privacy governing documents and approximately an additional (b)(4); (b)(3):6(f) privacy-focused policies, playbooks, procedures, tools, templates, and guidelines. (b)(4); (b)(3):6(f)

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

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

Facebook developed the Internal Privacy Policy to explain employees' role in supporting the Mandated Privacy Program

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

The policy was published on the

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

(b)(4); (b)(3):6(f) Each employee agrees to abide by the Internal Privacy Policy through their completion of the Code of Conduct training.

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

The policy is reviewed at least (b)(4); (b)(3):6(f) by the (b)(4); (b)(3):6(f)

Detailed testing of the (b)(4); (b)(3):6(f) were evaluated as part of the

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

Testing the (b)(4); (b)(3):6(f) focused on the *Internal Privacy Policy* and its related documentation. The Assessor considered standards including the National Institute of Standards and Technology (NIST) and the Generally Accepted Privacy Principles (GAPP) to evaluate the completeness of the Safeguard environment and to evaluate the approach Facebook took to document privacy-related policies and procedures. As many policies exist, additional policy and procedural documentation was reviewed in the testing of each respective (b)(4); (b)(3):6(f). The Assessor referenced the associated (b)(4); (b)(3):6(f) descriptions, Safeguard descriptions and parts of the Consent Order to evaluate the completeness of the Internal Privacy Policy, as well as Facebook's process for approving the policy and disseminating the requirements to Facebook personnel<sup>5</sup>.

Our evaluation of the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) included the review of approximately (b)(4); (b)(3):6(f) documents, reports, and evidence specific to the (b)(4); (b)(3):6(f). Key documentation we reviewed included but was not limited to the following:

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

<sup>5</sup> Facebook personnel includes current Facebook employees, contingent workers and interns.

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

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

In addition, the Assessor coordinated cross-(b)(4); (b)(3):6(f) discussions and documentation reviews with the Assessor teams responsible for evaluating the supporting documentation for each Safeguard assessing the overall Safeguard environment. The evaluation of the Safeguard environment included testing the completeness and accuracy of the supporting policies, procedures, and playbooks (“governing documents”) for each Safeguard. We evaluated the accuracy of the Safeguard description, whether the governing documents accurately reflect the respective process, and whether the tools and templates were sufficient for supporting the execution of the Safeguards. Through our evaluation, we requested and reviewed governing documents and facilitated walkthrough sessions with Safeguard Owners to understand how the respective process is executed and evaluated the design of each Safeguard. As part of our operating effectiveness testing, we also evaluated the operational evidence for each respective Safeguard.

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

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

Our design effectiveness testing included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) were as follows:

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

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

Our operating effectiveness testing included obtaining and evaluating documentation to determine whether the (b)(4); Safeguards operated as designed. Through our testing processes, we gained an understanding of how the Internal Privacy Policy was created, approved, published, and disseminated to Facebook personnel. We also reviewed company privacy-related policies,

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

The key objectives and our test procedures for operating effectiveness testing for the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) were as follows:

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

- [Redacted]
- (b)(4); (b)(3):6(f)

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

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


Overview

Part VII.A requires Facebook to document in writing the content, implementation, and maintenance of the Privacy Program. Specifically, VII.A.2 requires documented Safeguards required under Part VII.E, while VII.A.4 requires a description of the procedures adopted for implementing and monitoring the Privacy Program, including procedures used for evaluating and adjusting the Privacy Program as required under Part VII.J. Further, Part VII.E. of the Order requires Facebook to design, implement, maintain, and document Safeguards that control for the material internal and external risks identified in response to Part VII.D.


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

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

key governing activities for the Mandated

Privacy Program, including establishing two independent committees of Facebook’s Board of Directors:

- The Compensating, Nominating and Governance Committee; and
- The Privacy Committee that oversees the Privacy Program and Order compliance and the appointment of a Designated Compliance Officer.

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

Part VII.B: Provide the written program required under Part VII.A. of this Order, and any evaluations thereof or adjustments thereto, to the Principal Executive Officer and to the Independent Privacy Committee created in response to Part X of this Order at least once every twelve (12) months

Part VII.C: Designate a qualified employee or employees to coordinate and be responsible for the Privacy Program (“Designated Compliance Officer(s)”), one of whom will be the Chief Privacy Officer for Product, subject to the reasonable approval of the Independent Privacy Committee, and who may only be removed from such position by Respondent with an affirmative vote of a majority of the Independent Privacy Committee

Part VII.E: Design, implement, maintain, and document safeguards that control for the material Internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

Part VII.I: Consult with, and seek appropriate guidance from, independent, third-party experts on data protection and privacy in the course of establishing, implementing, maintaining, and updating the Privacy Program

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

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

Facebook developed and implemented a Privacy Governance and Accountability Structure comprising the teams and roles that are critical to the ongoing documentation, implementation, monitoring and maintenance of the Mandated Privacy Program. Facebook designated a Chief Privacy Officer-Product, established a cross functional oversight body (i.e., Privacy Leads Cross Functional (XFN) Committee), and implemented a Privacy Governance and Accountability Structure at the board-level consisting of Independent Directors, to govern the overall Mandated Privacy Program. This includes two independent committees of Facebook’s Board of Directors that have Order-related responsibilities. The first, the Compensation, Nominating and Governance Committee (CNGC), is an independent committee of Facebook’s Board of Directors with the authority and responsibility to recommend appointments to the Board and to the Privacy Committee and is responsible for ensuring that the Privacy Committee consists of directors who are both

independent and meet the Order's Privacy and Compliance Baseline Requirements. The CNGC vetted and recommended the current members of the second new committee, the Privacy Committee.

The Privacy Committee is also an independent committee of Facebook's Board of Directors and provides Board-level oversight of both the Privacy Program and Order compliance. The Privacy Committee's formation occurred in May 2020. The Privacy Committee approved the Company's selection of the Designated Compliance Officer, Chief Privacy Officer-Product (DCO), as well as its selection of the Independent Assessor. The Privacy Committee meets (b)(4); (b)(4); with the Independent Assessor, who provides briefings on the Assessment and material risks to Covered Information. The Assessor also meets with the Committee Chair separately, (b)(4); (b)(3):6(f) to provide briefings. Note that both the CNGC and Privacy Committee were deemed out-of-scope for the assessment as they fall under Part X of the Order and are related to compliance with the Legal and administrative requirements of the Order rather than mitigating risks identified in the risk assessment or addressing expected elements of a comprehensive privacy program.

The DCO is responsible for the Privacy Program and leads the overall Privacy Organization, which consists of more than (b)(4) employees. Additionally, the DCO and the Company's Principal Executive Officer are to sign quarterly and annual certifications regarding the Privacy Program and Facebook's Order compliance, respectively, to provide direct accountability at the highest levels of the Company.

In addition, the DCO operates a cross-functional Privacy Leads forum to oversee initiatives related to implementing and operating the Mandated Privacy Program and to address key privacy risks and issues, some examples of which include: (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f)

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

responsible for creating and maintaining the written documentation of the content, implementation, and maintenance of The Mandated Privacy Program as required in Part VII.A in the form of the Mandated Privacy Program Document. The Mandated Privacy Program Document is updated by the (b)(4); at least annually and is reviewed and approved by the DCO. A copy of the Mandated Privacy Program Document is also delivered to the Principal Executive Officer and the Privacy Committee on an annual basis. (b)(4); (b)(3):6(f)

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

Additionally, (b)(4) supplementary appendices are included within the Mandated Privacy Program Document that provide additional context and information for the program including: (b)(4); (b)(3):6(f)

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

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

The (b)(4); is also responsible for the Mandated Privacy Program evaluation and adjustment process. This process is designed to occur at least annually, but can also be triggered (b)(4); (b)(3):6(f)

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

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

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

External experts are engaged by Facebook on a variety of different topics, including privacy, as required by Part VII.I of the Order. Based on information gathered from the broader business, the Privacy and Data Policy team identified and engaged with independent privacy experts throughout the development and enhancement of the Privacy Program. Experts include external, independent individuals who have a background and focus in data protection, privacy, and compliance, including from industry, academia and non-governmental organizations.

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

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

The Assessor referenced the associated Safeguard descriptions and parts of the Order to evaluate the approach Facebook took to design, implement, and operate the (b)(4); (b)(3):6(f) (b)(4); We evaluated processes executed by Facebook, (b)(4); (b)(3):6(f)

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

Our evaluation of the (b)(4); (b)(4); (b)(3):6(f) included the review of over (b)(4) documents, reports and evidence of governing activities, and outputs from key processes used for the purpose of program governance. Key documentation we reviewed included but was not limited to the following:

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



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

We conducted over (b)(4) interviews with the following individuals: (b)(4); (b)(3):6(f)

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

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

In alignment

with the Assessment Methodology, we performed (b)(4) sample tests (b)(4); (b)(3):6(f)

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

An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the (b)(4); (b)(3):6(f) were as follows:

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

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

Our operating effectiveness testing included evaluating the efficacy of key governance processes by selecting and testing samples, leveraging the sample methodology described in Section II – Assessment Methodology. The key objectives and our test procedures for operating effectiveness testing for the (b)(4); (b)(4); were as follows:

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

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

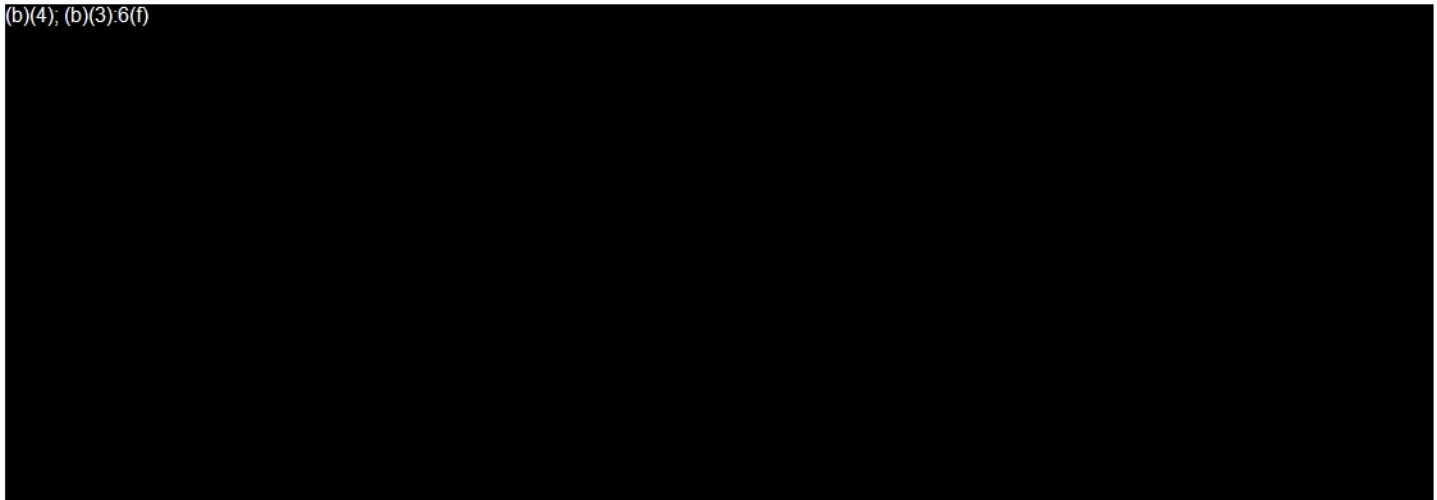
(b)(4); (b)(3):6(f)

Withheld pursuant to exemption

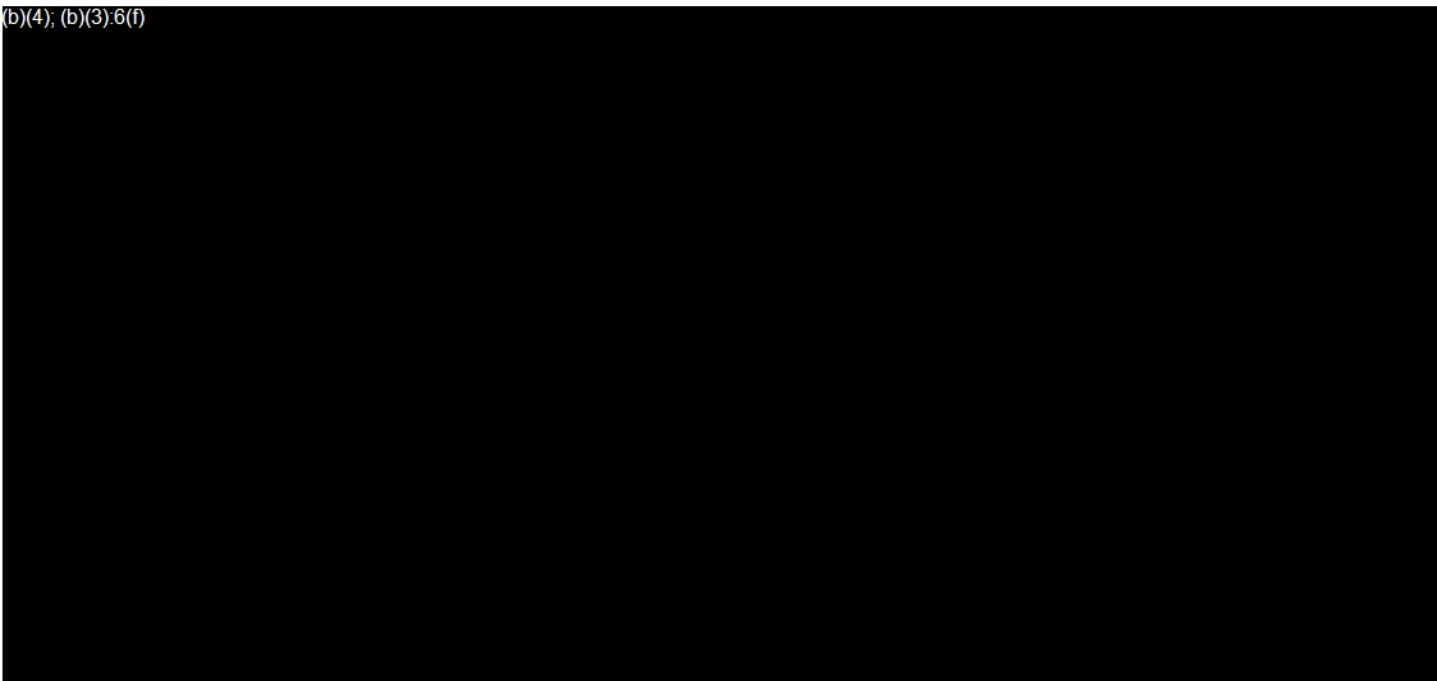
(b)(4); (b)(3):6(f)

of the Freedom of Information and Privacy Act

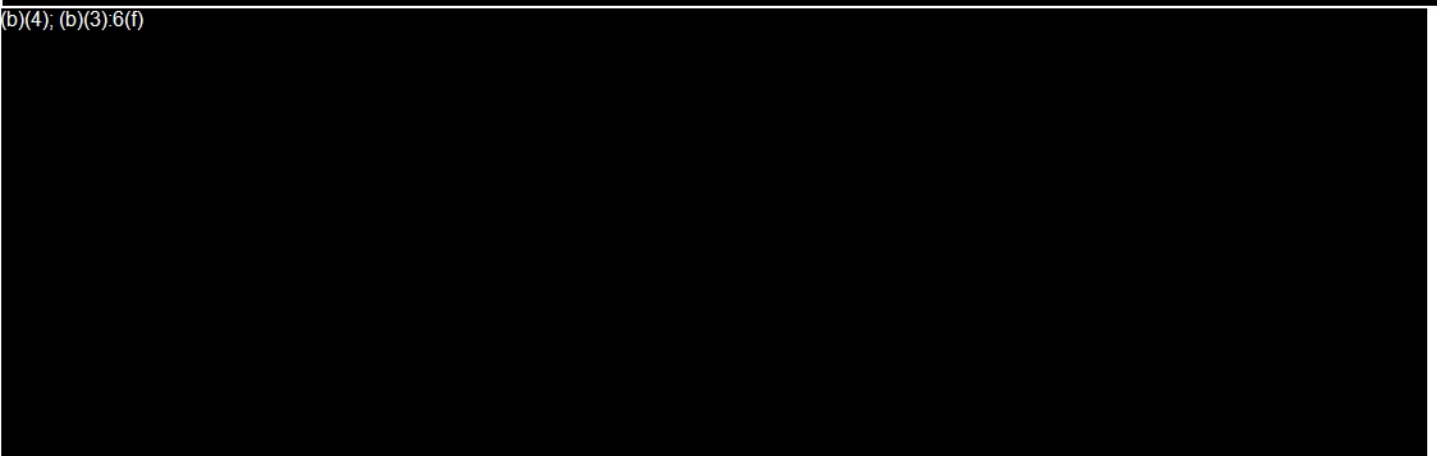
(b)(4); (b)(3):6(f)



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



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



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

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

Facebook designed the (b)(4); (b)(3):6(f) to address the following Order requirements through associated (b)(4); (b)(3):6(f) and Safeguards. The Order sub-requirements related to the (b)(4); (b)(3):6(f) include:

Part VII.E: Design, implement, maintain, and document safeguards that control for the material Internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

Part VII.G: Establish regular privacy training programs for all personnel on at least an annual basis, updated to address any Internal or external risks identified by Respondent in Part VII.D. of the Order and the safeguards implemented pursuant to Part VII.E. of the Order, that includes training on the requirements of the Order.

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

2021. Refer to Appendix A for details on the specific Safeguards within the (b)(4); (b)(3):6(f)

2. (b)(4); (b)(3):6(f)  
As mandated by the Order, Facebook's (b)(4); (b)(3):6(f) developed an Annual Privacy Training Program and a New Hire Privacy Training Program to be delivered to all personnel. (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)  
(b)(4); (b)(3):6(f) The Privacy Trainings were developed to provide foundational training on the Order requirements, as well as appropriate privacy practices and privacy-related expectations and commitments.

On (b)(4); (b)(3):6(f) 2020 the first Annual Privacy Training was deployed through (b)(4); (b)(3):6(f) to all existing personnel. (b)(4); (b)(3):6(f)

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

Learners were required to complete the training within (b)(4); (b)(3):6(f) days of assignment. (b)(4); (b)(3):6(f)

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

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

New Hire Privacy Training was deployed for all personnel hired on or after (b)(4); (b)(3):6(f) 2020. This included all newly hired personnel, interns and contingent workers (collectively known as “new hires”). (b)(4); (b)(3):6(f)

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

New hires have (b) days from their hire date to complete the New Hire Privacy Training. (b)(4); (b)(3):6(f)

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

Facebook also conducts some role-based Privacy Training (b)(4); (b)(3):6(f)

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

The (b)(4); (b)(3):6(f) plans to refresh the Annual Privacy Training on a (b)(4); (b)(3):6(f) basis. (b)(4); (b)(3):6(f)

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

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

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

The Assessor referenced the associated Safeguard descriptions and parts of the Order to evaluate the completeness and effectiveness of the (b)(4); (b)(3):6(f). We evaluated the end-to-end processes executed by Facebook, including Annual and New Hire Privacy Training development, deployment, completion monitoring, enforcement actions and planned refresh process as described herein.

