Independent Assessor's Report on Facebook's Privacy Program

Biennial Report

For the period February 12, 2015 to February 11, 2017

pwc

Table of Contents

pwc

Introduction

Facebook, Inc. and the Federal Trade Commission (FTC) entered into Agreement Containing Consent Order File No: 0923184 ("the Order"), which was served on August 15, 2012.

Part IV of the Order requires Facebook to establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information.

Part V of the Order requires Facebook to obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Facebook engaged PricewaterhouseCoopers LLP ("PwC") to perform the independent assessment.

As described on pages 6-14, Facebook established its privacy program by implementing privacy controls to meet or exceed the protections required by Part IV of the Order. As described on pages 15-18, PwC performed inquiry, observation, and inspection/examination procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order during the two years ended February 11, 2017, and our conclusions are on pages 4-5.

pwc

Report of Independent Accountants

To the Management of Facebook, Inc.:

We have examined Management's Assertion, that for the two years ended February 11, 2017 (the "Reporting Period"), in accordance with Parts IV and V of the Agreement Containing Consent Order (the "Order") with an effective date of service of August 15, 2012, between Facebook, Inc. ("Facebook" or "the Company") and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program ("the Facebook Privacy Program"), as described in Management's Assertion, based on Company-specific criteria, and the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period.

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

The Company's management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly, included examining, on a test basis, evidence supporting the effectiveness of the Facebook Privacy Program as described above and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

We are not responsible for Facebook's interpretation of, or compliance with, information security or privacy-related laws, statutes, and regulations applicable to Facebook in the jurisdictions within which Facebook operates. We are also not responsible for Facebook's interpretation of, or compliance with, information security or privacy-related self-regulatory frameworks. Therefore, our examination did not extend to the evaluation of Facebook's interpretation of or compliance with information security or privacy-related laws, statutes, regulations, and privacy-related self-regulatory frameworks with which Facebook has committed to comply.

In our opinion, Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects for the two years ended February 11, 2017, based upon the Facebook Privacy Program set forth in Management's Assertion.

pwc

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

This report is intended solely for the information and use of the management of Facebook and the United States Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.

PricewaterhouseCoopers LLP

San Jose
April 12, 2017

facebook

Facebook's Privacy Program Overview

Introduction

Facebook, Inc. (herein referred to as "Facebook" or "the Company") is a publicly traded U.S. company headquartered in Menlo Park, California. Established in February 2004, the Company aims to make the world more open and connected. People use Facebook to stay connected with their friends, family, and interests, to express what matters to them to the people they care about, and to build communities to share ideas. Developers use our Platform to build applications ("apps") and websites that integrate with Facebook to reach our global network of users and to build products and services that are more personalized, social, and engaging. In doing so, people entrust us with information when they use our services.

Facebook integrates privacy considerations into the creation of our product and business plans, and we constantly evaluate our services and privacy program ("Privacy Program") to account for evolving risks and to help ensure that the people who use our services understand the experience. For instance, Facebook's ad preferences allows users to, among other things, provide feedback on the ads they see and to control whether their own image appears in connection with social ads. We have a dedicated team of product managers and engineers who support ad preferences, and we continuously develop new ways to enhance our ads transparency and control features. In addition, within the past two years, we have: updated our Privacy Basics and About Facebook Ads webpages with user-friendly modules that clearly explain how we target ads and direct the user to controls where they can decide how their information is used in relation to ads. We also have updated our cookies policy to, among other things, explain our use of cookies in a way that is easy to understand, and we rolled out new tools that allow users to control how data collected about their interests on Facebook is used for ads outside the Facebook platform.

Facebook also recognizes how helpful and important supplemental privacy-related information has been to people who use other parts of the Facebook Services. As such, we recently revised the Privacy Basics feature to update and expand information about how users can use available tools and control their privacy preferences. We updated Privacy Basics based on user feedback, with the goal of making it easy for users to find information about protecting their privacy. The current version of Privacy Basics offers improved functionality, features a "Top Topics" section which answers frequently asked questions about privacy and security, and includes 32 interactive guides that are available in 44 languages.

Since Facebook submitted its 2015 Privacy Program Overview, we also have continued to build out teams that focus on specific areas of our Privacy Program. These include our Security Policy, Risk, and Compliance and Data Access teams, HR teams that manage the onboarding of employees, and IT teams that manage how we track assets. This in turn allows us to continually evaluate the effectiveness of our controls, alongside the reviews and tests conducted by our independent assessor PricewaterhouseCoopers LLP ("PwC"). This Privacy Program Overview describes the scope and background of Facebook's Privacy Program and the procedures developed to ensure we achieve our privacy objectives. The accompanying report submitted by PwC provides additional details on these controls and the results of the rigorous tests performed in connection with this assessment.

facebook

Background and Scope of the Privacy Program

Facebook designed the Privacy Program to accomplish two primary objectives: (a) to address privacy risks related to the development, management, and use of new and existing products, and (b) to protect the information Facebook receives from or about users. Facebook's Privacy Program is defined by eight assertions inspired by the Generally Accepted Privacy Principles ("GAPP") framework, set forth by the American Institute of Certified Public Accountants ("AICPA"). In particular, Facebook's assertions include the following:

A. **Responsibility for the Facebook Privacy Program:** Facebook has designated an employee or employees to coordinate and be responsible for the privacy program.