Our evaluation of the Annual and New Hire Training processes included the review of over (b)(4) documents, reports and evidence of the execution of the Privacy Training process. Key documentation we reviewed included but was not limited to the following:

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

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

We conducted [redacted] interviews with key stakeholders, (b)(4); (b)(3):6(f)

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

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

In alignment with the Assessment Methodology, we performed over [redacted] sample tests (b)(4); (b)(3):6(f). An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how the Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the [redacted] were as follows:

- [redacted]
- [redacted]
- [redacted]

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

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

Our operating effectiveness testing included evaluating the effectiveness of the Privacy Training Program by selecting and testing samples, following the sample methodology described in Section II – Assessment Methodology. The key objectives and our test procedures for operating effectiveness testing for the [redacted] (b)(4); (b)(3):6(f)

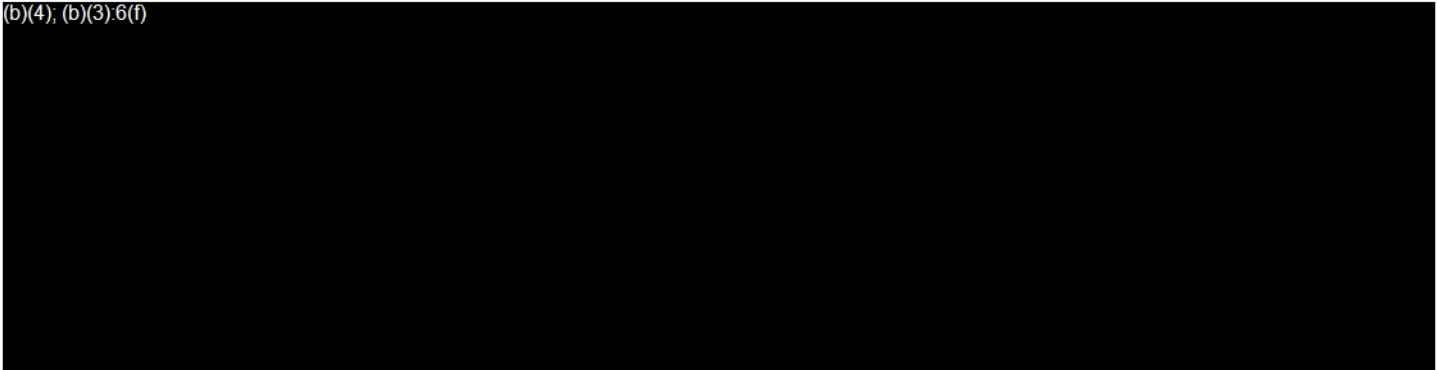
(b)(4); (b)(3):6(f) were as follows:

- Assessed if all personnel were assigned either Annual or New Hire Privacy Trainings through (b)(4); (b)(3):6(f)
- Evaluated whether the monitoring of personnel training completion metrics was effective through (b)(4); (b)(3):6(f) and
- Assessed whether the escalation process and enforcement actions for past due learners were effective through (b)(4); (b)(3):6(f).

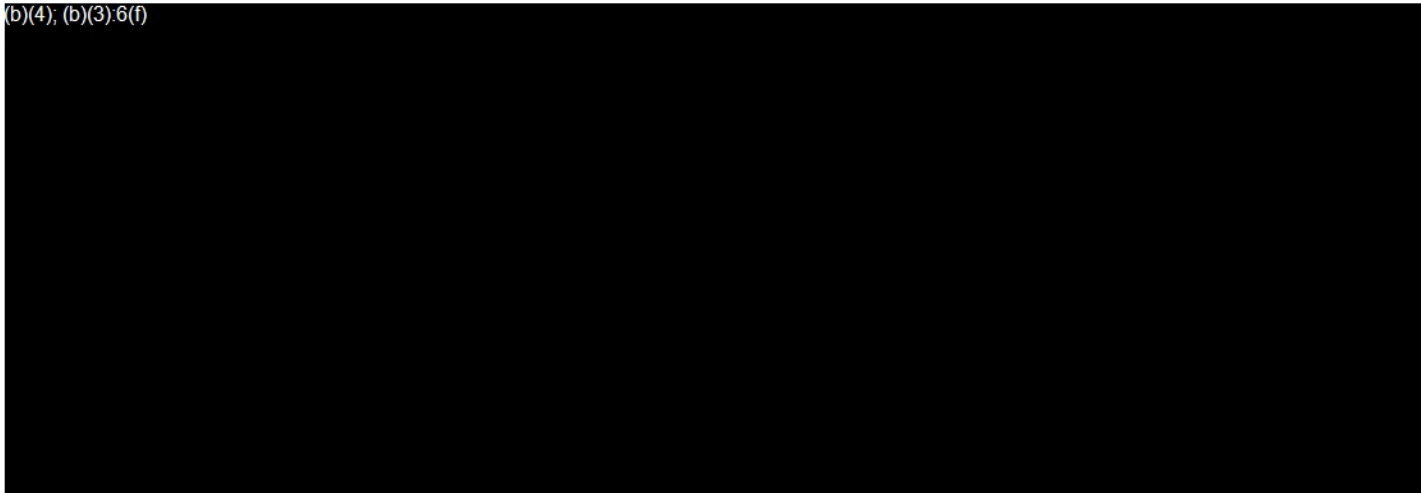
4. (b)(4); (b)(3):6(f)

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

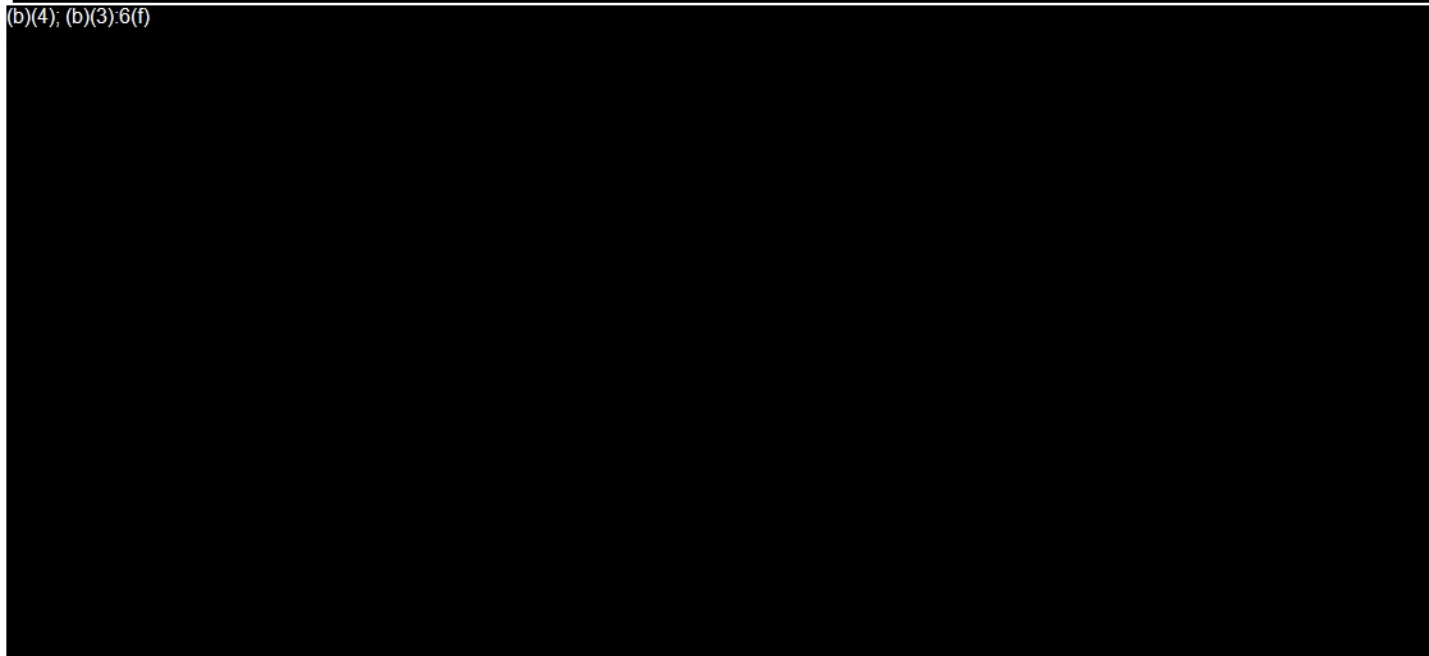
(b)(4); (b)(3):6(f)



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




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




---

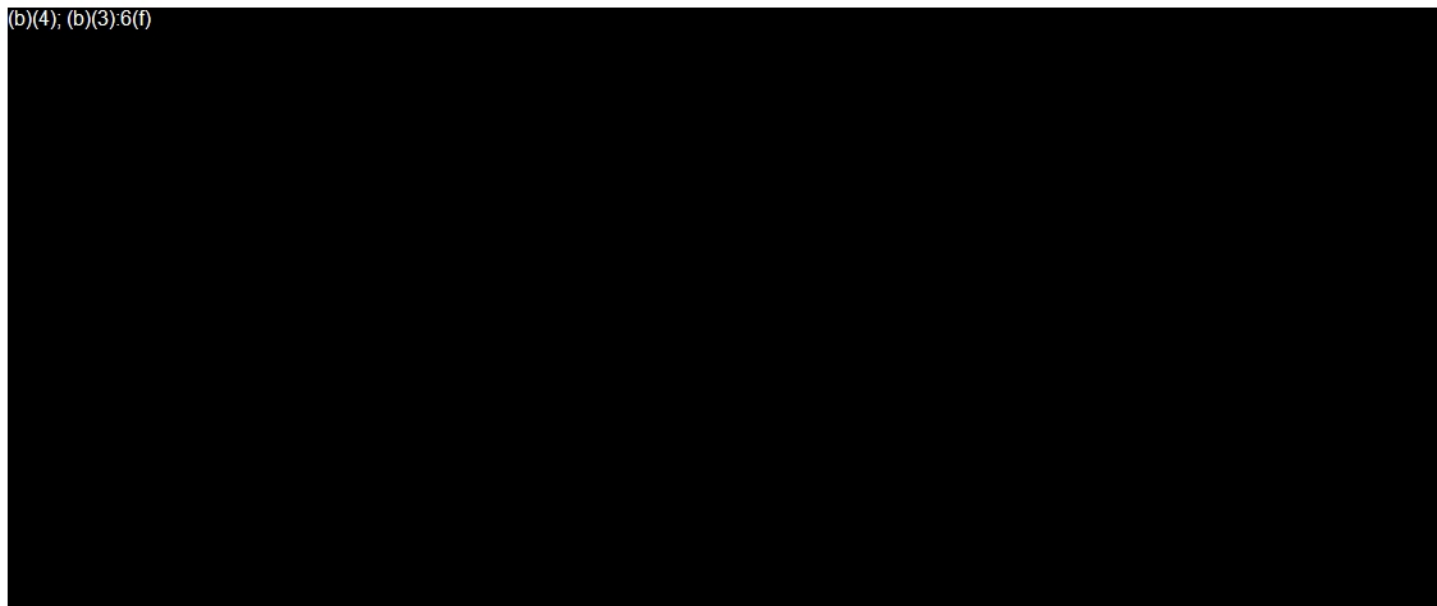
(b)(4); (b)(3):6(f)



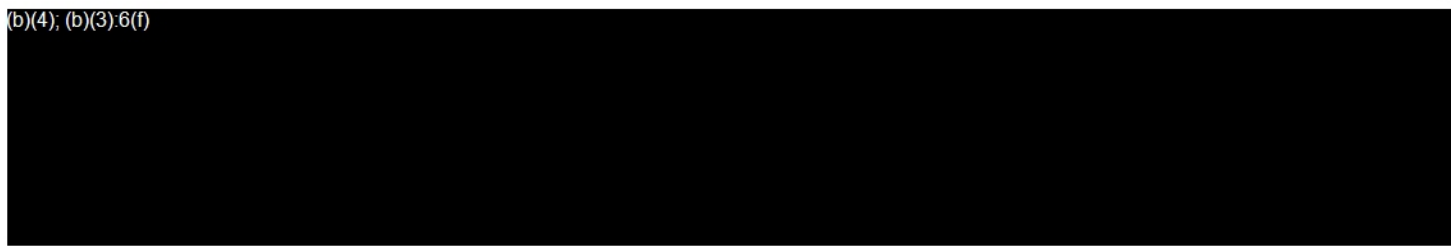
(b)(4); (b)(3):6(f)



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



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





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

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

Facebook designed the (b)(4); (b)(3):6(f) to address the Order requirements through associated (b)(4); (b)(3):6(f) and Safeguards. In relevant part, the Order sub-requirements related to the (b)(4); (b)(4); (b)(3):6(f) include:

Part VII.E: Design, implement, maintain, and document safeguards that control for the material Internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

The (b)(4); (b)(3):6(f) includes (b)(4); (b)(3):6(f) Safeguards. All (b)(4); (b)(3):6(f) Safeguards were implemented and executed during to the Assessment Period. Refer to Appendix A for details on the specific Safeguards within the (b)(4); (b)(3):6(f)

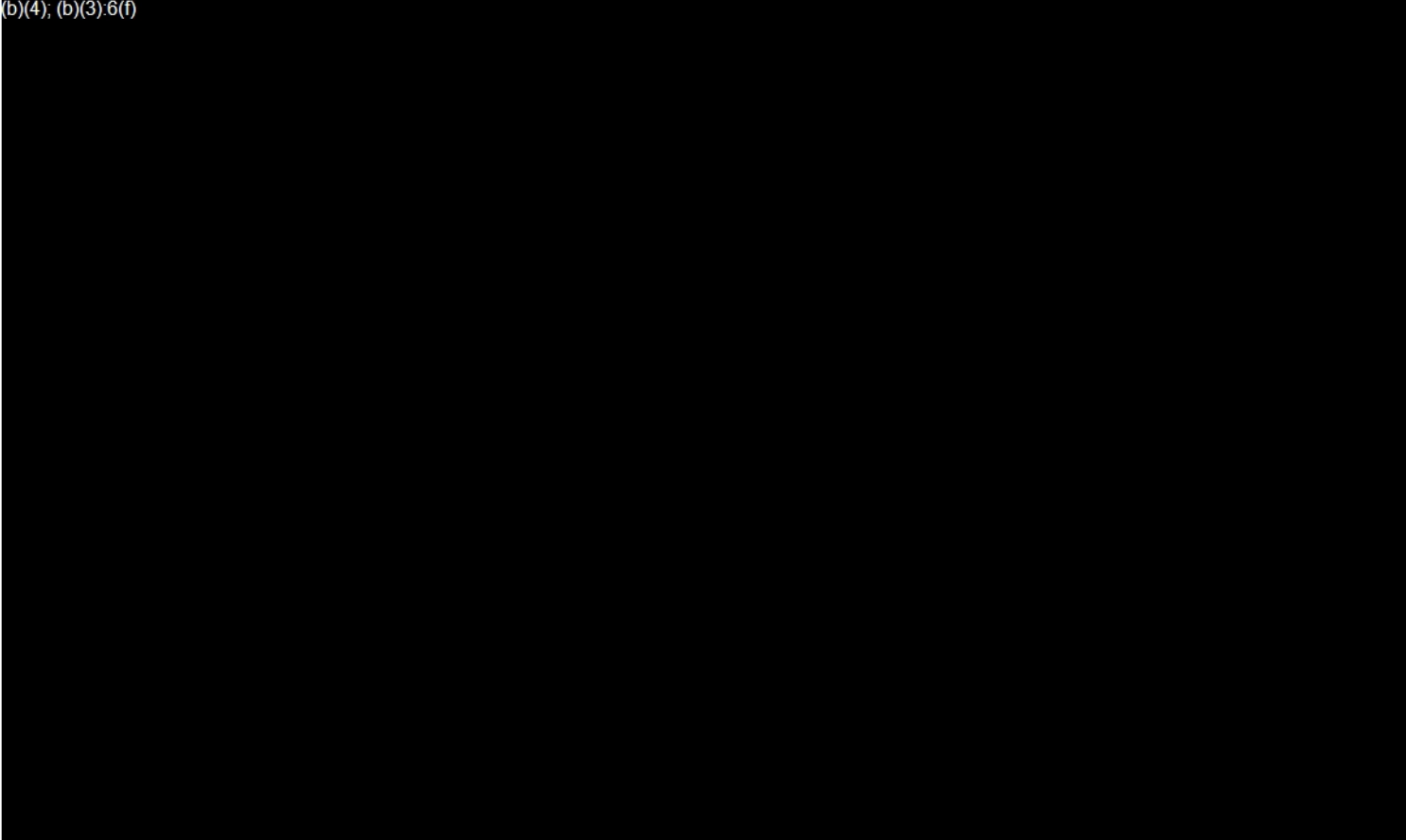
2. (b)(4); (b)(3):6(f)

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

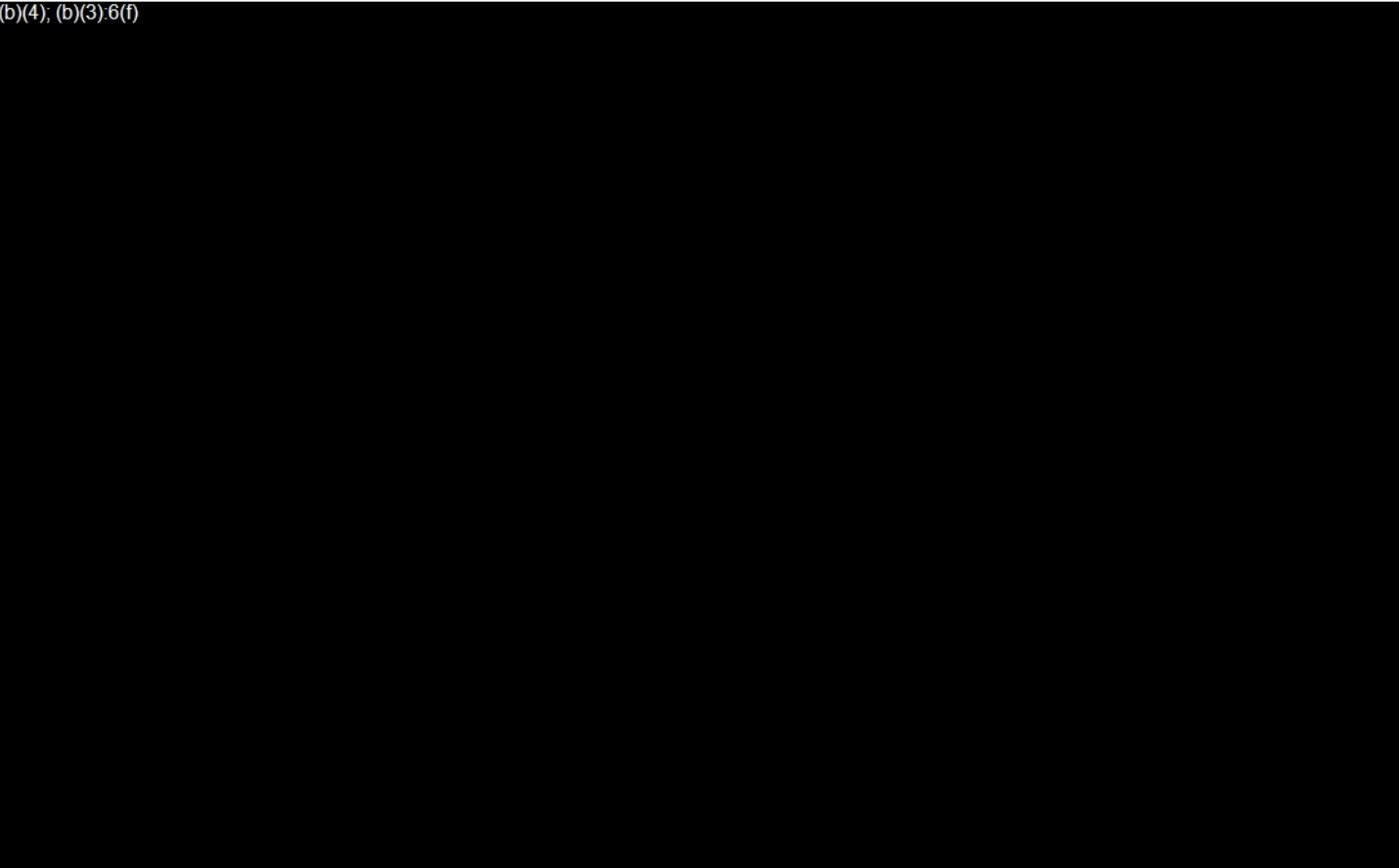
Facebook's Global Privacy Operations team maintains a process for receiving, handling, resolving, monitoring, and reporting external inquiries, a subset of which may be privacy-related complaints, regarding Facebook's privacy practices (refer to Figure III.D.2.i). A user can submit an external inquiry through a web-based contact form or through a physical mailing address, both of which are located on the Facebook Data Policy site. (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)

The [redacted] provided free online privacy dispute resolution services to anyone who filed an eligible complaint about Facebook. [redacted]

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

[redacted] consumers can continue to escalate privacy-related complaints, including those where the user disagrees with the resolution, through Facebook's existing communication channels. [redacted]

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

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

Facebook's [redacted] (b)(4); (b)(3):6(f) team maintains a process for receiving, handling, resolving, monitoring, and reporting Internal complaints regarding Facebook's privacy practices (refer to Figure III.D.2.iii). (b)(4); (b)(3):6(f)

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

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

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

The [redacted] (b)(4); [redacted] maintains a process to identify, track, assess, and manage issues arising from privacy risks and Safeguards that could impact Facebook's ability to meet its privacy compliance obligations. These issues are specifically identified, tracked, assessed, and managed as privacy issues. (b)(4); (b)(3):6(f)

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

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

- External Privacy Complaints: (b)(4); (b)(3):6(f)

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

- Internal Privacy Complaints: (b)(4); (b)(3):6(f)

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

- External Assessment: (b)(4); (b)(3):6(f)

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

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

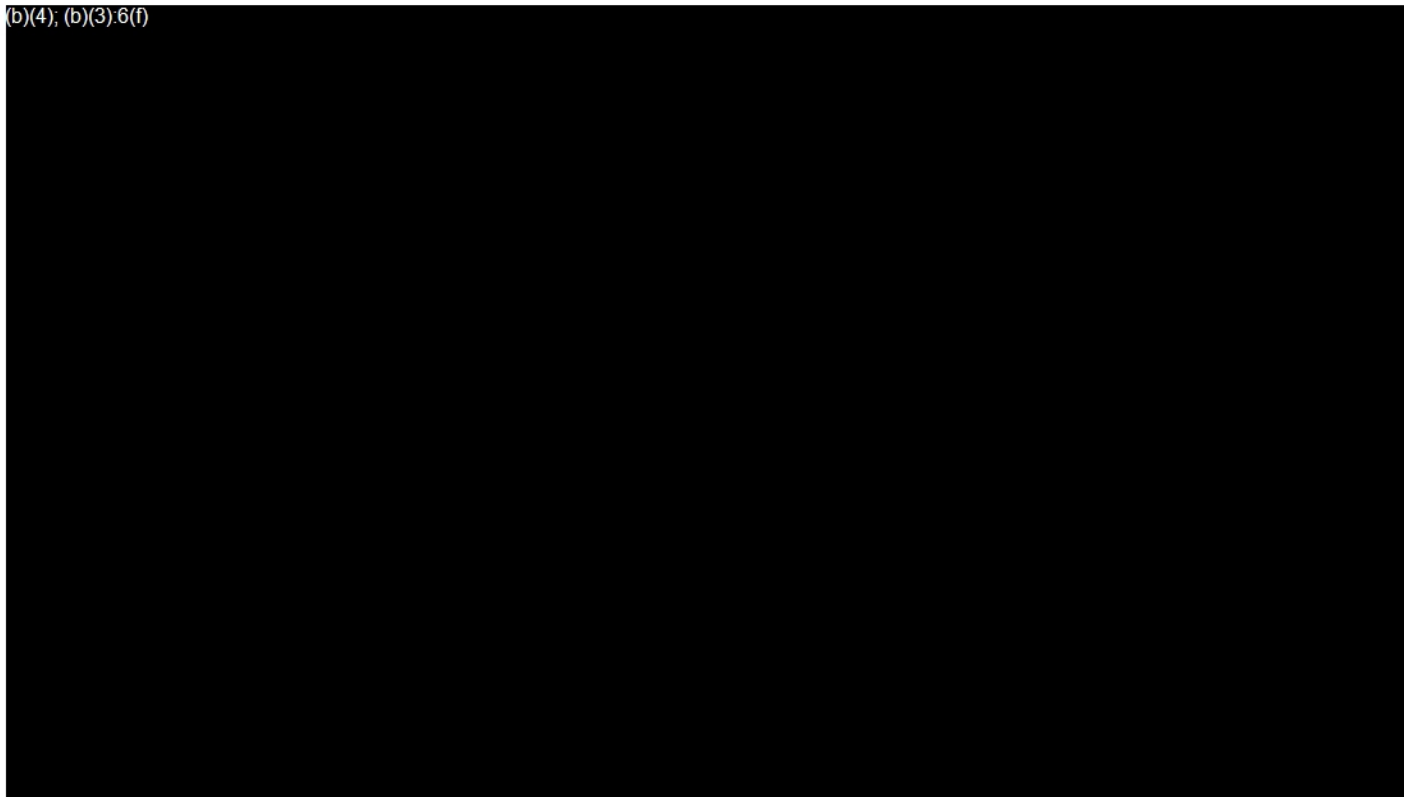
(b)(4); (b)(3):6(f)

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

The Assessor evaluated the end-to-end processes executed by Facebook, including receiving, handling, resolving, monitoring, and reporting privacy-related complaints and issues. Our evaluation of the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) included the review of over (b)(4); (b)(3):6(f) documents, reports, and evidence of the complaints process and Issue Management process related to privacy-related matters. Key documentation reviewed included, but was not limited to, the following:

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

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



The Assessor's evaluation of the (b)(4); (b)(3):6(f) included facilitating approximately (b)(4); (b)(3):6(f) interviews with key stakeholders, (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f)

The Safeguards identified as part of the (b)(4); (b)(3):6(f) were assessed through design and operating effectiveness testing as described in the Section II – Assessment Methodology above. Our testing included evaluation of (b)(4); (b)(3):6(f) Safeguards aligned to the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) In alignment with the Assessment Methodology, we performed over (b)(4) sample tests (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f). An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing included reviews of procedural documentation and completion of walkthroughs with Safeguard Owners to understand the design of the Safeguards and associated processes. Where applicable, a demonstration was provided by Facebook to show the progression of specific processes to better understand how the Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the

(b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) were as follows:

- Evaluated whether the processes for receiving, handling, responding to, and documenting external complaints regarding Facebook's privacy practices were designed to assess and resolve complaints;
- Evaluated whether the processes for receiving, handling, responding to, and documenting internal complaints regarding Facebook's privacy practices were designed to assess and resolve complaints; and
- Evaluated whether the processes to document and monitor the resolution of issues related to privacy risks (b)(4); (b)(3):6(f) surfaced during compliance reviews, assessments, and audits were designed to assess whether appropriate and timely action is taken.



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

Our operating effectiveness testing included detailed reviews of samples across (b)(4); (b)(3):6(f) Safeguards for which sample-based testing was executed, leveraging the sample methodology described in Section II – Assessment Methodology. The key objectives and our test procedures for operating effectiveness testing for the (b)(4); (b)(3):6(f)

were as follows:

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

4. (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)

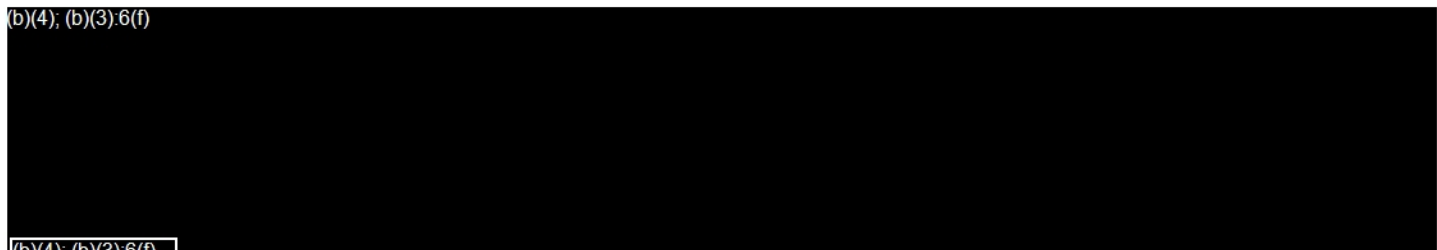
(b)(4); (b)(3):6(f)



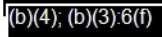
(b)(4); (b)(3):6(f)



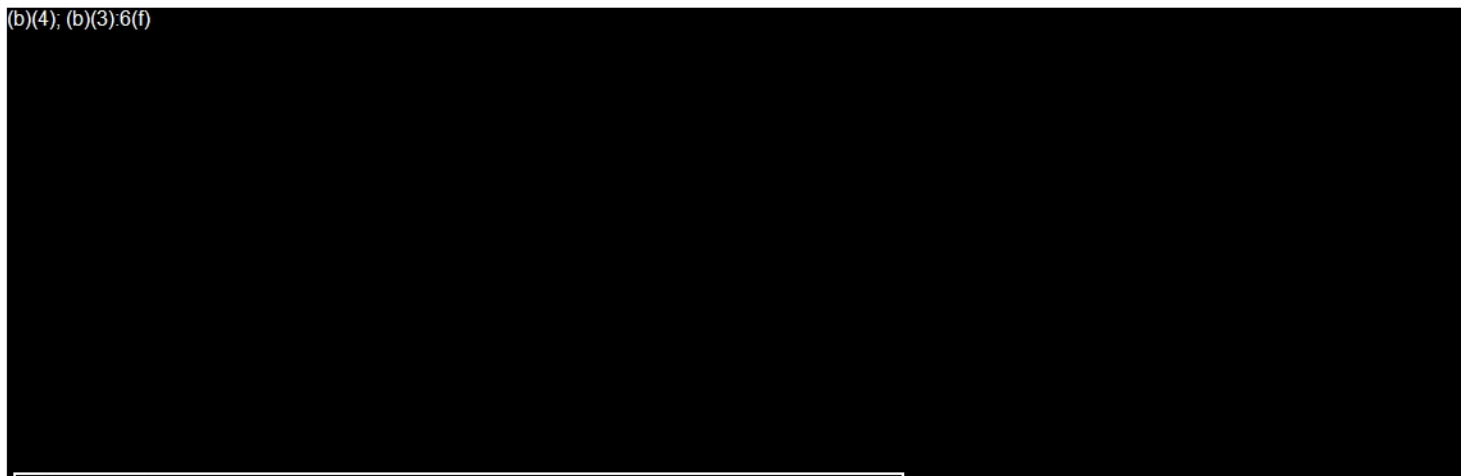
(b)(4); (b)(3):6(f)




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



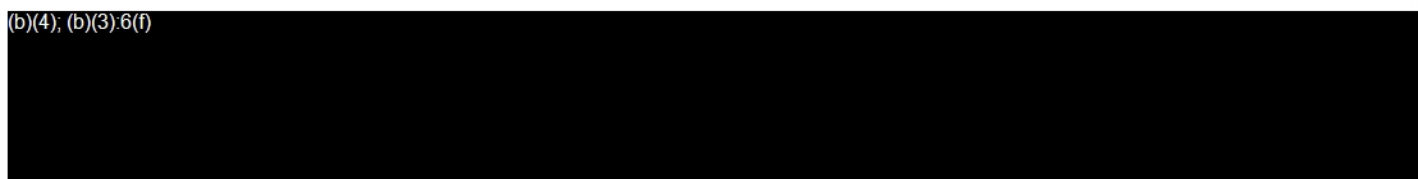
(b)(4); (b)(3):6(f)



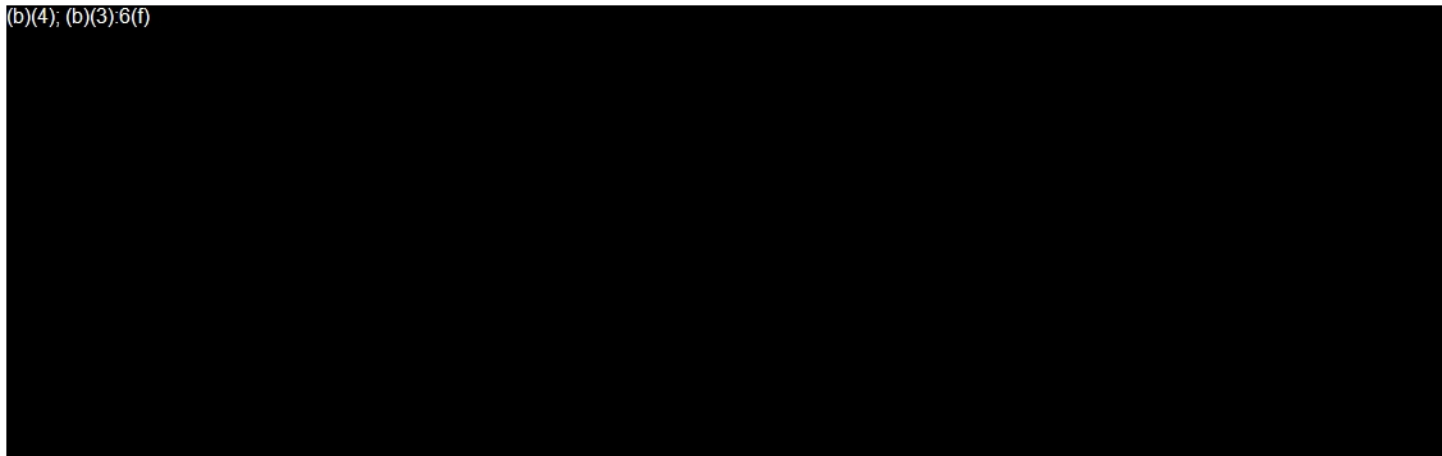
(b)(4); (b)(3):6(f)



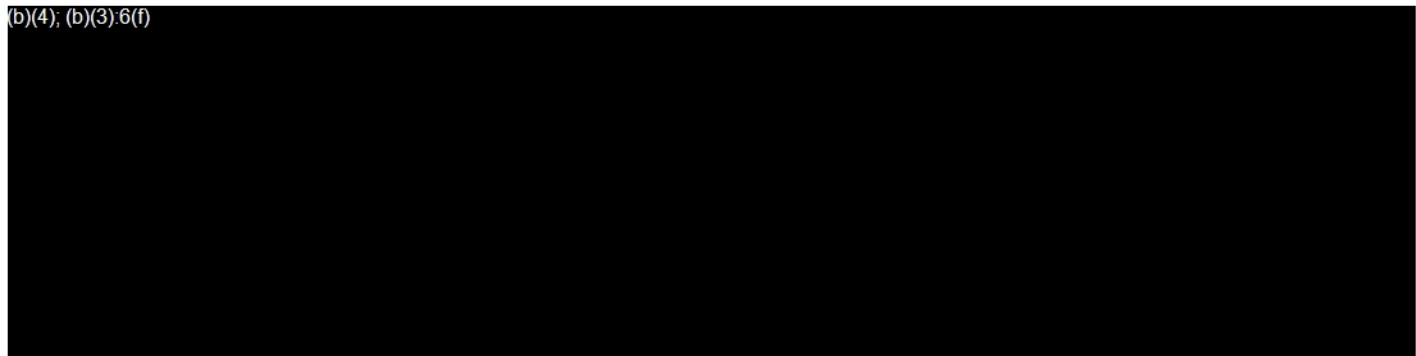
(b)(4); (b)(3):6(f)




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



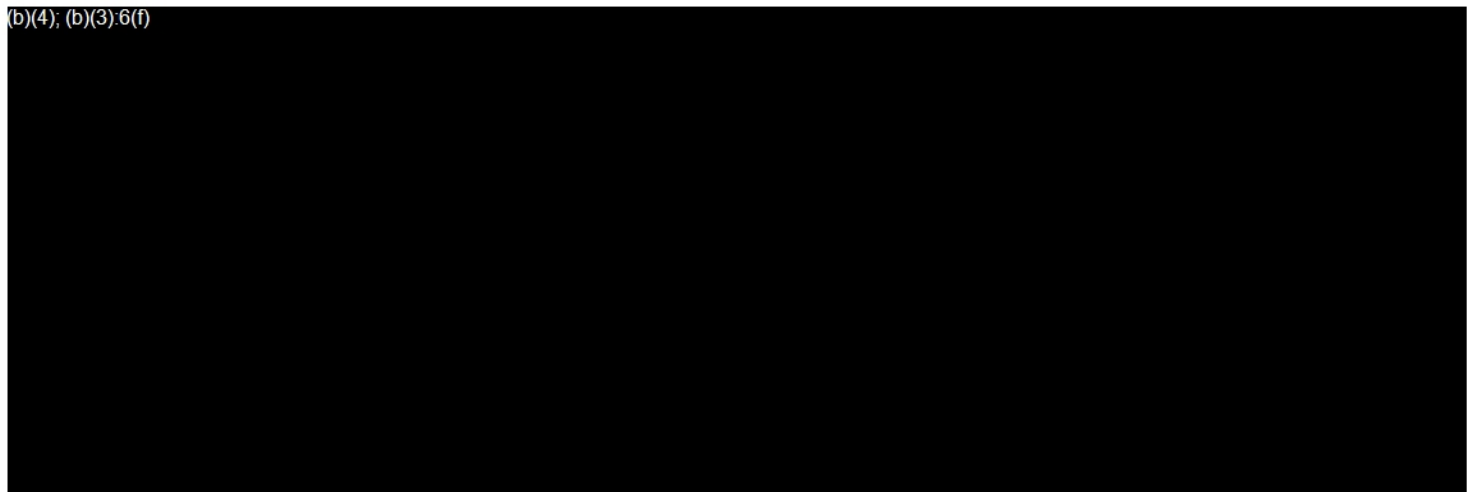
(b)(4); (b)(3):6(f)



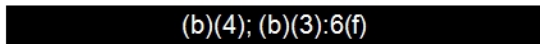
(b)(4); (b)(3):6(f)




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



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

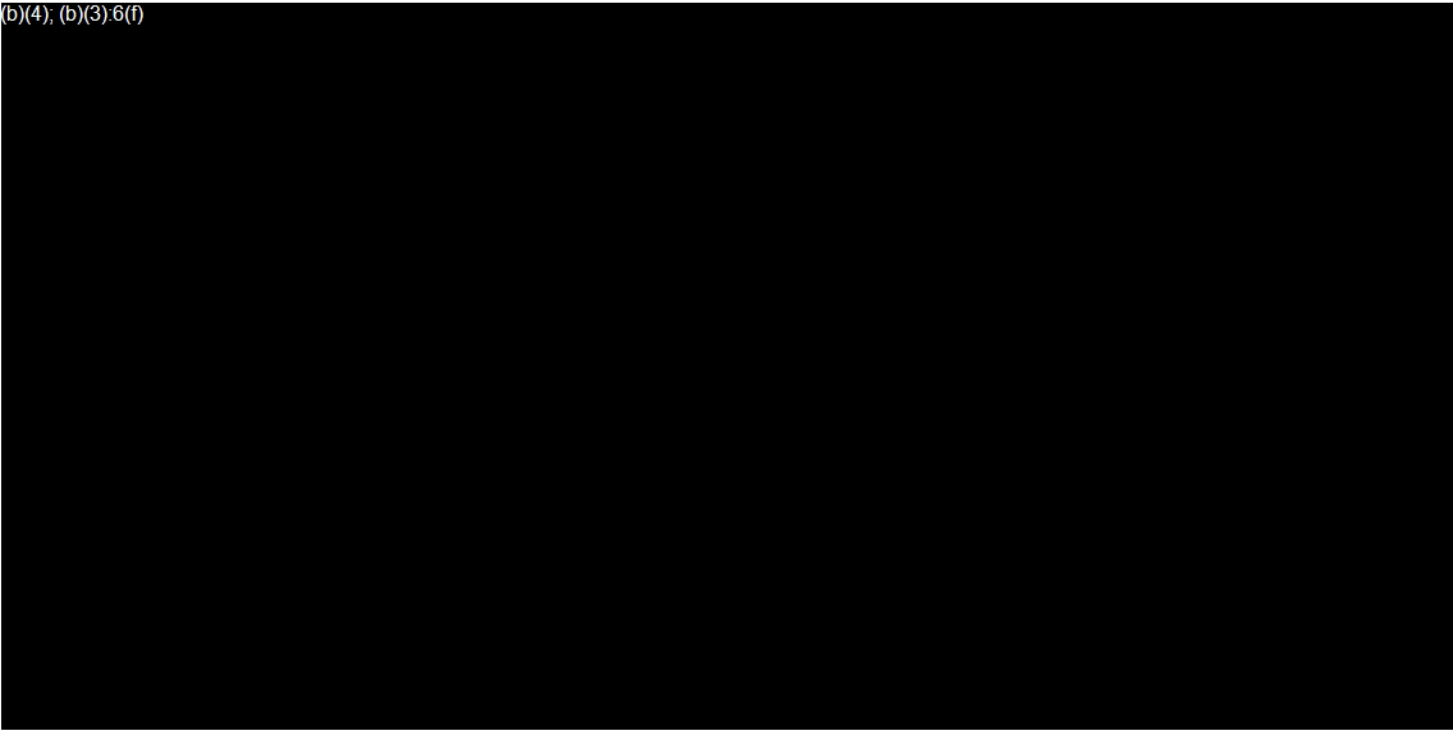


(b)(4); (b)(3):6(f)





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



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

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

Within the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f), Facebook has established an annual Privacy Risk Assessment (PRA) process.