B. **Privacy Risk Assessment:** Facebook has identified reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. This privacy risk assessment includes consideration of risks in areas of relevant operations, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

C. **Privacy and Security Awareness:** Facebook has a privacy and security awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels and training.

D. **Transparency, Consent, Access, Use, and Deletion:** Facebook provides notices and other informational materials about its privacy policies and procedures, and about its terms of service. These materials explain the purposes for which covered information is collected, used, and deleted and describe the choices available to users. Facebook obtains consent for such practices. Facebook has implemented controls, including a Privacy Cross-Functional ("XFN") process, to ensure that it only collects and uses covered information for the purposes identified in the notices and provides users with access to their covered information for review and update. Facebook retains covered information for as long as necessary to provide services or fulfil the stated purposes, or as required by law or regulations, and thereafter appropriately disposes of such information.

E. **Security for Privacy:** Facebook protects covered information of users against unauthorized access.

F. **Third-Party Developers:** Facebook discloses covered information to third-party developers only for the purposes identified in the notices and with the implicit or explicit consent of the individual.

G. **Service Providers:** Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

H. **Ongoing Monitoring of the Privacy Program:** Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program.

As discussed further below, Facebook has implemented numerous procedures ("controls") to achieve and effectuate these objectives. This includes assessing impact on the Privacy Program from acquisitions and new or updated products and services. For example, the Privacy Governance Team, as well as other privacy experts from across the company, convene to discuss privacy risks associated with newly acquired companies. Likewise, new Facebook products or features incorporating newly acquired technology are routinely reviewed by the Privacy XFN team.

Privacy Program Operations and Control Activities

Facebook has identified (b controls to support the above-listed assertions. This section provides a summary of some of the processes Facebook implements to ensure that we achieve each of our privacy objectives.

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

A. Responsibility for the Facebook Privacy Program

Facebook has designated a team of employees who are directly responsible for the Facebook Privacy Program (the "Privacy Governance Team"). The Privacy Governance Team is responsible for reviewing company-wide privacy decisions, including product decisions and establishing, communicating and monitoring relevant control policies and procedures. These policies and procedures are reviewed periodically and updated as needed.

The team members include:

- Vice President and Chief Privacy Officer
- Vice President and Deputy General Counsel
- Vice President, Global Public Policy
- Vice President, International and Policy Communications
- Chief Marketing Officer

- Chief Security Officer
- Head of the Privacy Program, who coordinates the initiatives of the Privacy Program Management team.

The Privacy Governance Team and many employees (including engineers, product managers, security experts [discussed further *infra* at Part E], product and privacy lawyers, and representatives from the public policy privacy team) are responsible for various aspects of the Privacy Program and play a crucial role driving and implementing decisions of the Privacy Governance Team.

Of particular note are the Privacy Program Managers, who play a critical role in the functioning of the Privacy Program. The Privacy Program Managers work closely with the product organization and are responsible for: (1) engaging closely with Legal, Policy, and other members of the Privacy XFN Team to drive privacy decisions; (2) coordinating privacy reviews and presenting privacy issues to the Privacy XFN Team; (3) coordinating any necessary escalations to the Privacy Governance Team, and (4) maintaining records of privacy decisions and completed implementation reviews. The Privacy Legal, Policy, and Privacy Program Management teams work closely with relevant stakeholders throughout Facebook to regularly (a) assess compliance with established privacy controls; (b) improve design and operation of privacy controls; and (c) evaluate and document privacy risks, as discussed further below.

B. Privacy Risk Assessment

A central aspect of Facebook's Privacy Program is a continuous assessment of privacy risks. In our privacy risk assessment, Facebook identifies reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information, and assesses the sufficiency of any safeguards in place to control these risks. As part of this process, members of the Privacy Governance Team consider risks in relevant areas of Facebook's operations. These areas include governance, product design, engineering (including product development and research), community operations (including third-party developers), advertising, service providers, employee awareness and training, employee management, and security. Through this process, Facebook has documented reasonably foreseeable material risks to user privacy, and has put in place reasonable privacy processes and controls to address those risks.

Facebook has implemented numerous avenues through which relevant stakeholders can identify, assess, and remediate risk. For example, members of the Privacy XFN Team assess risks and controls on an ongoing basis through focused subject-matter-specific discussions and weekly intra- and inter-team meetings, such as weekly privacy meetings and bi-weekly product and regulatory updates. Likewise, Facebook's privacy team works to identify, discuss, and assess compliance with privacy policies and procedures as well as applicable laws and regulations. This cross-functional and collaborative effort that allows Facebook to continually evaluate and adjust the Privacy Program in light of the results of testing and monitoring of the program, as well as other relevant circumstances.

facebook

C. Privacy and Security Awareness

Facebook communicates Privacy and Security awareness matters to new and existing employees, agency workers, and vendors, and tailors such communications according to the audience's applicable role and responsibility. For example, upon hiring all new employees must complete a privacy and security awareness training, while all existing employees are required to complete the privacy training biennially. (b)(3):6(f),(b)(4)

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

Above and beyond the controls tested as part of the privacy assessment, Facebook provides additional training material to key stakeholders who have access to covered information. Key stakeholders include: new project managers, product managers and engineers.

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

D. Transparency, Consent, Access, Use, and Deletion

Facebook provides notice of its privacy policy and practices and implements robust procedures to ensure that the privacy polices comply with the choice, collection, and access principles described therein. More specifically, Facebook's Data Policy – which all users must agree to upon signing up to receive our services and which is always available and readily locatable to users across platforms – describes the types of data collected, the purposes for which it is used, and the parties with whom it is shared, among other things. Facebook amended the Data Policy to make it easier for people to read and understand, and implemented Privacy Basics and new content in the Facebook Help Center to provide additional privacy tools and education.

Facebook also offers multiple tools that help users access, delete, and edit information as described in the Data Policy. For example, Facebook allows users to select an audience for their content through various tools, such as account settings and in-line privacy controls. Likewise, Facebook's Activity Log allows users to review, update, delete or correct information they have previously provided, while the Download Your Information tool allows users to create a downloadable archive of their activity.

Facebook implements a variety of procedures to honor the promises defined in the Data Policy. (b)(3):6(f),(b)(4)

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

The controls and protections discussed in Sections E, F, and G below, outline a range of controls and protections used to ensure that data is accessed, stored, and shared in accordance with Facebook's Data Policy.

E. Security for Privacy

The Facebook Security team is led by the Chief Security Officer ("CSO") and the team is responsible for developing and maintaining security policies, enforcing security operations, and monitoring technical security aspects within the Company. The CSO is supported by Security leadership with dedicated teams focusing on (b)(3):6(f),(b)(4)

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

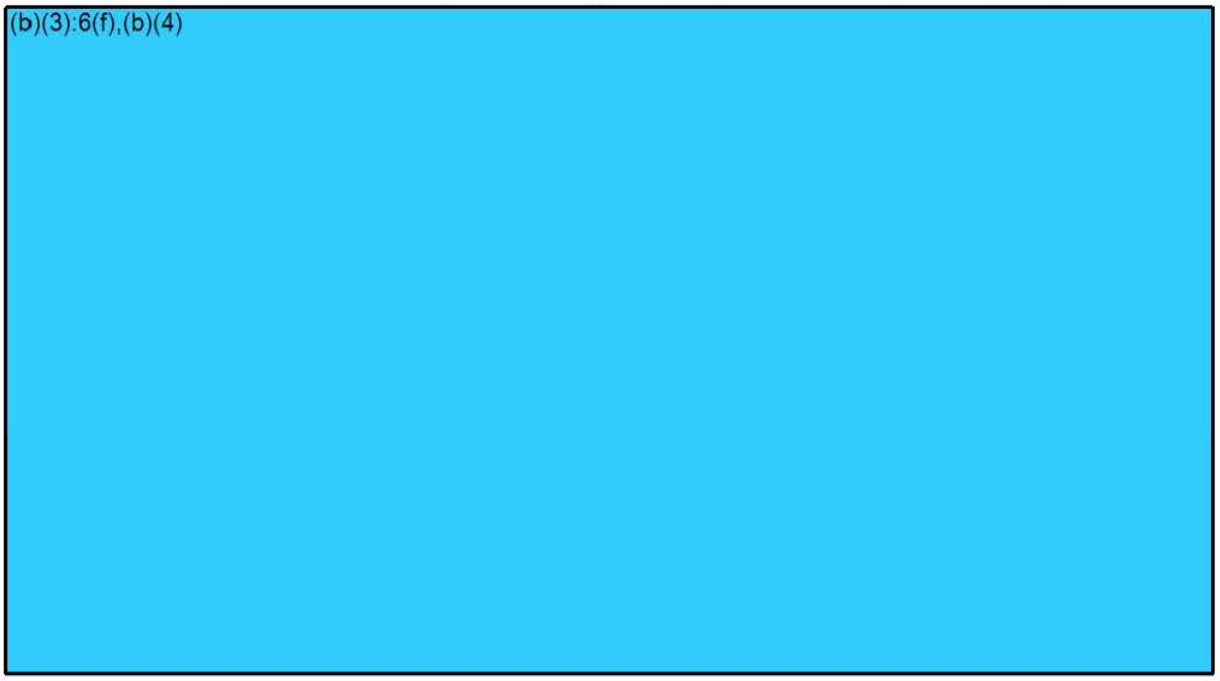
Given that Facebook protects the data of over 1.7 billion people, security is critical to our operations and success. As with the controls described above, Facebook's security program has developed significantly since the inception of the Privacy Program (b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4) For example, Facebook has completed several assessments – all conducted by independent professionals – under the SOC3 and the Payment Card Industry ("PCI") standards. These assessments, which cover a wide range of Facebook's services above and beyond those tested as part of the PwC's independent assessment, verify that the technical, physical, and administrative security controls designed to protect covered information from unauthorized access, as well as those designed to prevent, detect, and respond to security threats and vulnerabilities, are functioning properly.