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

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

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

Part VII.D: Assess and document, at least once every twelve (12) months, internal and external risks in each area of operation to the privacy, confidentiality, or Integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of such information.

Assess and document internal and external risks as described above as they relate to a Covered Incident, promptly following verification or confirmation of such an Incident, not to exceed thirty (30) days after the incident is verified or otherwise confirmed.

Part VII.E: Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

Part VII.J: Evaluate and adjust the Privacy Program in light of any material changes to Respondent’s operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Part VII.D. of this Order, and any other circumstances that Respondent knows or has reason to believe may have a material impact on the effectiveness of the Privacy Program. Respondent may make this evaluation and adjustment to the Privacy Program at any time, but must, at a minimum, evaluate the Privacy Program at least once every twelve (12) months and modify the Privacy Program as necessary based on the results.

The (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) was designed to include (b)(4); (b)(3):6(f) Safeguards. (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) Refer to Appendix A for details on the specific Safeguards within the (b)(4); (b)(3):6(f)

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

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

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

The Assessor considered standards including the National Institute of Standards and Technology (NIST) Privacy Framework and the Generally Accepted Privacy Principles (GAPP) to evaluate the completeness of the Risk Register and the Safeguard environment and to evaluate the approach Facebook took to executing (b)(4). We evaluated the end-to-end process executed by Facebook,

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

Our evaluation of (b)(4); included the review of over (b)(4) documents, reports, and evidence of the (b)(4); outputs. Key documentation we reviewed included but was not limited to the following:

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

We conducted over [redacted] interviews with key stakeholders, [redacted]

[redacted]

[redacted] The Safeguards identified as part of the [redacted] were covered through design and operating effectiveness testing as described in Section II – Assessment Methodology above. Our testing included the evaluation of [redacted] Safeguards [redacted]

[redacted]

[redacted] In alignment with the Assessment Methodology, we performed over [redacted] sample tests [redacted]

The testing of the [redacted] [redacted] included deviations for the testing of Safeguards [redacted] which included the evaluation of [redacted] and the [redacted] (b)(4); (b)(3):6(f) Through the testing of these activities, we did not conduct sample-based testing, but rather evaluated the full population of results of the Safeguards. An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how the Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the [redacted] (b)(4); (b)(3):6(f) were as follows:

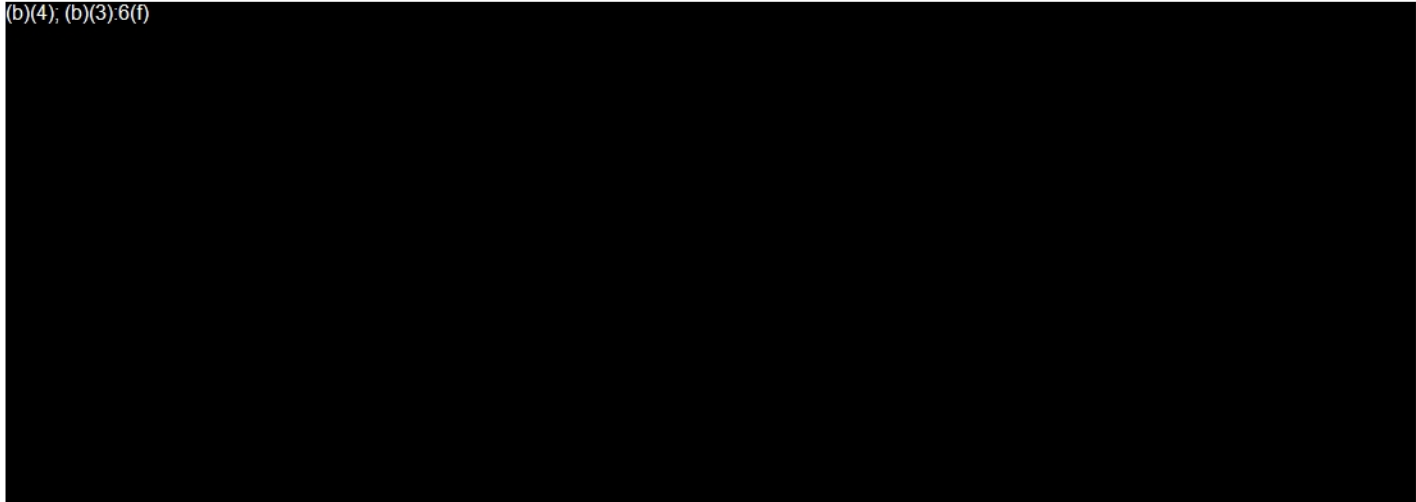
- Evaluated if the design and approach of [redacted] (b)(4); [redacted] complied with the Order requirements and was consistent with standards commonly accepted in the industry by analyzing the [redacted] (b)(4); (b)(3):6(f) [redacted], which defines the execution approach for [redacted] (b)(4); [redacted] and through conducting interviews with the [redacted] (b)(4); (b)(3):6(f) [redacted];
- Determined if the [redacted] (b)(4); (b)(3):6(f) [redacted];
- Assessed whether the adequacy of the [redacted] (b)(4); (b)(3):6(f) [redacted] approach and process was developed by evaluating the [redacted] (b)(4); (b)(3):6(f) [redacted] and [redacted] (b)(4); (b)(3):6(f) [redacted];
- Evaluated whether the design of the supporting risk assessment processes, [redacted] (b)(4); (b)(3):6(f) [redacted] were adequate by reviewing the respective procedural documentation and conducting interviews with the respective Safeguard Owners.

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

Our operating effectiveness testing included evaluating the results of [redacted] by testing [redacted] (b)(4); [redacted] Safeguards, consistent with the sampling methodology described in Section II - Assessment Methodology above. The key objectives and our test procedures for operating effectiveness testing for the [redacted] (b)(4); (b)(3):6(f) were as follows:

- Validated that all relevant privacy risks were identified through the [redacted] (b)(4); [redacted] process by evaluating the [redacted] (b)(4); [redacted] against the NIST and GAPP standards;

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




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

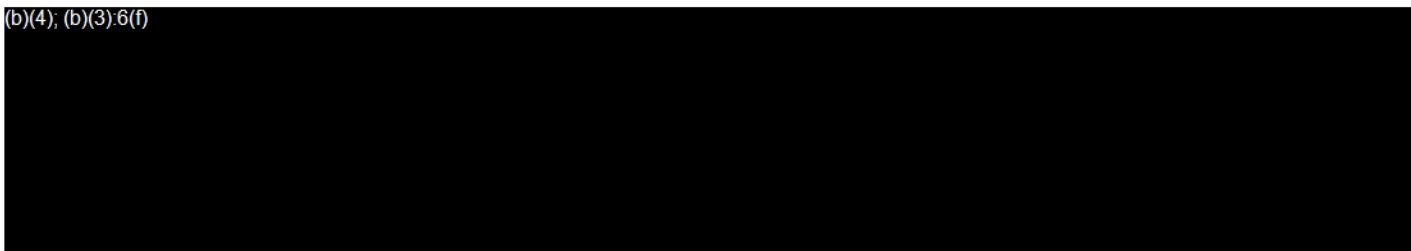
(b)(4);

Part VII.D of the Order requires that Facebook “(a)ssess and document...internal and external risks in each area of its operation...to the privacy, confidentiality, or Integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of such information.” Further, Part VII.E requires Facebook to “Design, implement, maintain, and document Safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D...”. The Order requires that Facebook comply with the requirements of both Part VII.D and Part VII.E within 180 days of the Order effective date.

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



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



Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



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

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

Facebook established (b)(4); (b)(3):6(f) for managing compliance with the MPP, including monitoring and enforcing Program policies and requirements, and reporting on Program results. These (b)(4); (b)(3):6(f) were aggregated to create the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f)

Through associated (b)(4); (b)(3):6(f) and Safeguards, Facebook designed (b)(4); (b)(3):6(f) to address both Order requirements and industry standards. In relevant part, the Order sub-requirements related to (b)(4); (b)(3):6(f) include:

Part VII.B: Provide any evaluations thereof or adjustments to the written program required under Part VII.A. of the Order the Principal Executive Officer and to the Independent Privacy Committee created in response to Part X of the Order at least once every twelve (12) months.

Part VII.E: Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

Part VII.E.2.c: The Designated Compliance Officer(s) shall deliver a quarterly report (Quarterly Privacy Review Report) to the Principal Executive Officer and to the Assessor that provides: (i) a summary of the Privacy Review Statements generated during the prior fiscal quarter under Part VII.E.2.b, including a detailed discussion of the material risks to the privacy, confidentiality, and Integrity of the Covered Information that were identified and how such risks were addressed; (ii) an appendix with each Privacy Review Statement generated during the prior fiscal quarter under Part VII.E.2.b; and (iii) an appendix that lists all privacy decisions generated during the prior fiscal quarter under Part VII.E.2.a

Part VII.E.2.d: The appendices required under Part VII.E.2.c.(ii) and (iii) shall be provided to the Assessor no fewer than twenty-one (21) days in advance of the quarterly meeting of the Independent Privacy Committee as specified in Part X.A.5. A copy of the summary in the Quarterly Privacy Review Report required under VII.E.2.c.(i) shall be provided to Assessor no fewer than fourteen (14) days in advance of the quarterly meeting

Part VII.E.2.e: A copy of the Quarterly Privacy Review Report shall also be furnished, upon request, to the Commission

Part VII.F: Assess, monitor, and test, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the effectiveness of any safeguards put in place pursuant to Part VII.E. of this Order to address risks to the privacy, confidentiality, or Integrity of Covered Information, and modify the Privacy Program based on the results.

Additionally, to enforce employee compliance with Part VII of the Order, Facebook implemented measures to discipline Employees (and agents, contingent workers, or representatives who have access to Covered Information) who violate Facebook’s privacy policies and data handling practices, as appropriate.

Facebook also implemented a records management program that is designed to identify and define record retention requirements necessary to support and evidence the operation of the U.S. Privacy Program (Part VII of the Order), including procedures for confirming the appropriate retention of records.



The above referenced Order requirements are addressed through (b)(4); (b)(3):6(f) Safeguards<sup>28</sup> which were designed, implemented, and executed during the Assessment Period. As described within this section:

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

Refer to Appendix A for details on the specific in-scope Safeguards within (b)(4); (b)(3):6(f).

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

To comply with Part VII.F Order requirement, Facebook implemented (b)(4); (b)(3):6(f) Safeguards intended to assist Facebook's assessment, monitoring and testing of the effectiveness of implemented privacy Safeguards. (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)(4); (b)(3):6(f)

---

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

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

[Redacted]

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

To comply with its obligations to assess risk and review Safeguards following a Covered Incident (CI), Facebook conducts a Covered Incident Privacy Risk Assessments (CIPRA).

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

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

[Redacted]

[Redacted]

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

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

[Redacted]

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

[Redacted]

<sup>29</sup> Under Part VII.F of the Order, assessment, monitoring, and testing activities are required to occur at least once every twelve (12) months. Such assessments are required to occur within thirty (30) days following the resolution of a Covered Incident.

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

[Redacted]

[Redacted]

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

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

#### Quarterly Privacy Review Reporting

Quarterly reports are delivered to the Principal Executive Officer and to the Assessor that provide a summary of the Privacy Review Statements generated during the prior fiscal quarter in accordance with Part VII.E.2.b of the Order. The reports include a discussion of the material risks to the privacy, confidentiality, and integrity of the Covered Information, that were identified and how such risks were addressed; an appendix with each Privacy Review Statement (PRS) generated during the prior fiscal quarter pursuant to Part VII.E.2.b of the Order; and an appendix that lists all privacy decisions generated during the prior fiscal quarter pursuant to Part VII.E.2.a of the Order.

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

Facebook provides briefings to the Privacy Committee at least quarterly on privacy-related matters, including the state of the Mandated Privacy Program, compliance with the Order, and material risks to the privacy, confidentiality and integrity of Covered Information. Facebook also provides the Privacy Committee an annual briefing on Facebook's assessment of material risks to the privacy, confidentiality, and integrity of Covered Information and steps taken or planned to monitor or mitigate such risks, including procedures and policies with respect to risk assessment and risk management.

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

(b)(4); (b)(3):6(f) Inclusive in its recordkeeping activities, Facebook has developed training about the importance of recordkeeping at the company and a plan for monitoring and testing compliance with its recordkeeping policy and process.

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

The Assessor evaluated the design and implementation of each of the processes that comprise Safeguards within the (b)(4); (b)(3):6(f) Control Domain from end-to-end, (b)(4); (b)(3):6(f)

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

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

We reviewed over (b)(4); (b)(3):6(f) documents, reports, and evidence of the underlying processes including the following:

(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)

We conducted over [redacted] interviews with key stakeholders, (b)(4), (b)(3):6(f)

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

(b)(4); (b)(3):6(f) In alignment with the Assessment Methodology, we performed over (b) sample tests (b)(4); (b)(3):6(f). An overview of our design and operating effectiveness testing is described below.

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

Our design effectiveness testing included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how the documented Safeguards achieve their corresponding

(b)(4); (b)(3):6(f) In conducting design effectiveness testing of the Safeguards within (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f), our key objectives and test procedures sought to determine the adequacy and comprehensiveness of Safeguard documentation detailing:

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

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

Assessor's operating effectiveness testing included selecting and testing samples across the (b) Safeguards for which sample-based testing was appropriate, leveraging the sample methodology described in Section II – Assessment Methodology. The key objectives and our test procedures for operating effectiveness testing for the

(b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) were as follows:

- 
- 
- 
- 
- 

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

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

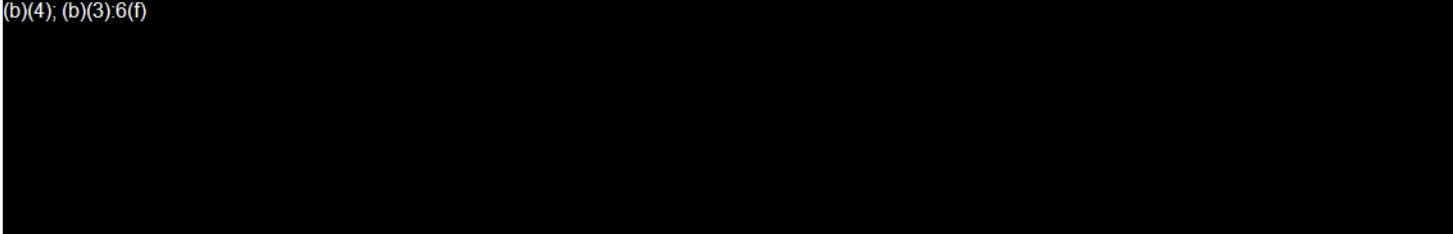


Withheld pursuant to exemption

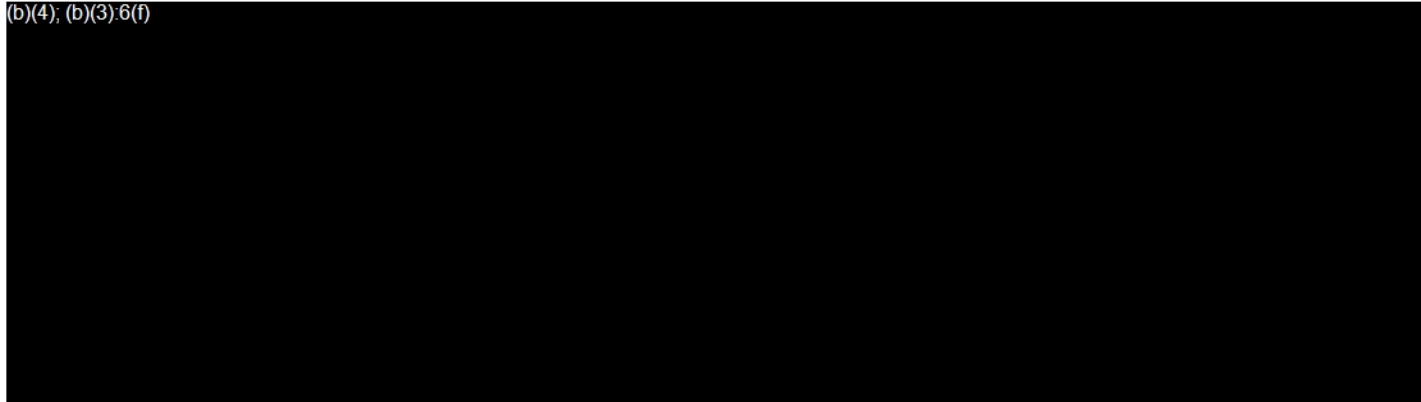
(b)(4); (b)(3):6(f)

of the Freedom of Information and Privacy Act

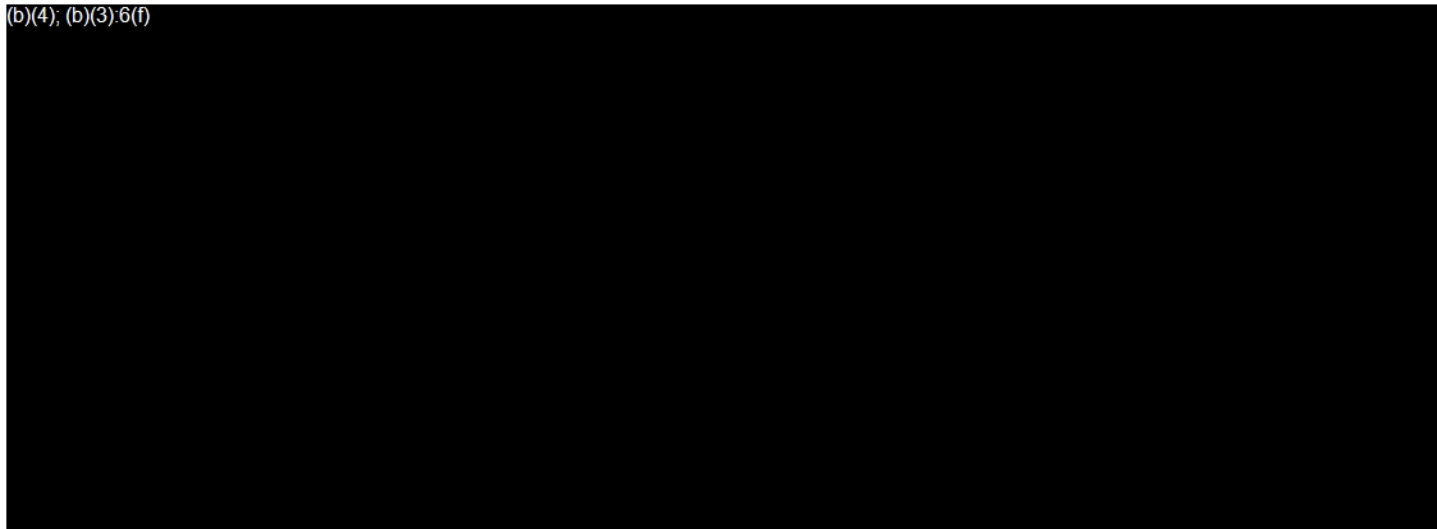
(b)(4); (b)(3):6(f)

A large black rectangular redaction box covering the majority of the page's content.