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

To ensure that these technical safeguards are managed appropriately, various policies are in place that have been approved by management and communicated to employees. (b)(3):6(f),

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



F. Third-Party Developers

Platform applications and developers are required to comply with, and are subject to, Facebook's Statement of Rights and Responsibilities, Platform Principles, and Platform Policies. These terms and policies outline a variety of privacy obligations and restrictions, such as limits on a third-party application's use of data received through Facebook, requirements that an application obtain consent for certain data uses, and restrictions on sharing covered information. Facebook's Platform privacy settings and Granular Data Permissions ("GDP") process allow users to control the transfer of covered information from Facebook to third-party applications.

G. Service Providers

Facebook has implemented controls with respect to third-party service providers, including implementing policies to select and retain service providers capable of appropriately protecting the privacy of covered information received from Facebook.

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

H. On-Going Monitoring of the Privacy Program

Facebook's Privacy Program has built-in procedures to evaluate and adjust the Privacy Program in light of testing and monitoring results, as well as other relevant circumstances. As mentioned above, Facebook's privacy team works to identify, discuss, and assess compliance with privacy policies and procedures as well as applicable laws and regulations. Additionally, the Privacy Governance Team regularly discusses the Privacy Program in the context of various product and operational considerations. During these discussions, the team considers and reviews the effectiveness and efficiency of the Privacy Program and, when appropriate, makes adjustments to maintain the program's strength.

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

pwc

PwC's Privacy Assessment Approach

PwC's Assessment Standards

Part V of the Order requires that the Assessments be performed by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. This report was issued by PwC under professional standards which meet these requirements.

As a public accounting firm, PwC must comply with the public accounting profession's technical and ethical standards, which are enforced through various mechanisms created by the American Institute of Certified Public Accountants ("AICPA"). Membership in the AICPA requires adherence to the Institute's Code of Professional Conduct. The AICPA's Code of Professional Conduct and its enforcement are designed to ensure that CPAs who are members of the AICPA accept and achieve a high level of responsibility to the public, clients, and colleagues. The AICPA Professional Standards provide the discipline and rigor required to ensure engagements performed by CPAs consistently follow specific General Standards, Standards of Fieldwork, and Standards of Reporting ("Standards").

In order to accept and perform this FTC assessment ("engagement"), the Standards state that PwC, as a practitioner, must meet specific requirements, such as the following.

General Standards:

- Have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users. Suitable criteria must be free from bias (objective), permit reasonably consistent measurements, qualitative or quantitative, of subject matter (measurable), be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted (complete), and be relevant to the subject matter;
- Have adequate technical training and proficiency to perform the engagement;
- Have adequate knowledge of the subject matter; and
- Exercise due professional care in planning and performance of the engagement and the preparation of the report.

Standards of Fieldwork:

- Adequately plan the work and properly supervise any assistants; and
- Obtain sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.

Standards of Reporting:

- Identify the assertion being reported on in the report; and
- State the practitioner's conclusion about the assertion in relation to the criteria.

In performing this assessment, PwC complied with all of these Standards.

Independence

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

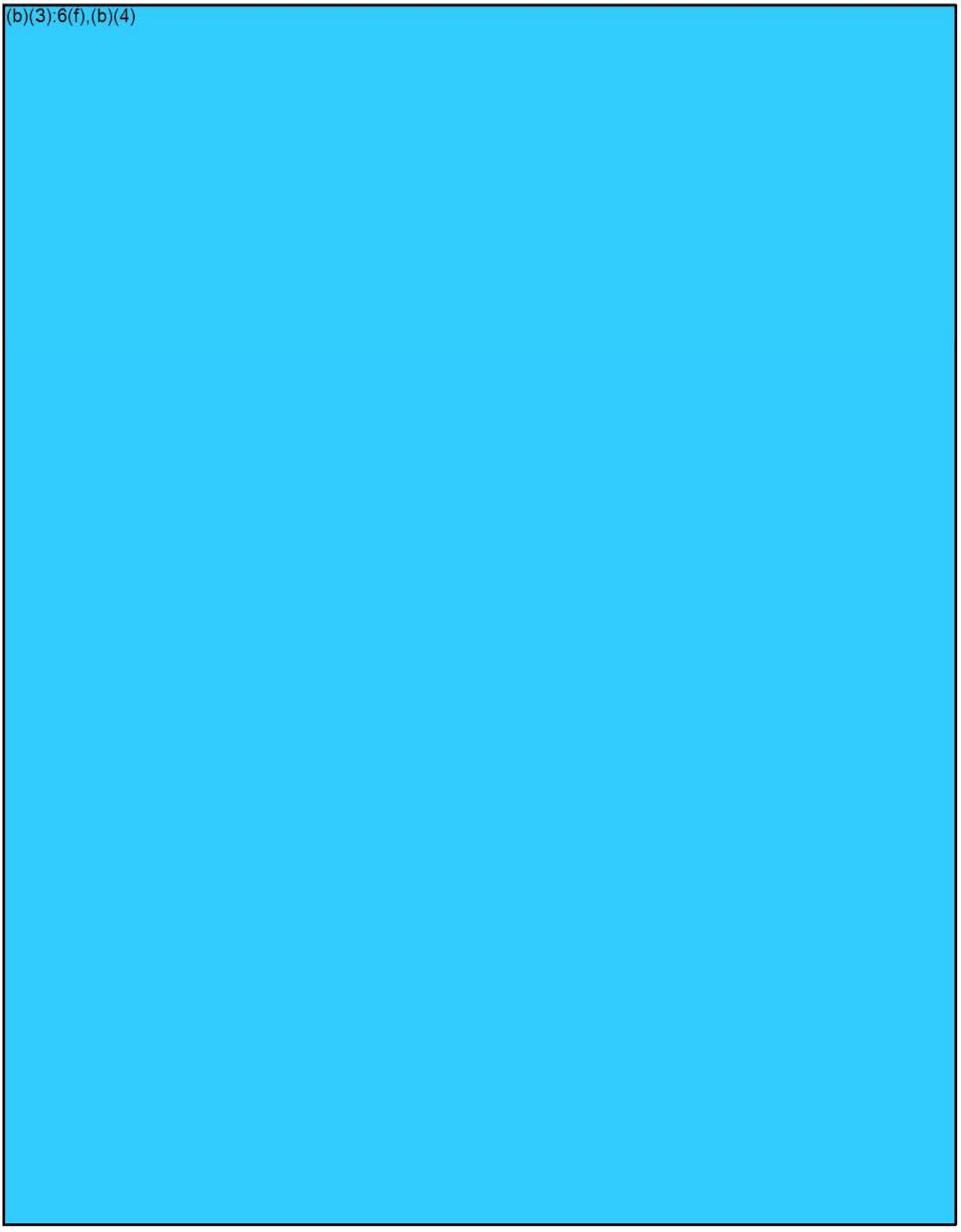
PwC is independent with respect to the Standards required for this engagement.

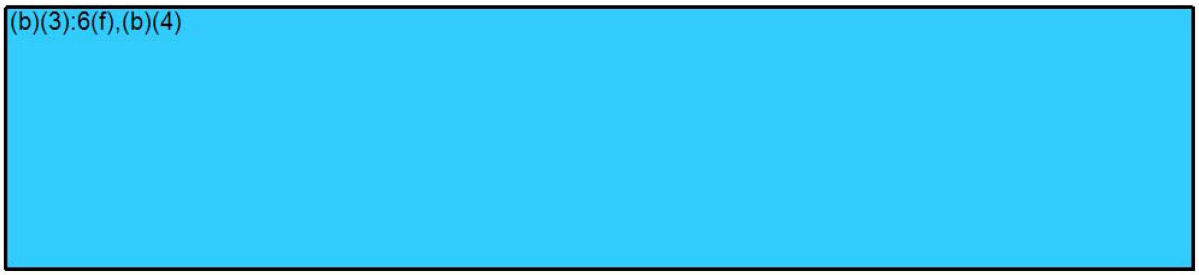
PwC Assessor Qualifications

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

PwC Assessment Process Overview

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


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


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

pwc

PwC's Assessment of Part IV A, B, C, D and E, of the Order

The tables in section "Facebook's Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results" of this report describe the scope of Facebook's Privacy Program referenced in the Management Assertion on pages 52-53. Facebook established its privacy program by implementing privacy controls to meet or exceed the protections required by Part IV of the Order. The table also includes PwC's inquiry, observation, and inspection/examination test procedures to assess the effectiveness of Facebook's program and test results. PwC's final conclusions are detailed on pages 4-5 of this document.

A. Set forth the specific privacy controls that respondent has implemented and maintained during the reporting period.

As depicted within the table on pages 22-51, Facebook has listed the privacy controls that were implemented and maintained during the reporting period.

B. Explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information.

Based on the size and complexity of the organization, the nature and scope of Facebook's activities, and the sensitivity of the covered information (as defined in by the Order), Facebook management developed the company-specific criteria (assertions) detailed on pages 52-53 as the basis for its Privacy Program. The management assertions and the related control activities are intended to be implemented to address the risks identified by Facebook's privacy risk assessment.

C. Explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of the Order.

As summarized in the Facebook's Privacy Program on pages 6-14, Facebook has implemented the following protections:

> A. Designation of an employee or employees to coordinate and be responsible for the privacy program.
>
> As described above, Facebook has designated a team of employees to coordinate and be responsible for the Privacy Program as required by Part IV of the Order. As described on pages 22-23 (Management's Assertion A), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.
>
> B. The identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation,

including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

As described above, Facebook has identified reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information, and assessed the sufficiency of any safeguards in place to control these risks as required by Part IV of the Order. As described on page 24 (Management's Assertion B), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

C. The design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.

As described above, Facebook has designed and implemented reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures as required by Part IV of the Order. As described on pages 25-44 (Management's Assertions C, D, E, and F), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

D. The development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

As described above, Facebook has developed and implemented reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Facebook as required by Part IV of the Order. Facebook also includes terms in contracts with service providers requiring that such service providers implement and maintain appropriate privacy protections. As described on pages 45-46 (Management's Assertion G), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Part IV of the Order.