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

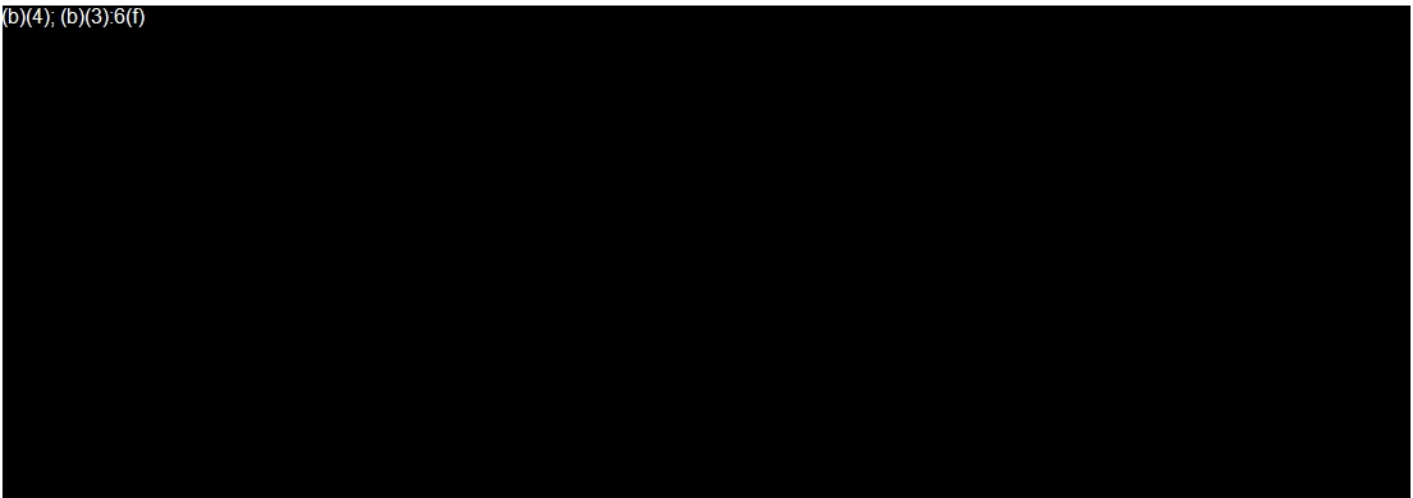
A large black rectangular redaction box covering the majority of the page's content.

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


A large black rectangular redaction box covering the majority of the page's content.

---

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

A large black rectangular redaction box covering the majority of the page's content.

<sup>41</sup> Under Part VII.F. of the Order, the effectiveness of Safeguards must be assessed and tested at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident. As detailed in the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) Facebook has designed a process to test each Safeguard annually.

A small black rectangular redaction box at the bottom left of the page.

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

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

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

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

<sup>43</sup> Part VII.F. of the Order requires Facebook to assess, monitor, and test, at least once every twelve (12) months the effectiveness of such Safeguards and modify the Privacy Program based on the results.

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

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

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

Pursuant to Part VII.E.2.c. of the Order, a quarterly report is to be delivered to the Principal Executive Officer and to the Assessor that provides:

- i. a summary of the Privacy Review Statements (PRS) generated during the prior fiscal quarter under Part VII.E.2.b of the Order, including a detailed discussion of the material risks to the privacy, confidentiality, and Integrity of the Covered Information that were identified and how such risks were addressed;
- ii. an appendix with each PRS generated during the prior fiscal quarter under Part VII.E.2.b of the Order; and
- iii. an appendix that lists all privacy decisions generated during the prior fiscal quarter under Part VII.E.2.a of the Order.

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

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

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

As described in the Mandated Privacy Program Document, Facebook's (b)(4); (b)(3):6(f) has established the (b)(4); (b)(3):6(f) process. (b)(4); (b)(3):6(f)

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

Facebook designed the (b)(4); (b)(3):6(f) to address multiple Order requirements through associated (b)(4); (b)(3):6(f) and Safeguards. In relevant part, the Order sub-requirements related to the (b)(4); (b)(4); (b)(4); include:

Part VII.E: Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information;

Part VII.E.2: Specifically with respect to Respondent's collection, use, or sharing of Covered Information in any new or modified product, service, or practice, such safeguards shall include:

Part VII.E.2.A: Prior to implementing each new or modified product, service, or practice, (i) conducting a privacy review that assesses the risks to the privacy, confidentiality, and Integrity of the Covered Information, the safeguards in place to control such risks, and the sufficiency of the User notice and, if necessary, consent; and (ii) documenting a description of each reviewed product, service, or practice that was ultimately implemented; any safeguards being implemented to control for the identified risks; and the decision or recommendation made as a result of the review (e.g., whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected)

Part VII.E.2.B: For each new or modified product, service, or practice that presents a material risk to the privacy, confidentiality, or Integrity of the Covered Information (e.g., a completely new product, service, or practice that has not been previously subject to a privacy review; a material change in the sharing of Covered Information with a Facebook-owned affiliate; a modified product, service, or practice that includes a material change in the collection, use, or sharing of Covered Information; a product, service, or practice directed to minors; or a product, service, or practice involving health, financial, biometric, or other similarly sensitive information), producing a written report ("Privacy Review Statement") that describes:

Part VII.E.2.B.1: The type(s) of Covered Information that will be collected, and how that Covered Information will be used, retained, and shared;

Part VII.E.2.B.2: The notice provided to Users about, and the mechanism(s), if any, by which Users will consent to, the collection of their Covered Information and the purposes for which such information will be used, retained, or shared by Respondent;

Part VII.E.2.B.3: Any risks to the privacy, confidentiality, or Integrity of the Covered Information;

Part VII.E.2.B.4: The existing safeguards that would control for the identified risks to the privacy, confidentiality, and Integrity of the Covered Information and whether any new safeguards would need to be implemented to control for such risks;

Part VII.E.2.B.5: Any other known safeguards or other procedures that would mitigate the identified risks to the privacy, confidentiality, and Integrity of the Covered Information that were not implemented, such as minimizing the amount or type(s) of Covered Information that is collected, used, and shared; and each reason that those alternates were not implemented;

Part VII.E.2.C: The Designated Compliance Officer(s) shall deliver a quarterly report (“Quarterly Privacy Review Report”) to the Principal Executive Officer and to the Assessor that provides: (i) a summary of the Privacy Review Statements generated during the prior fiscal quarter under Part VII.E.2.b, including a detailed discussion of the material risks to the privacy, confidentiality, and Integrity of the Covered Information that were identified and how such risks were addressed; (ii) an appendix with each Privacy Review Statement generated during the prior fiscal quarter under Part VII.E.2.b; and (iii) an appendix that lists all privacy decisions generated during the prior fiscal quarter under Part VII.E.2.a;

Part VII.E.4: Specifically with respect to Respondent’s sharing of Covered Information with any other Facebook-owned affiliate, Respondent shall design, implement, maintain, and document safeguards that control for risks to the privacy, confidentiality, and Integrity of such Covered Information, based on the volume and sensitivity of such Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information; and

Part VII.E.5: Specifically with respect to facial recognition, such safeguards shall include: a. Prior to using or sharing any Facial Recognition Template for a User in a manner that materially exceeds the types of uses or sharing disclosed to that User at the time that User’s consent was previously obtained, (i) Clearly and Conspicuously disclosing (such as in a stand-alone disclosure or notice), separate and apart from any “Privacy Policy,” “data policy,” “statement of rights and responsibilities” page, or other similar document, how Respondent will use or, to the extent applicable, share, such Facial Recognition Template; and (ii) Obtaining the User’s affirmative express consent; b. Nothing in this provision shall limit Respondent’s ability to use Facial Recognition Templates for fraud prevention or remediation, or protecting the safety, reliability and security of Respondent’s platform or Users, so long as Respondent discloses these types of uses in Respondent’s Privacy Policy or similar document.

The (b)(4); (b)(3):6(f) within the (b)(4); (b)(3):6(f) are addressed through (b)(4); (b)(3):6(f) Safeguards, (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f)

[Redacted]

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

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

[Redacted]

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



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

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

The Assessor evaluated the coverage, consistency and efficacy of the (b)(4); (b)(3):6(f) process and the enforcement of (b)(4); (b)(3):6(f). The scope of the Assessor's evaluation included the intake of changes into the (b)(4); (b)(3):6(f) process, the execution of the (b)(4); (b)(3):6(f) to identify risks and associated mitigations, and the enforcement of the implementation of the mitigations, along with the governance controls overseeing the end-to-end process.

Our evaluation of the (b)(4); (b)(3):6(f) included the review of over (b)(4) documents, reports, and evidence of the (b)(4); (b)(3):6(f) process outputs. Key documentation we reviewed included but was not limited to the following:

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

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

We conducted over (b)(4); (b)(3):6(f) interviews with key stakeholders, (b)(4); (b)(3):6(f)

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

The Safeguards identified as part of the (b)(4); (b)(3):6(f) were covered through design and operating effectiveness testing as described in Section II – Assessment Methodology above. Our testing included evaluation of samples across (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) Safeguards aligned to the (b)(4); (b)(3):6(f)

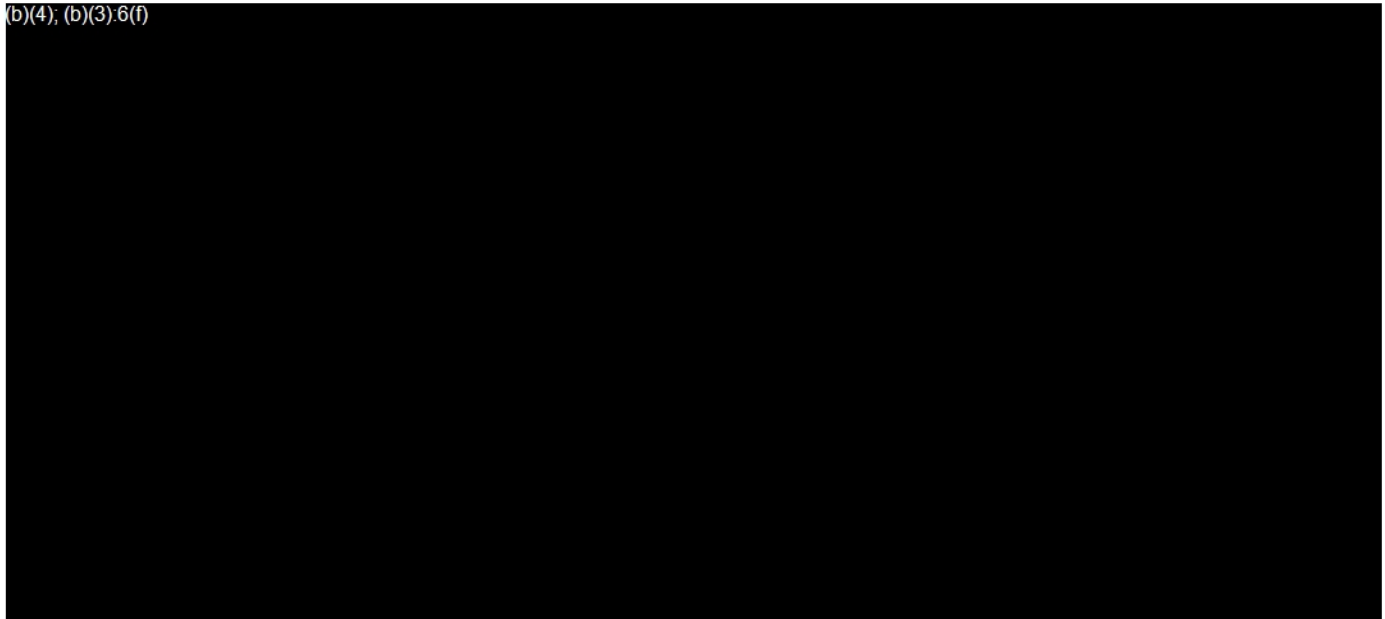
(b)(4); (b)(3):6(f). In alignment with the Assessment Methodology, we performed over 4 (b)(4); (b)(3):6(f) sample tests (b)(4); (b)(3):6(f). An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how the Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) were as follows:

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

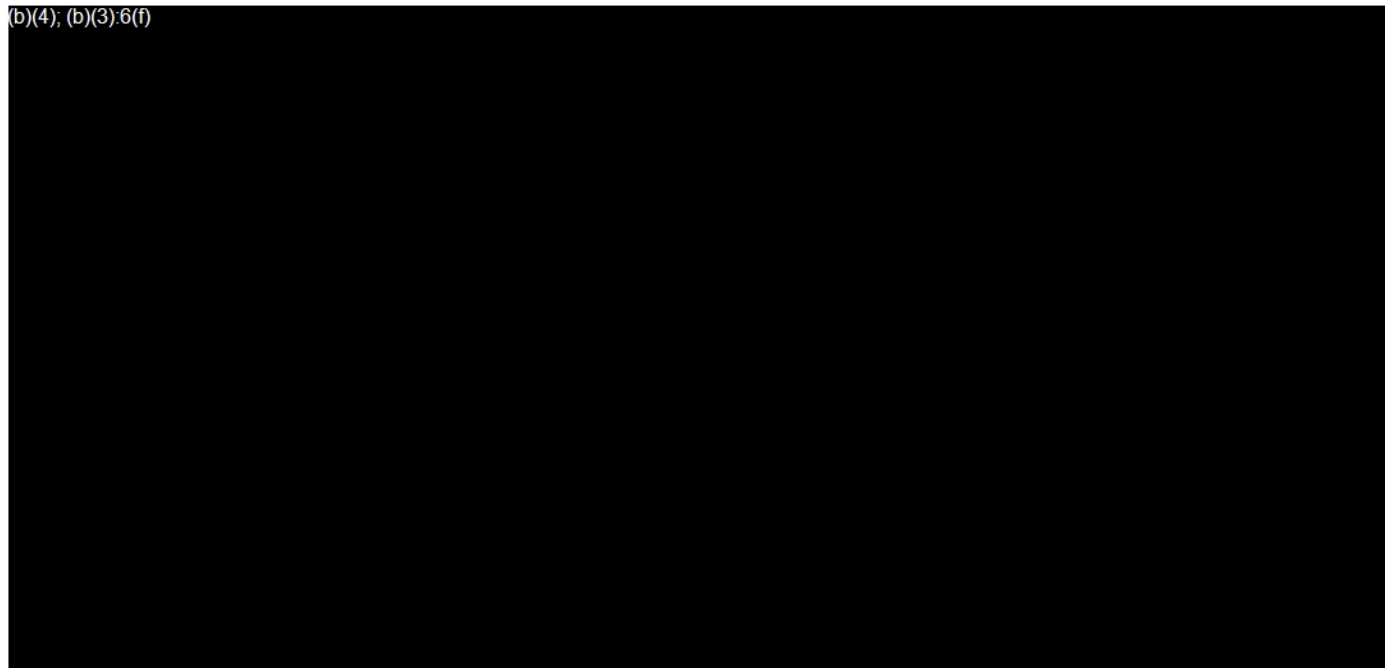
(b)(4); (b)(3):6(f)



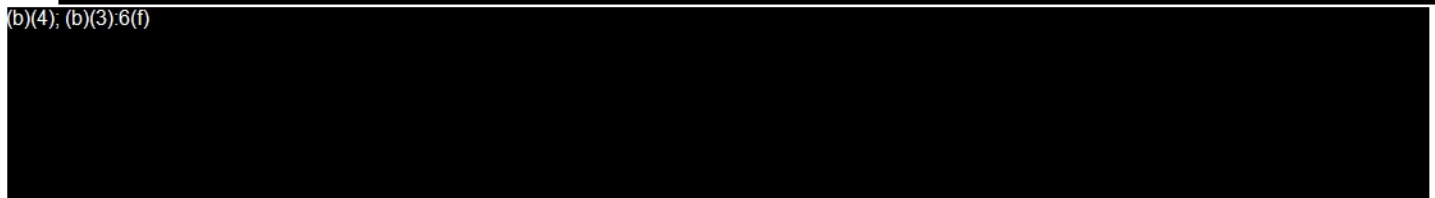
(b)(4); (b)(3):6(f)

Our operating effectiveness testing included evaluating the end-to-end process, as defined above. The key objectives and our test procedures for operating effectiveness testing for the were as follows:

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



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



to limitations in identifying a complete and accurate population of (b)(4); (b)(3):6(f) specific to criteria<sup>49</sup> called out in the Order, the Assessor was provided approximate populations by Facebook utilizing the current querying capabilities available to Facebook and those approximate populations were used for sampling.

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

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

At the time of the assessment, Facebook employed approximately (b)(4); (b)(3):6(f), deployed approximately (b)(4); (b)(3):6(f) code changes quarterly, and conducted over (b)(4); (b)(3):6(f) quarterly<sup>50</sup>.

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

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

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

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

As described in the Mandated Privacy Program, the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) was created to establish standards for the deletion and retention of data, the management or prevention of surfacing deleted data to third parties (anyone outside of the Facebook Organization), and the sharing of Covered Information between Facebook and Facebook-owned affiliates. Facebook has organized a central team to oversee their data management programs and verify its compliance with the Order requirements relative to this (b)(4); (b)(3):6(f)

Facebook designed the (b)(4); (b)(3):6(f) (b)(4); to address multiple Order requirements through associated (b)(4); and Safeguards. In relevant part, the Order sub-requirement related to the (b)(4); (b)(4); (b)(3):6(f) includes:

Part VII.E: Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

The (b)(4); (b)(3):6(f) within the (b)(4); (b)(3):6(f) are addressed through (b)(4); Safeguards, (b)(4); (b)(3):6(f)

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

At Facebook, data is stored in many different systems. (b)(4); (b)(3):6(f)

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

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

The Assessor evaluated the coverage, consistency, and efficacy of the data deletion, retention, and sharing processes and technical enforcement of these controls at a systemic level throughout the data life cycle. The scope of the Assessor’s evaluation included the mechanisms to protect user data in (b)(4); (b)(3):6(f)

Our evaluation of the (b)(4); (b)(3):6(f) included the review of over (b)(4) documents containing system and process documentation, requested screenshots taken during tool testing, code extracts, log files, data extracts from their management systems, and written explanations for topics discussed in meetings. Key documentation we reviewed included but was not limited to the following:

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

We conducted over (b)(4); (b)(3):6(f) interviews with key stakeholders, (b)(4); (b)(3):6(f)

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

The Safeguards identified as part of the (b)(4); (b)(3):6(f) were covered through design and operating effectiveness testing as described in Section II – Assessment Methodology above. Our testing included evaluation of samples, code review, system architecture review, and scenario validation testing techniques across (b)(4) Safeguards aligned to the (b)(4); (b)(3):6(f)

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

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

(b)(4); (b)(3):6(f) In alignment with the Assessment Methodology, we performed over (b)(4) sample tests (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how the Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the (b)(4); (b)(3):6(f) were as follows:

- Determined whether the User Data Deletion Policy (UDDP) and Data Store definition guidelines and standards complied with the Order requirements; and
- Reviewed automated software systems as well as manual processes and determined whether they complied with the UDDP and Data Store governance programs and operated effectively by evaluating:
  - (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 operating effectiveness included evaluating the (b)(4); (b)(3):6(f) systems and processes, as defined above. The key objectives and our test procedures for operating effectiveness testing for the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) were as follows:

- (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)

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

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

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



Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

The (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) establishes standards for maintaining a (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f). The Safeguards in this (b)(4); (b)(3):6(f) detail the processes designed to identify, manage, document, and report Incidents that could impact the privacy, confidentiality or integrity of Covered Information and processes for testing the effectiveness of the (b)(4); (b)(3):6(f)

Facebook designed the (b)(4); (b)(3):6(f) to address Order requirements through associated (b)(4); (b)(3):6(f) and Safeguards. The Order sub-requirements related to the (b)(4); (b)(3):6(f) include:

Part VII.E: Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

Part VII.E.3: Specifically with respect to Respondent’s employees’ access to Covered Information maintained in Respondent’s data warehouse(s), such safeguards shall include designing, implementing, and maintaining access policies and controls that limit employee access to any table(s) or other comparable data storage units known to contain Covered Information to only those employees with a business need to access such Covered Information.