E. The evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

As described above, Facebook has evaluated and adjusted its Privacy Program in light of the results of the testing and monitoring required by subpart C within Part IV of the Order, any material changes to Facebook's operations or business arrangements, or any other circumstances that Facebook knows or has reason to

know may have a material impact on the effectiveness of its privacy program as required by Part IV of the Order. As described on pages 47-51 (Management's Assertion H), PwC performed test procedures to assess the effectiveness of the Facebook privacy controls implemented to meet or exceed the protections required by Paragraph IV of the Order.

D. Certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

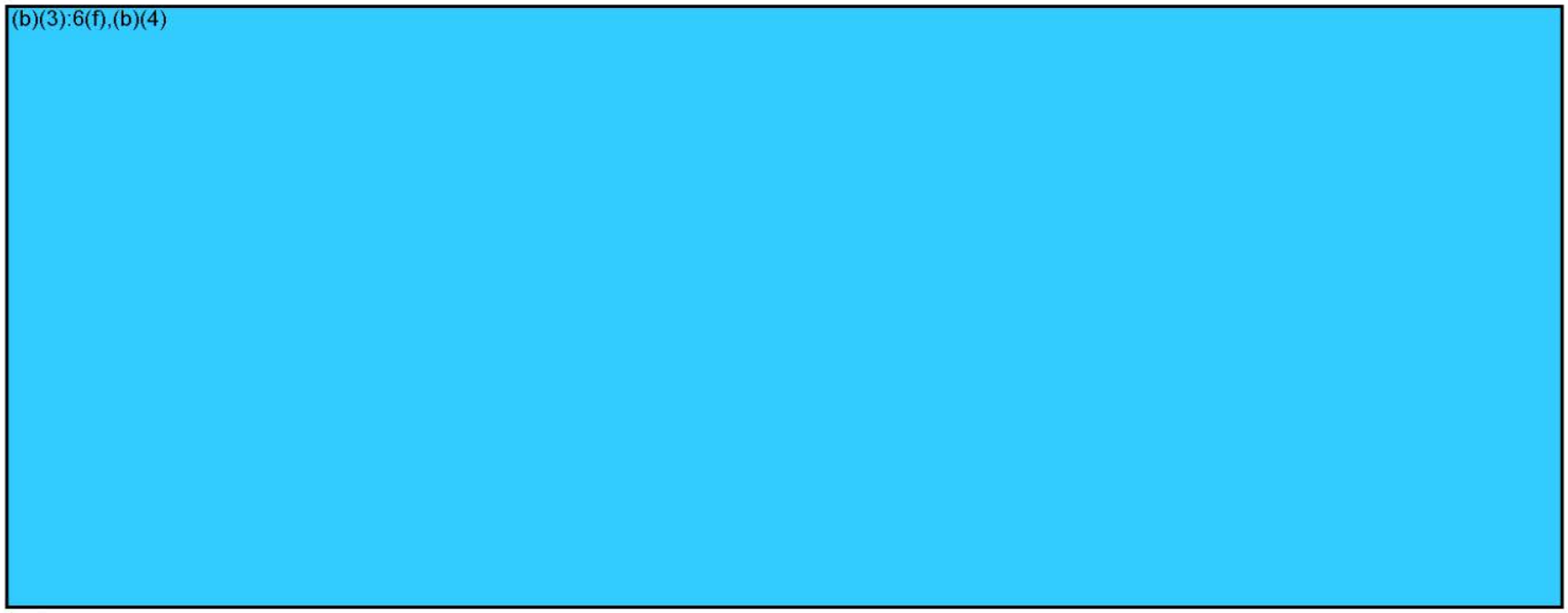
As described in the PwC Assessment Process Overview section above, PwC performed its assessment of Facebook's Privacy Program in accordance with AICPA Attestation Standards. Refer to pages 4-5 of this document for PwC's conclusions.

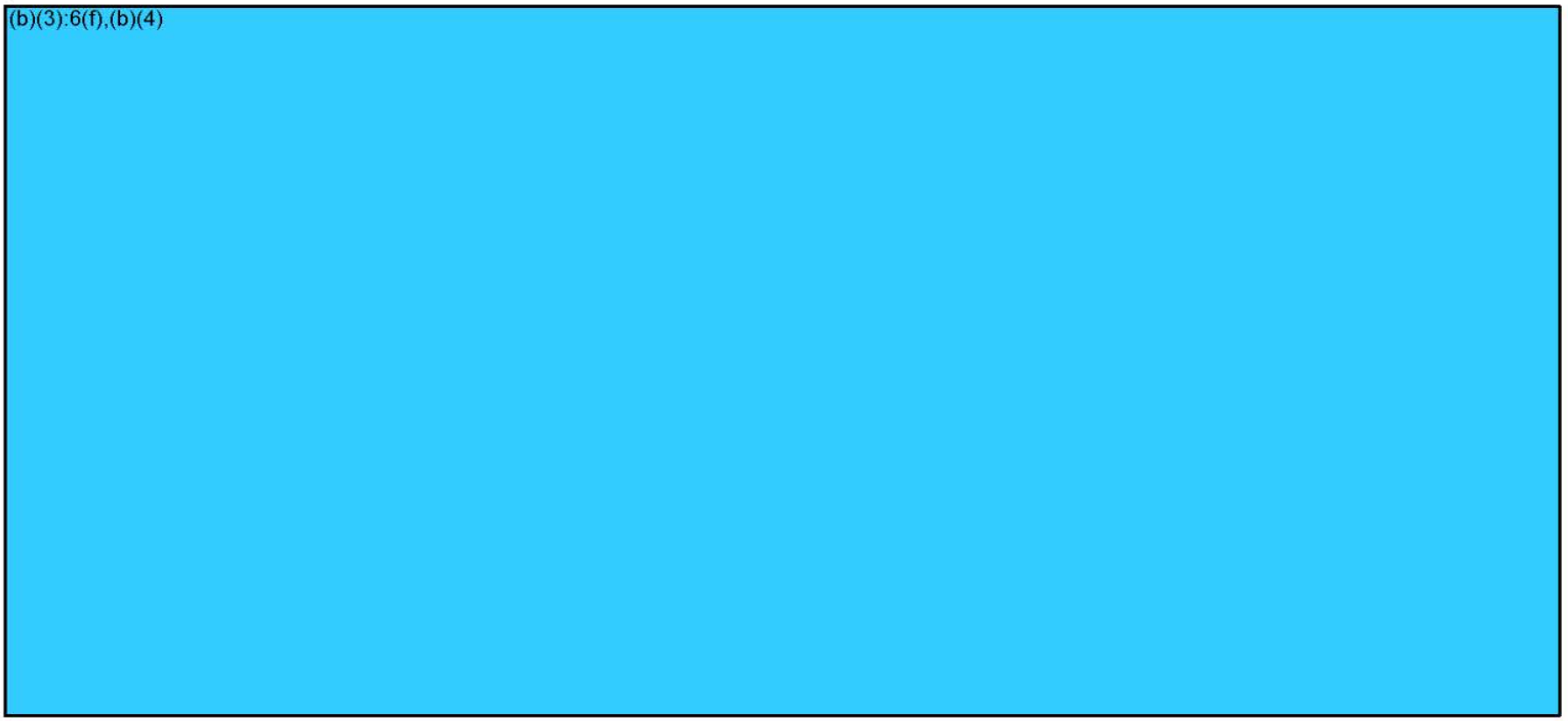
pwc

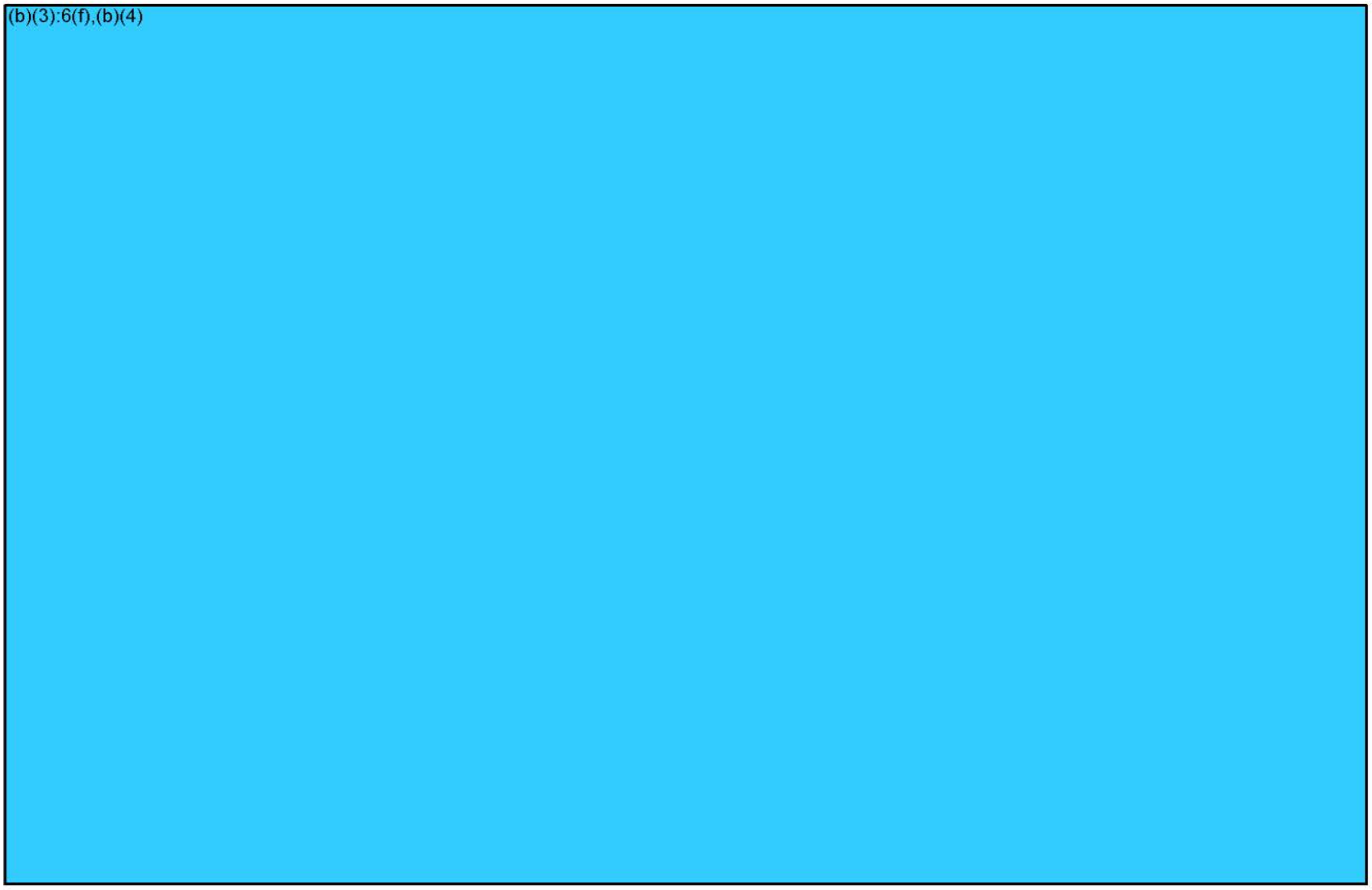
Facebook's Privacy Program: Assertions, Control Activities and PwC's Tests Performed and Results