The (b)(4); (b)(3):6(f) includes (b)(4); (b)(3):6(f) Safeguards. (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) Refer to Appendix A for details on the specific Safeguards within the (b)(4); (b)(3):6(f)

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

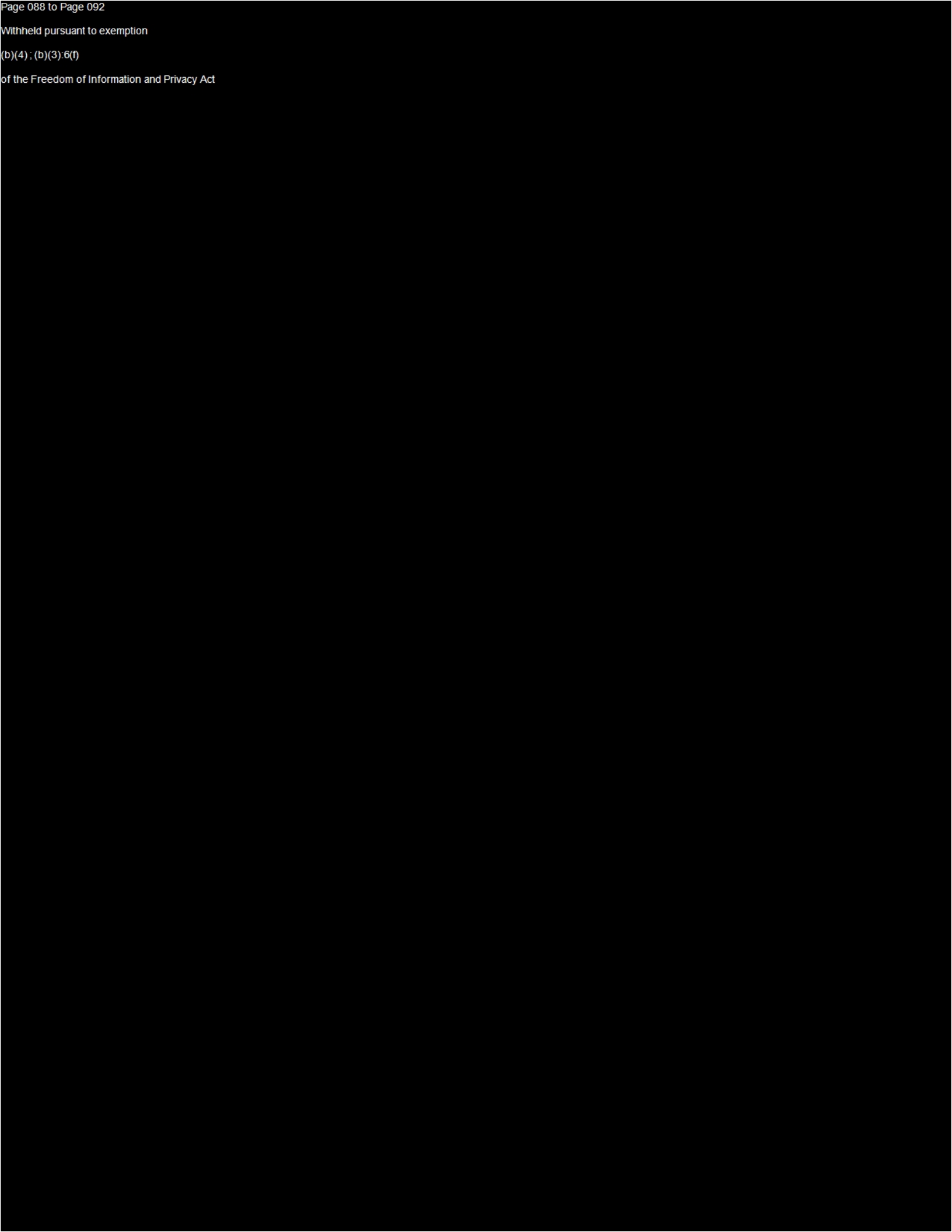
(b)(4); (b)(3):6(f)

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



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

3. (b)(4); (b)(3):6(f)  
The Assessor evaluated the (b)(4); (b)(3):6(f) process executed by Facebook, including identification, investigation, remediation and enforcement, and reporting of privacy-related Incidents relevant to the (b)(4); (b)(4); as described above. Our evaluation of the (b)(4); (b)(3):6(f) (b)(4); included the review of over (b)(4); (b)(3):6(f) documents, reports, and evidence of the (b)(4); (b)(3):6(f) process.

Key documentation reviewed included, but was not limited to, the following:

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

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

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

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

We conducted over [REDACTED] interviews with key stakeholders to gain an understanding of each of the (b)(4); (b)(3):6(f) Safeguards including responsibilities by functional area, the underlying process, and the involvement of any systems or tools utilized as part of the execution of the Safeguard. (b)(4); (b)(3):6(f)

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

The Safeguards identified as part of the [REDACTED] were covered through design and operating effectiveness testing as described in the Section II – Assessment Methodology above. In alignment with the Assessment Methodology, we performed over [REDACTED] sample tests (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how the Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the [REDACTED] (b)(4); (b)(3):6(f) were as follows:

- Determined whether processes were in place to identify, investigate, and document potential Privacy Incidents (evaluated across Incident types whether policy and procedure documentation was sufficient, and roles and responsibilities were clearly defined);
- Determined whether the processes in place to assess, track, and execute remediation and enforcement actions for Privacy Incidents were adequately designed (evaluated across Incident types whether policy and procedure documentation was sufficient, and roles and responsibilities were clearly defined); and
- Determined whether the processes in place for preparing and submitting reports of confirmed Covered Incidents in compliance with the Order requirements were adequately designed (evaluated across Incident types whether policy and procedure documentation was sufficient, and roles and responsibilities were clearly defined).

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

Our operating effectiveness testing included coverage of (b)(4); (b)(3):6(f) Safeguards aligned to the (b)(4); (b)(3):6(f)

(b)(4);

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

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

Our

operating effectiveness testing was consistent with the sampling methodology described in Section II – Assessment Methodology. The key objectives and our test procedures for operating effectiveness testing for the (b)(4);

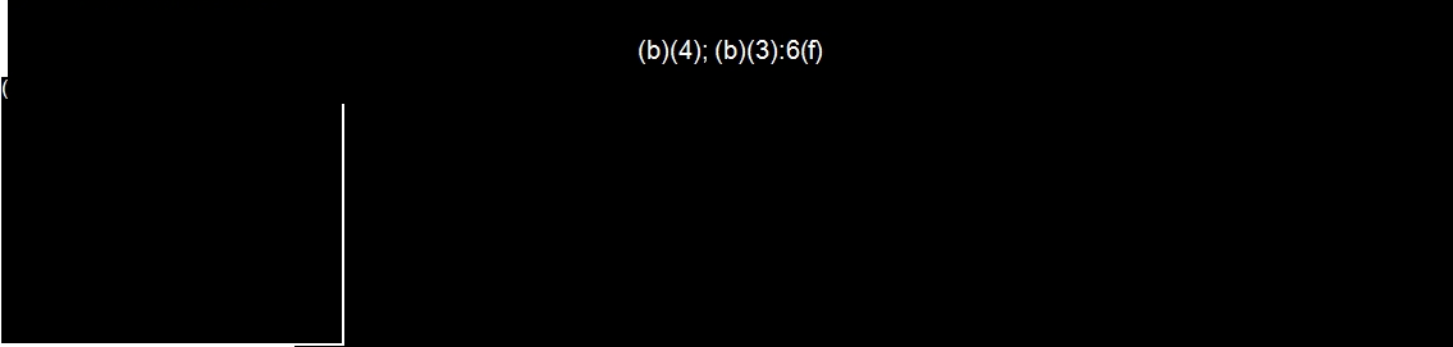
(b)(4); (b)(3):6(f) were as follows:

- 
- 
- 
- 
- 
- 
- 
- 
- 



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

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



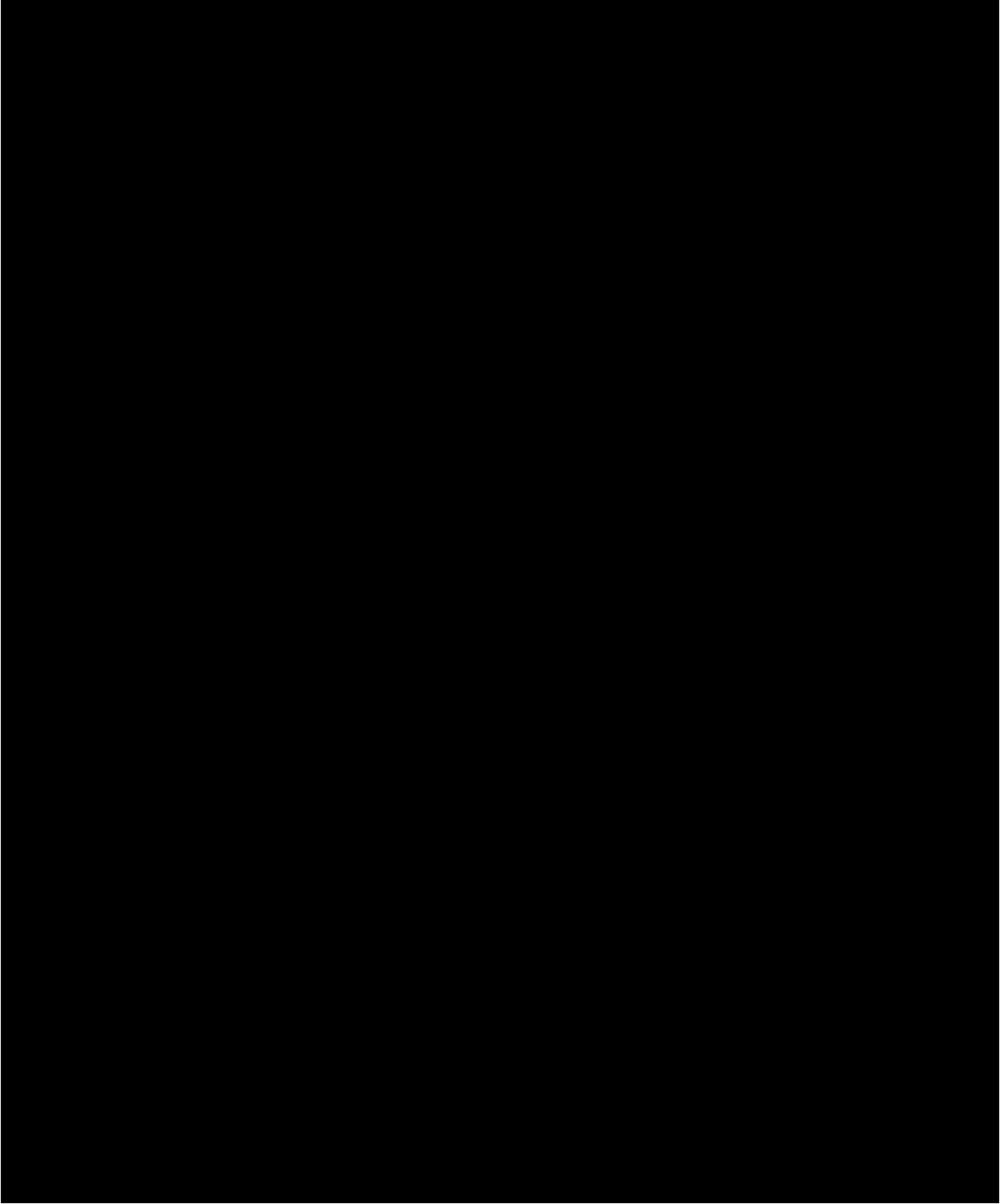
(b)(4); (b)(3):6(f)

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



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

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

The (b)(4); establishes specific Safeguards for protecting the confidentiality, integrity, and availability of Covered Information. Within the (b)(4); are technologies, processes, and procedures for: restricting employee access to Covered Information based on business need, limiting access to toolsets that can access Covered Information, securing passwords (both at rest and in transit), monitoring and responding to employee access violations, detecting privacy related security vulnerabilities in software, and documenting a comprehensive information security program to support the overall privacy objectives.

Prior to the beginning of the assessment, the FTC, the Assessor, and Facebook determined the scope of this (b)(4); and the Assessor’s review was specifically limited to those Safeguards at the application and data level. While Facebook maintains of complimentary processes and procedures throughout the organization to manage security risks as part of their Comprehensive Information Security Program (e.g., physical security, penetration testing, firewalls, disaster recovery, asset management, etc.), our assessment was limited to those Safeguards specifically designed to address security risks at the application and database levels identified as part of the risk assessment in Part VII.D and the following relevant Parts of the Order:

Part VII.E: Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

Part VII.E.3: Specifically, with respect to Respondent’s employees’ access to Covered Information maintained in Respondent’s data warehouse(s), such safeguards shall include designing, implementing, and maintaining access policies and controls that limit employee access to any table(s) or other comparable data storage units known to contain Covered Information to only those employees with a business need to access such Covered Information.

The within the (b)(4); (b)(3):6(f) are addressed through (b)(4) Safeguards which were implemented during the Assessment Period. (b)(4); (b)(3):6(f)

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

(b)(4); (b)(3):6(f) Refer to Appendix A for details on the specific Safeguards within the (b)(4); (b)(3):6(f).

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

*Comprehensive Information Security Program*

Facebook implemented a Comprehensive Information Security Program (CISP) to manage controls that protect the confidentiality, integrity, and availability of data stored on Facebook’s systems, platforms, and products. The CISP is divided into the following (b)(4); (b)(3):6(f), each of which covers a key component of how Facebook protects their information systems:

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



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



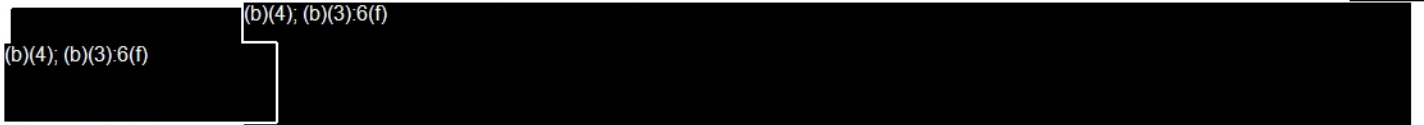
The Assessor reviewed the CISP for the completeness of the [redacted] (b)(4); (b)(3):6(f) but did not test the design or operating effectiveness of controls outside those that were part of the (b)(4); (b)(3):6(f) scope defined in the Order.

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

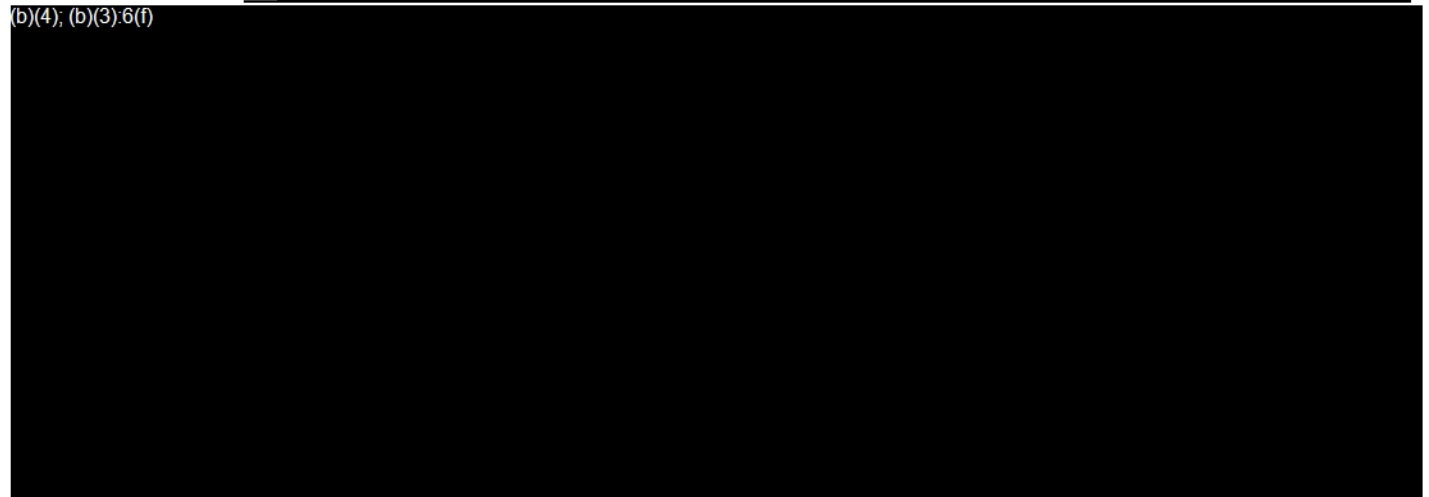
Facebook implemented Safeguards to govern employee access to Covered Information stored within the [redacted]

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

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



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



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



Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

The Assessor considered standards including the National Institute of Standards and Technology (NIST) and the Generally Accepted Privacy Principles (GAPP) to evaluate the completeness of the Comprehensive Information Security Program and the Security for Privacy Safeguards. We evaluated the processes executed by Facebook to protect Covered Information, including the provisioning of access to Covered Information through Access Modeling, Access Control, and verifying business need; password encryption, heuristics, and scanning; and Software Development Lifecycle (SDLC) practices.

Our evaluation of the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) included the review of over (b)(4) documents, reports, and process descriptions. Key documentation reviewed included, but was not limited to, the following:

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

We conducted over (b)(4) interviews with key stakeholders, (b)(4); (b)(3):6(f)

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

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

The Safeguards identified as a part of the (b)(4); (b)(3):6(f) were covered through design and operating effectiveness testing as described in Section II – Assessment Methodology above. In alignment with the Assessment Methodology, we performed over [redacted] sample tests (b)(4); (b)(3):6(f). An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing included reviews of procedural documentation and completion of walkthroughs with Safeguard Owners to understand the design of the Safeguards and associated processes. Where applicable, live demos were performed by Facebook to demonstrate the process of limiting access to Covered Information, password encryption, and SDLC practices to better understand how the Safeguards operate in practice. The key objectives and our test procedures for design effectiveness testing for the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) were as follows:

- Evaluated the processes for requesting, provisioning, and expiration of access to Covered Information at the application and database level;
- Evaluated the processes for storing and encrypting passwords when in transit over the Internet or Facebook transmission channels;
- Evaluated the processes for scanning, detecting, and cryptographically protecting plain text passwords within the (b)(4); (b)(3):6(f)
- Evaluated the processes to document and monitor the resolution of issues related to inappropriate access to Covered Information which surfaced during manual reviews, automated scans, and audits to assess whether appropriate and timely action is taken;
- Evaluated the process for preventing, identifying, analyzing, and mitigating application security vulnerabilities and bugs; and
- Evaluated the process for managing access and protecting Covered Information specific to the Cloud environments of in-scope business units.

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

Our operating effectiveness testing included a detailed review of samples across (b)(4) Safeguards leveraging the sampling methodology described in Section II – Assessment Methodology, code walkthroughs, and live observations of the processes being executed. The key objectives and our test procedures for operating effectiveness testing for the (b)(4); (b)(3):6(f) were as follows:

- Assessed the execution of the practices for requesting, provisioning, and expiration of access to Covered Information at the application and database level. This was performed by testing samples of new, current, and removed access to the (b)(4); (b)(3):6(f) We obtained evidence of documented access requests with details of business needs and approvals as well as the actions performed to provision the access and confirmation that the appropriate access was granted.
- Assessed the execution of the practices for storing and encrypting passwords when in transit over the Internet or Facebook transmission channels. This was performed by participating in detailed walkthroughs of system configurations with Facebook to evaluate the configurations behind the password encryption security measures in place. We obtained snapshots of the relevant code discussed in the walkthroughs, reviewing them to confirm completeness and accuracy.

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

The (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) establishes standards for accurately explaining Facebook data practices to users. Facebook designed this (b)(4); (b)(3):6(f) to provide accurate privacy notices and updates to users regarding their privacy rights and Facebook's policies and practices concerning the collection, processing, and storage of Covered Information.

This (b)(4); (b)(3):6(f) includes processes to help prevent misrepresentations about the privacy and security of Covered Information in connection with products or services; including information obtained for specific purposes such as enabling account security features. This (b)(4); also addresses affirmative express consent to be obtained from users prior to sharing Nonpublic User Information beyond that consented to within individually managed user Privacy Settings or Facial Recognition Templates.

To help manage the objectives described above, this (b)(4); (b)(3):6(f) relies on the (b)(4); process to help ensure users are appropriately notified of updates regarding their privacy rights concerning Covered Information and to obtain special consent when required.

The (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) addresses Consent Order requirements through associated (b)(4); (b)(3):6(f) and Safeguards. As Facebook implements new or modified products, services, or practices, there may be new commitments, notices or choices that are introduced. The Safeguards in this (b)(4); (b)(3):6(f) in combination with the (b)(4); process work to address the requirements in the relevant Order Parts below:

Part VII.E: Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

Part VII.E.2.a: Prior to implementing each new or modified product, service, or practice, (i) conducting a privacy review that assesses the risks to the privacy, confidentiality, and integrity of the Covered Information, the safeguards in place to control such risks, and the sufficiency of the User notice and, if necessary, consent; and (ii) documenting a description of each reviewed product, service, or practice that was ultimately implemented; any safeguards being implemented to control for the identified risks; and the decision or recommendation made as a result of the review (e.g., whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

Part VII.E.2.b.ii: The notice provided to Users about, and the mechanism(s), if any, by which Users will consent to, the collection of their Covered Information and the purposes for which such information will be used, retained, or shared by Respondent.

Part VII.E.5: Specifically with respect to facial recognition, such safeguards shall include:

- a. Prior to using or sharing any Facial Recognition Template for a User in a manner that materially exceeds the types of uses or sharing disclosed to that User at the time that User's consent was previously obtained,
  - (i) Clearly and Conspicuously disclosing (such as in a stand-alone disclosure or notice), separate and apart from any "Privacy Policy," "data policy," "statement of rights and responsibilities" page, or other similar document, how Respondent will use or, to the extent applicable, share, such Facial Recognition Template; and
  - (ii) Obtaining the User's affirmative express consent;

b. Nothing in this provision shall limit Respondent’s ability to use Facial Recognition Templates for fraud prevention or remediation, or protecting the safety, reliability and security of Respondent’s platform or Users, so long as Respondent discloses these types of uses in Respondent’s Privacy Policy or similar document.

The [redacted] (b)(4); (b)(3):6(f) includes (b)(4); (b)(3):6(f) Safeguards. [redacted] (b)(4); (b)(3):6(f)

[redacted] Refer to Appendix A for details on the specific Safeguards within the [redacted] (b)(4); (b)(3):6(f)

2. [redacted] (b)(4); (b)(3):6(f) [redacted] (b)(4); (b)(3):6(f) is composed of five general process areas summarized below, and described in more detail throughout the remainder of the section:

- [redacted] (b)(4); (b)(3):6(f)
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted] Facebook maintains processes intended to provide users with clear, conspicuous, and accurate notice of their privacy rights and Facebook’s policies and practices regarding the processing of Covered Information, including how that information will be collected, used, shared, retained and deleted. Facebook has processes in place to identify and determine when Terms of Service and Data Privacy Policy updates are needed. There are reasons to ensure that terms or policies are appropriately maintained from a privacy perspective including:

- To prevent or correct an actual or potential inaccuracy or misrepresentation regarding Facebook’s processing of user data identified in the course of [redacted] or periodic review by Facebook Legal;
- To provide necessary transparency in the event of a change in applicable legal requirements or based on the results of [redacted] or periodic review by Facebook Legal; and
- To reflect changes in applicable legal requirements.

[redacted] (b)(4); (b)(3):6(f)

[redacted] (b)(4); (b)(3):6(f) Facebook has implemented processes to ensure that prior to the creation, use, or sharing of Facial Recognition Templates, users are eligible and have provided consent for facial recognition features. Eligibility of users is based on a set of criteria that includes age (i.e., must be 18 or above), type of account (e.g., Facebook, Workplace, Memorialized, etc.), location (e.g., EU/Canada, Brazil, rest of the world), and consent status (i.e., previously obtained or not).

If consent has not been obtained and all other criteria for eligibility has been met, users are presented with a consent flow where they have the option to consent to, and enable, facial recognition. Once consent has been provided, the

[redacted]

user still maintains the ability to control their Face Recognition setting and turn it On or Off at their discretion. Eligibility of users is checked every time an image is uploaded to Facebook where a face is detected. Users that do not meet the eligibility criteria or who have their Face Recognition setting set to No (Off), do not have a face template and cannot be recognized in images. At any time, users can opt out of facial recognition at which point their template is deleted.

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

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

Under requirements of the Order, telephone numbers collected from users prior to the effective date of the Order for the exclusive purpose of enabling account security features cannot be shared or used for the purpose of serving advertisements. To address these and other requirements, Facebook created a category of numbers that it refers to as Security Phone Numbers (SPNs). (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)

Facebook makes external statements to users regarding the privacy and security of their Covered Information. These privacy commitments could be made in sources such as policies, notices, blogs, or other official company communication. Historical Commitments are commitments that are currently active but made prior to the implementation of the (b)(4); (b)(3):6(f) process and the Assessment Period. (b)(4); (b)(3):6(f)

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

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

This (b)(4); (b)(3):6(f) relies on the (b)(4); (b)(3):6(f) process. For any collection, use, or sharing of Covered Information in any new or modified product, service, or practice across the Facebook family of products; (b)(4); is designed to consider multiple aspects related to user data, including the following:

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



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

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

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

The Assessor evaluated processes executed by Facebook relevant to the (b)(4); (b)(3):6(f) as described above. We reviewed over (b)(4) documents, conducted walkthroughs with Safeguard Owners, and observed process and tool demonstrations. Key documentation reviewed and processes observed included but were not limited to the following:

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

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

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

For more details regarding (b)(4); please see

Section III.G – (b)(4); (b)(3):6(f)

We conducted over (b)(4); (b)(3):6(f) interviews with key personnel and Safeguard Owners (b)(4); (b)(3):6(f)

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

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

The Safeguards identified as part of the

(b)(4); (b)(3):6(f) were covered through design and operating effectiveness testing as described in Section II – Assessment Methodology above. Our testing included evaluation of (b)(4); Safeguards aligned to the (b)(4); (b)(3):6(f)

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

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

. In alignment with the Assessment Methodology, we performed over (b)(4); sample

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

An overview of our design and

operating effectiveness testing is included below.

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

The key objectives and test procedures for our design effectiveness testing for the (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) were as follows:

- Evaluated whether the processes described appropriately mitigated the risks that user facing privacy notices, representations, and disclosures are inadequate or inaccurate;

- Verified that the (b)(4); (b)(3):6(f) performed appropriately mitigated the risk that user privacy disclosures are not sufficiently prominent, accessible, or visible;
- Evaluated if processes designed to prevent misrepresentations appropriately mitigated the risk that external representations are inaccurate;
- Verified that the design of the facial recognition Safeguards adequately mitigated the risk that affirmative express consent was not obtained prior to the creation, use, or sharing of Facial Recognition Templates;
- Confirmed that the design of the facial recognition Safeguards adequately mitigated the risk that users not eligible for facial recognition do not have Facial Recognition Templates available for use or sharing;
- Evaluated whether the Access Control processes over SPNs adequately mitigated the risk of unauthorized access;
- Determined if the monitoring processes appeared to be designed with the proper scope and capability to detect the unauthorized use or relocation of SPNs;
- Evaluated that the filtering mechanism used to prevent ad targeting for SPNs was designed effectively; and
- Evaluated whether the process for remediating issues related to SPNs adequately mitigated the risk of improper use of SPNs.

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

The key objectives and test procedures for our operating effectiveness testing for the

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

(b)(4); (b)(3):6(f) were as follows:

- [Redacted]
- [Redacted]
- [Redacted]

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

Our methods for validation were as follows:

- Inspected a sample of updates to policies to ensure:
  - Process steps were adequately followed;
  - Required legal approvals were obtained including Privacy Decisions;
  - Updated policies were properly published via the Content Management System or other appropriate methods; and
  - Policies were translated to other languages, where required.
- Inspected video evidence of execution of test steps to validate that a sample of data policies were presented to end users as expected;
- Reviewed sample task tool evidence to ensure remediation activities were in process for data/Terms of Service policies where results were not as expected;
- Independently reperformed Quality Assurance test steps to ensure data and Terms of Service policies for a selected sample were presented to users as expected;
- Identified and observed 17 live test scenarios (test scenarios executed by Facebook and observed by the Assessor in real time) to validate that the user consent flow was appropriately presented to users who have not previously consented and meet eligibility requirements;

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

(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);

The Order states that telephone numbers “identified through its source tagging system as being obtained from a User prior to the effective date of this Order for the specific purpose of enabling an account security feature designed to protect against unauthorized account access (i.e., two-factor authentication, password recovery, and login alerts)” cannot be shared or used for the purpose of serving advertisements. Facebook refers to these numbers as Security Phone Numbers (SPNs).

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

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

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

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

As of October 25, 2020, Oculus no longer allows new Oculus-only accounts. All new accounts are part of a Facebook account and fall under Facebook policies and processes.

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

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

The Order sub-requirements related to the (b)(4); include:

Part VII.A: Document in writing the content, implementation, and maintenance of the Privacy Program that includes: (1) the documented risk assessment required under Part VII.D. of this Order; (2) the documented safeguards required under Part VII.E. of this Order

Part VII.E: Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

Part VII.E.1: Specifically, with respect to any Covered Third Party that obtains or otherwise has access to Covered Information from Respondent for use in an independent, third-party consumer application or website, such safeguards shall include:

Part VII.E.1.a: Requiring an annual self-certification by each Covered Third Party that certifies: (i) its compliance with each of Respondent’s Platform Terms; and (ii) the purpose(s) or use(s) for each type of Covered Information to which it requests or continues to have access, and that each specified purpose or use complies with Respondent’s Platform Terms;

Part VII.E.1.b: Denying or terminating access to any type of Covered Information that the Covered Third Party fails to certify pursuant to Part VII.E.1.a.(ii) above, or, if the Covered Third Party fails to complete the annual self-certification, denying or terminating access to all Covered Information unless the Covered Third Party cures such failure within a reasonable time, not to exceed thirty (30) days;

Part VII.E.1.c: Monitoring Covered Third Party compliance with Respondent’s Platform Terms through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months; and

Part VII.E.1.d: Enforcing against any Covered Third Party violations of Respondent’s Platform Terms based solely on the severity, nature, and impact of the violation; the Covered Third Party’s malicious conduct or history of violations; and applicable law.

Part VII.H: Select and retain service providers capable of safeguarding Covered Information they receive from Respondent, and contractually require service providers to implement and maintain safeguards for Covered Information.

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

The (b)(4); (b)(3):6(f) includes (b)(4); (b)(3):6(f) Safeguards. (b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f) Refer to Appendix A for details on the specific Safeguards within the (b)(4); Facebook employs

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



Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

The Product-based Engagement lifecycle applies to third party engagements where access to Covered Information is governed and managed by the platform-based API governance and API platform products. These third parties are mostly app developers that benefit from being on the Facebook platform and from using Facebook application integrations such as Facebook Login. (b)(4); (b)(3):6(f)

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

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

Facebook requires all third party apps that access non-Public Covered Information to obtain user consent before accessing it. With respect to Facebook Login integrations, this consent is obtained when the user first signs in through the app. At the initial login, Facebook Login requires a user to grant consent to share the non-Public Covered Information that a third party app requests. The app may only access those categories of non-Public Covered Information to which the user consents and a user may decline consent for the requested types of non-Public Covered Information as shown in figure III.L.2.iv-vi. (b)(4); (b)(3):6(f)

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

After initial consent is received by an app, users can edit their consent in their Facebook profile at any time through their profile settings under their "Apps & Websites Settings" or "Business Integrations Settings" pages. Additionally, a user can subsequently revoke their consent.

Figure III.L.2.iv: User Consent

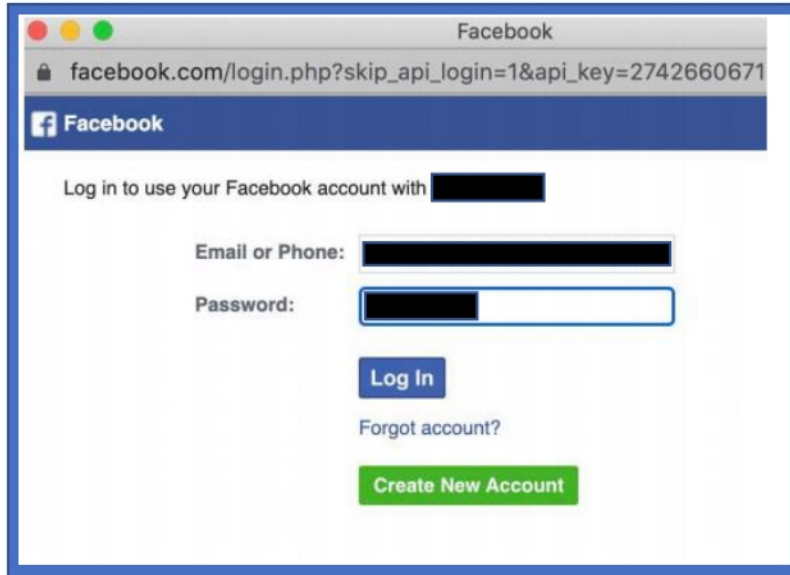


Figure III.L.2.v

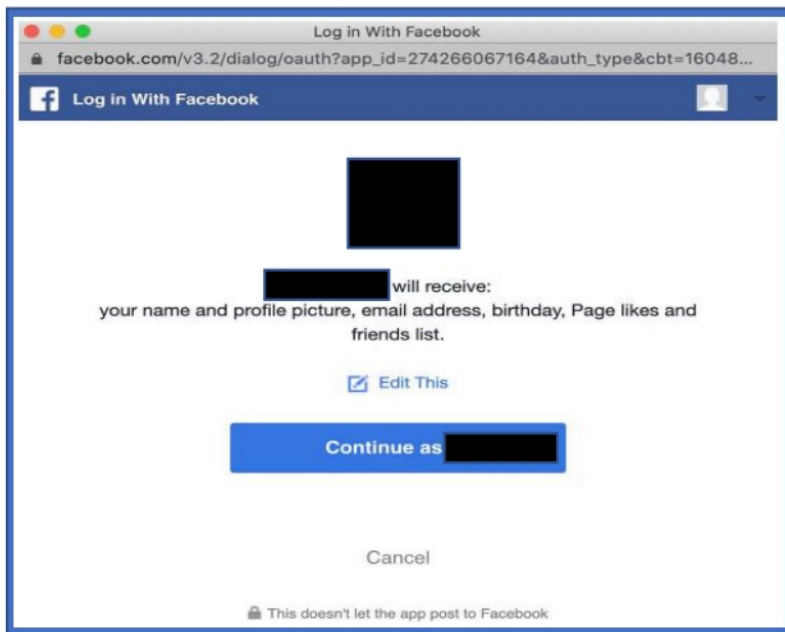
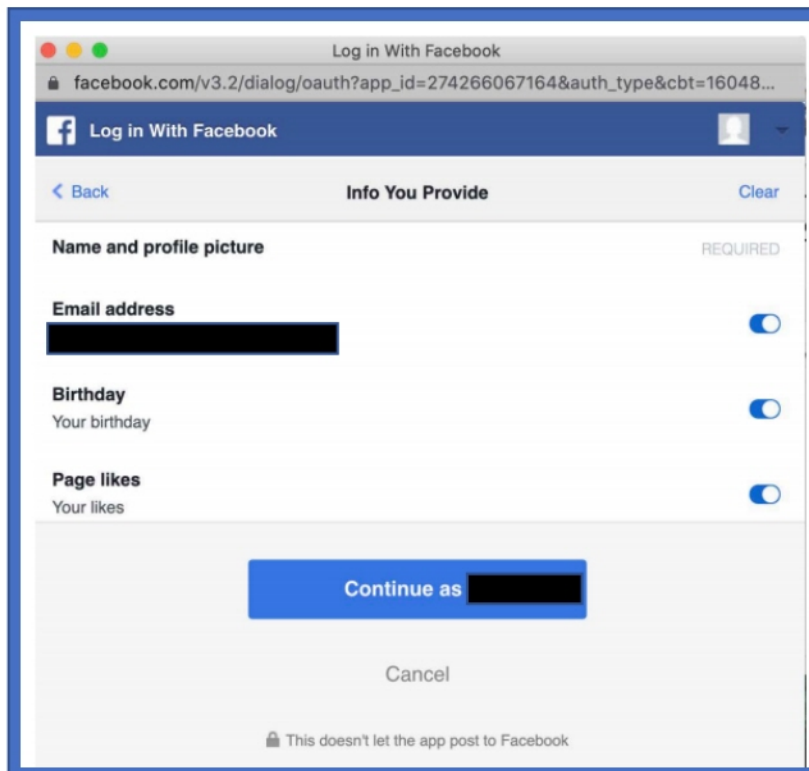


Figure III.L.2.vi



If the third party app does not use a permission for 90 days, that permission is automatically expired. Once the permissions have expired, the third party app will no longer have access to Covered Information and will have to re-request access to Covered Information.

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

Facebook maintains a process to ensure proper deprecation of API products. Deprecation of API products could have an impact on third party apps which use API products; therefore the process is designed to provide sufficient lead time for third party communications.

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

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

Once an app has passed the compliance requirements including App Review or Partner Grant Review where applicable, the app has access to the requested permissions, capabilities and/or features. In order to maintain access to permissions, capabilities, and/or features associated with E1 API products Facebook requires developers to annually (i) certify continued compliance with applicable Facebook terms, and (ii) certify that each one of their purpose(s) or use(s) for Covered Information complies with Facebook's permissible purpose(s) or uses(s) for that type of Covered Information.

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

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

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

Facebook maintains a process for developers to appeal enforcement actions against them by submitting a request through the external developer portal. (b)(4); (b)(3):6(f)

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

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

Facebook maintains an external developer portal for developers to unregister their accounts. (b)(4); (b)(3):6(f)

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

Once a platform app's state is changed to deleted, the developer can no longer



access the application dashboard or receive users' Covered Information. (b)(4); (b)(3):6(f)

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

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

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

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

The Assessor evaluated the coverage, consistency, and efficacy of Facebook's (b)(4); (b)(3):6(f) processes. The scope of the Assessor's evaluation included the full third party lifecycle from intake to offboarding within the (b)(4); (b)(3):6(f) process, the execution of third party reviews to identify risks and associated mitigations, and the enforcement of third parties' adherence to Facebook's security and privacy terms.

The Safeguards identified as part of the (b)(4); (b)(3):6(f) were evaluated through design and operating effectiveness testing as described in the Section II – Assessment Methodology above. Our testing included evaluation of (b)(4) Safeguards aligned to the (b)(4); (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f)

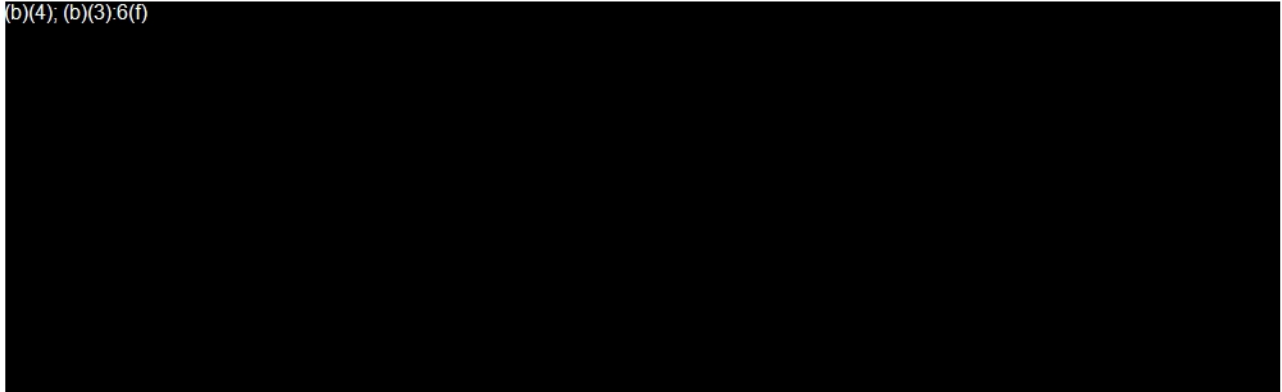
Our evaluation of the (b)(4); (b)(3):6(f) included the review of over (b)(4) documents, reports, and evidence of the (b)(4); (b)(3):6(f) process outputs. Key documentation we reviewed included but was not limited to the following:

- Playbook and Runbooks:

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

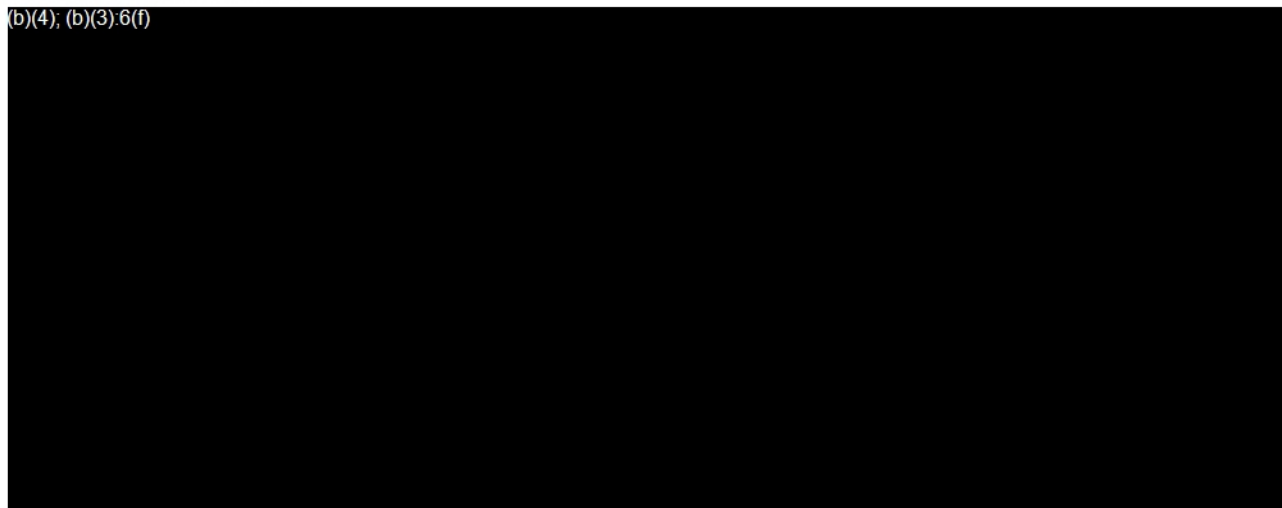
- Policies:

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



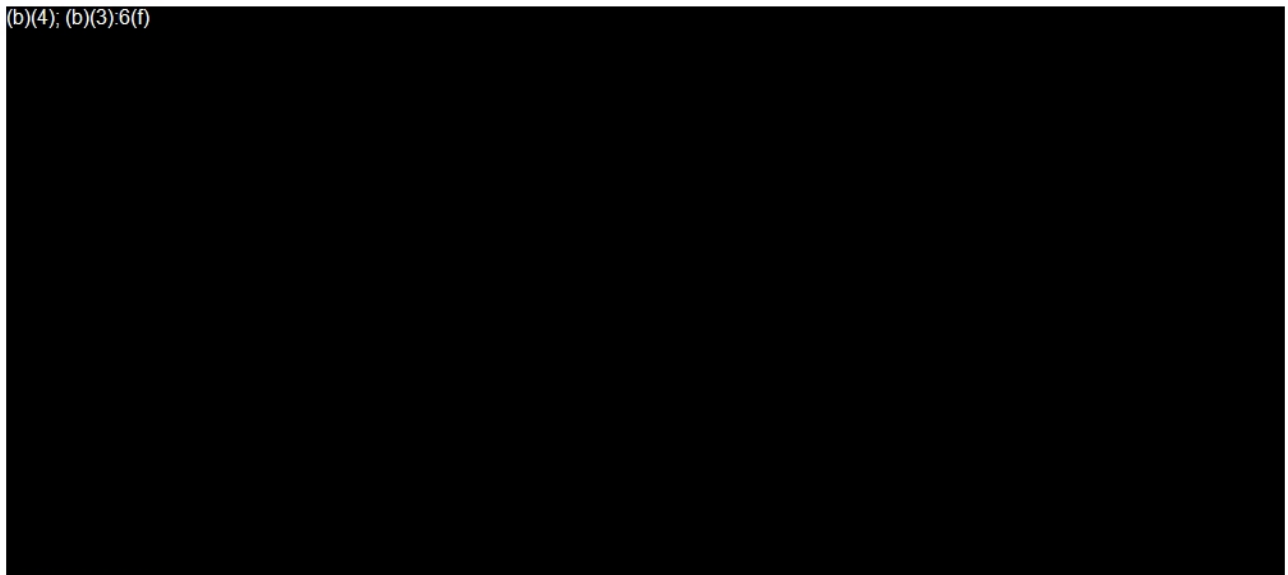
- Procedural Documentation:

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

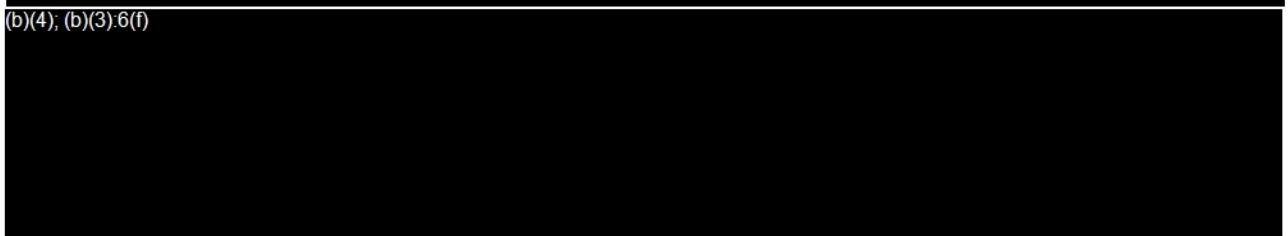


- Evidence:

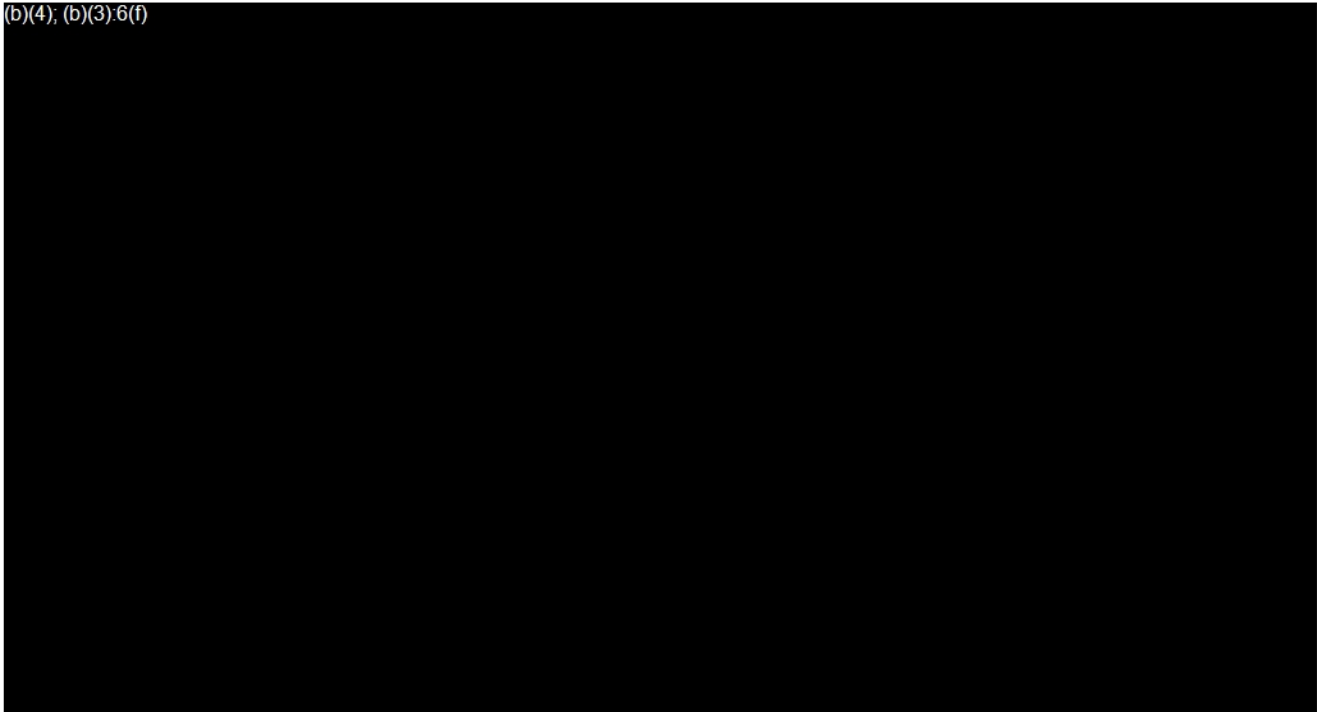
(b)(4); (b)(3):6(f)



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

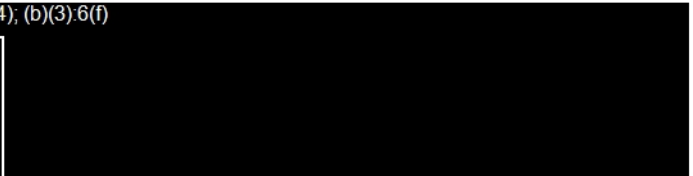
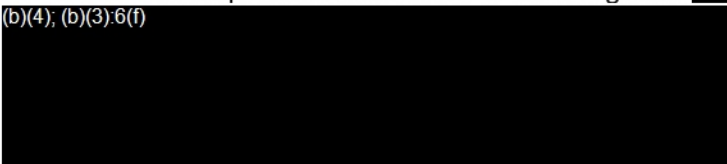


(b)(4); (b)(3):6(f)



We also conducted over [redacted] interviews with key stakeholders to gain an understanding of each of the (b)(4); (b)(3):6(f) Safeguards including responsibilities by functional area and underlying processes and the involvement of any systems or tools utilized as part of the execution of the Safeguard. (b)(4); (b)(3):6(f)

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



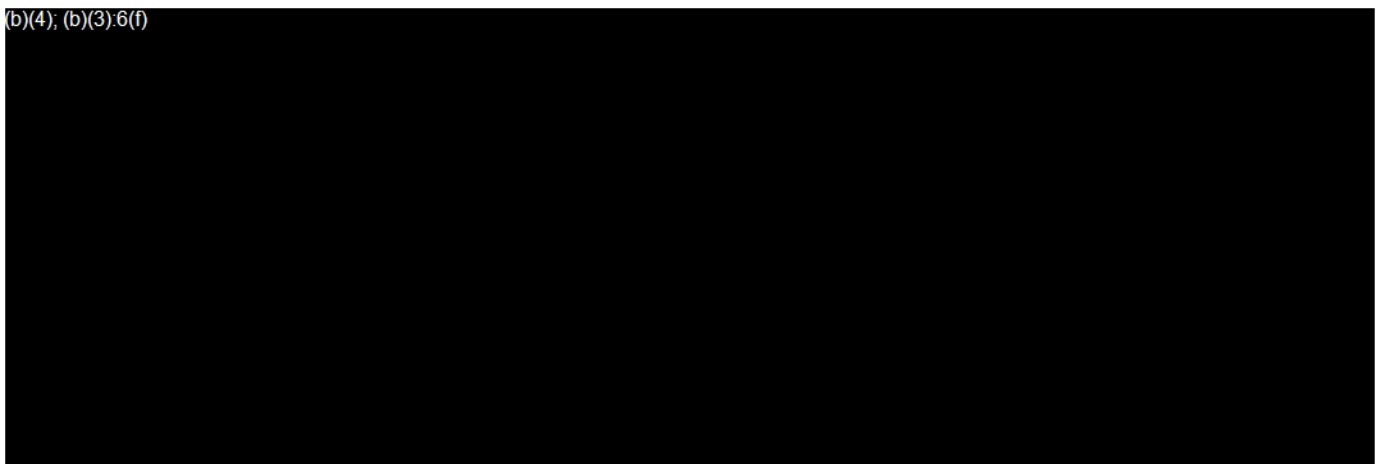
In alignment with the Assessment Methodology, we performed over [redacted] sample tests (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) An overview of our design and operating effectiveness testing is included below.

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

Our design effectiveness testing approach included obtaining and reviewing procedural documentation and conducting walkthroughs with Safeguard Owners to understand how Safeguards are designed to operate. The key objectives and our test procedures for design effectiveness testing for the (b)(4); (b)(3):6(f)

(b)(4); were as follows:

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



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

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

Our operating effectiveness testing included selecting and testing (b)(4) Safeguards, leveraging the sample methodology described in Section II – Assessment Methodology. The key objectives and our test procedures for operating effectiveness testing for the (b)(4); (b)(3):6(f) (b)(4); (b)(3):6(f) were as follows:

- For Contract-based engagement Safeguards, we verified the signed contracts for third parties include appropriate privacy and security terms. Our detailed testing included:

- 
- 
- 
- 
- 

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

- For Product-based engagement Safeguards (occurrence-driven), we determined whether appropriate governance was in place to control access to APIs by E1 Covered Third Parties. Our detailed testing included the following:

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

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

- For Product-based engagement Safeguards (automated-based), we verified whether proper mechanisms were in place to prevent or respond to privacy or security-related violations of third party contractual agreements. Our testing effort included the following:

- 
- 
- 
- 
- 
- 
- 

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

- Our operating effectiveness testing was structured to determine whether the third party apps can only operate within the bounds described by technical documentation, engineering teams, and the Platform Terms. This included:

- 
- 
- 
- 
- 
- 
- 

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

- To assess whether the monitoring and auditing of third party compliance to the Platform Terms was sufficient based on requirements of the Order, our analysis and testing included the following:

- 
- 
- 
- 
- 
- 
- 

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

[Redacted]

4. (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);

Under the Order (Part VII.E.1.c, Monitoring of Third Party Compliance), Facebook must implement Safeguards for “monitoring Covered Third Party compliance with Respondent’s Platform Terms through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months”.

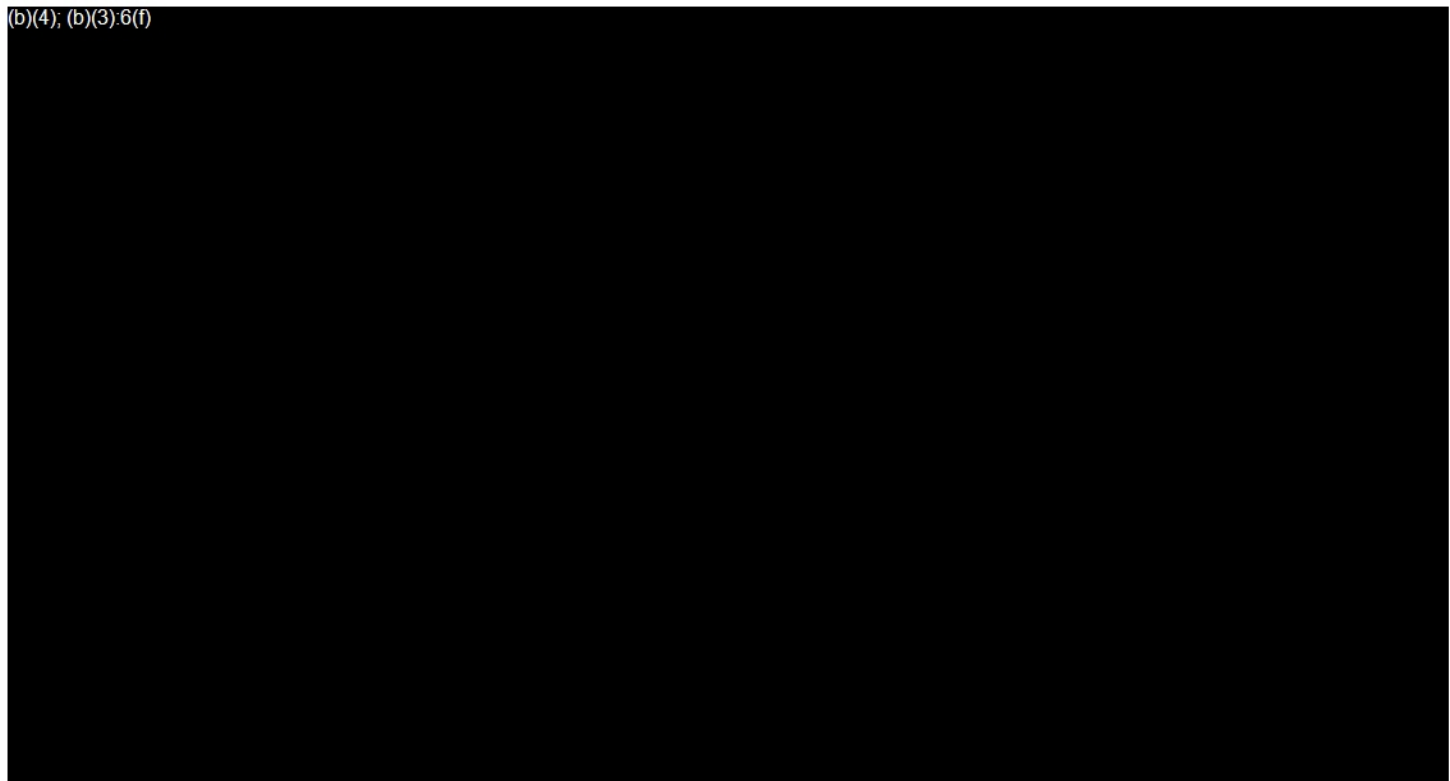
(b)(4); (b)(3):6(f)

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


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

Each E1 Covered Third Party must agree to the Platform Terms and Developer Policies<sup>54</sup> prior to gaining access to the development platform and agree to maintain compliance until the E1 Covered Third Party removes its app(s) from the Facebook platform.

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



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



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

---

<sup>54</sup> <https://developers.facebook.com/terms/>; <https://developers.facebook.com/devpolicy>; <https://www.oculus.com/legal/privacy-policy/>

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



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

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

Oculus is a virtual reality hardware, software, and developer ecosystem brand acquired by Facebook in 2014. The business unit produces consumer focused Virtual Reality (VR) headsets, including the Oculus Quest 1 & 2, Oculus Rift, and Oculus Go headsets. The VR headsets have access to the Oculus App Store, where users can download over 1,600 free or for-purchase applications that include games, simulators, and other virtual reality experiences.

The majority of the applications available for use on Oculus are developed and maintained by 3rd party developers. To support development efforts, Oculus maintains an ecosystem platform solution where third party developers can build, test, and distribute VR applications. Oculus also maintains multiple Software Development Kits (SDKs) and APIs for use by third party developers.

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

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

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

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act