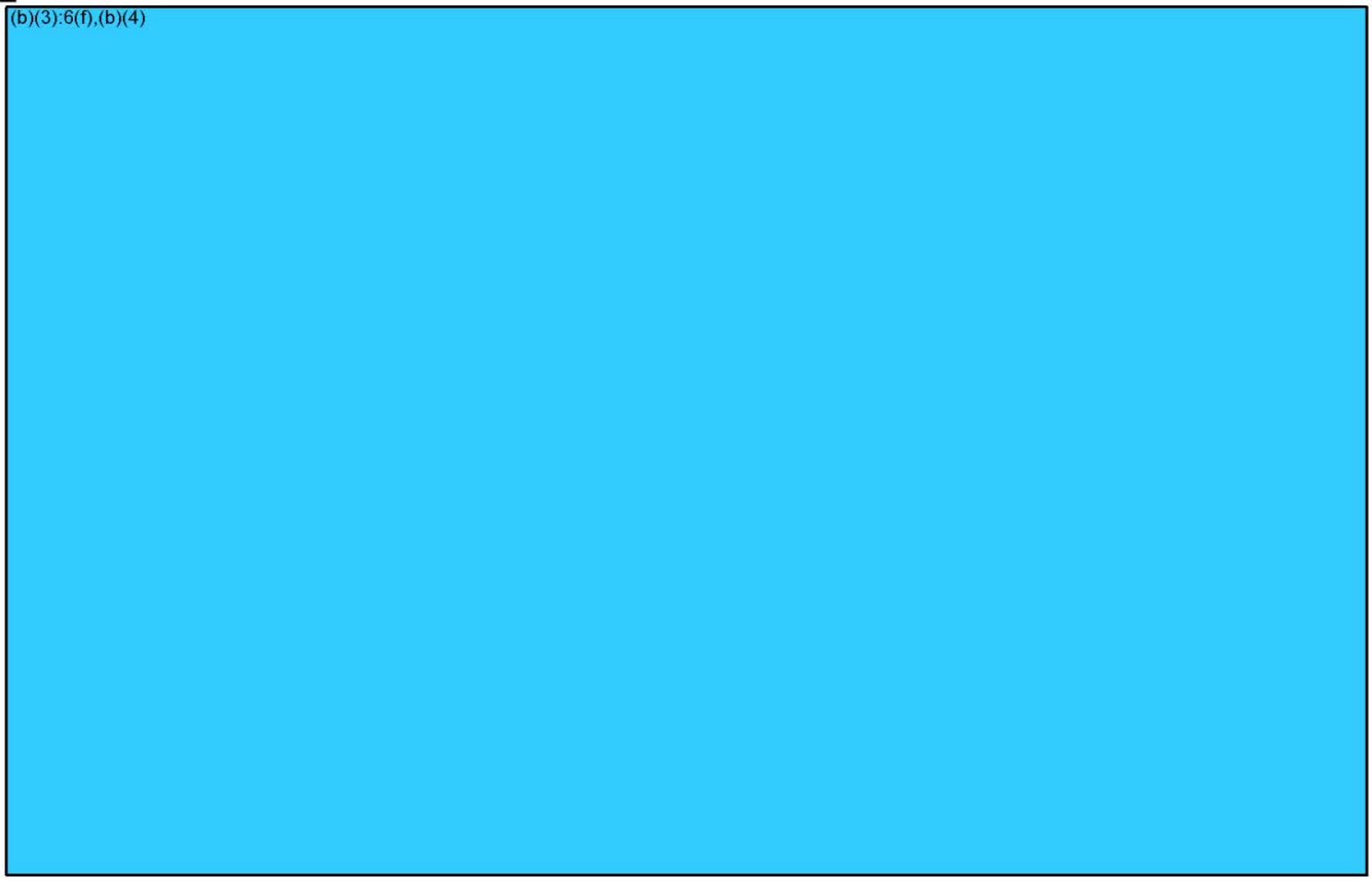
Provided below are the Facebook Privacy Program controls and PwC's tests performed. Also provided are the results of the testing performed by PwC. Finally, additional information has been provided by PwC for the instances in which PwC identified an exception during testing. This information is provided in an effort to enhance the FTC's understanding of the exception.

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

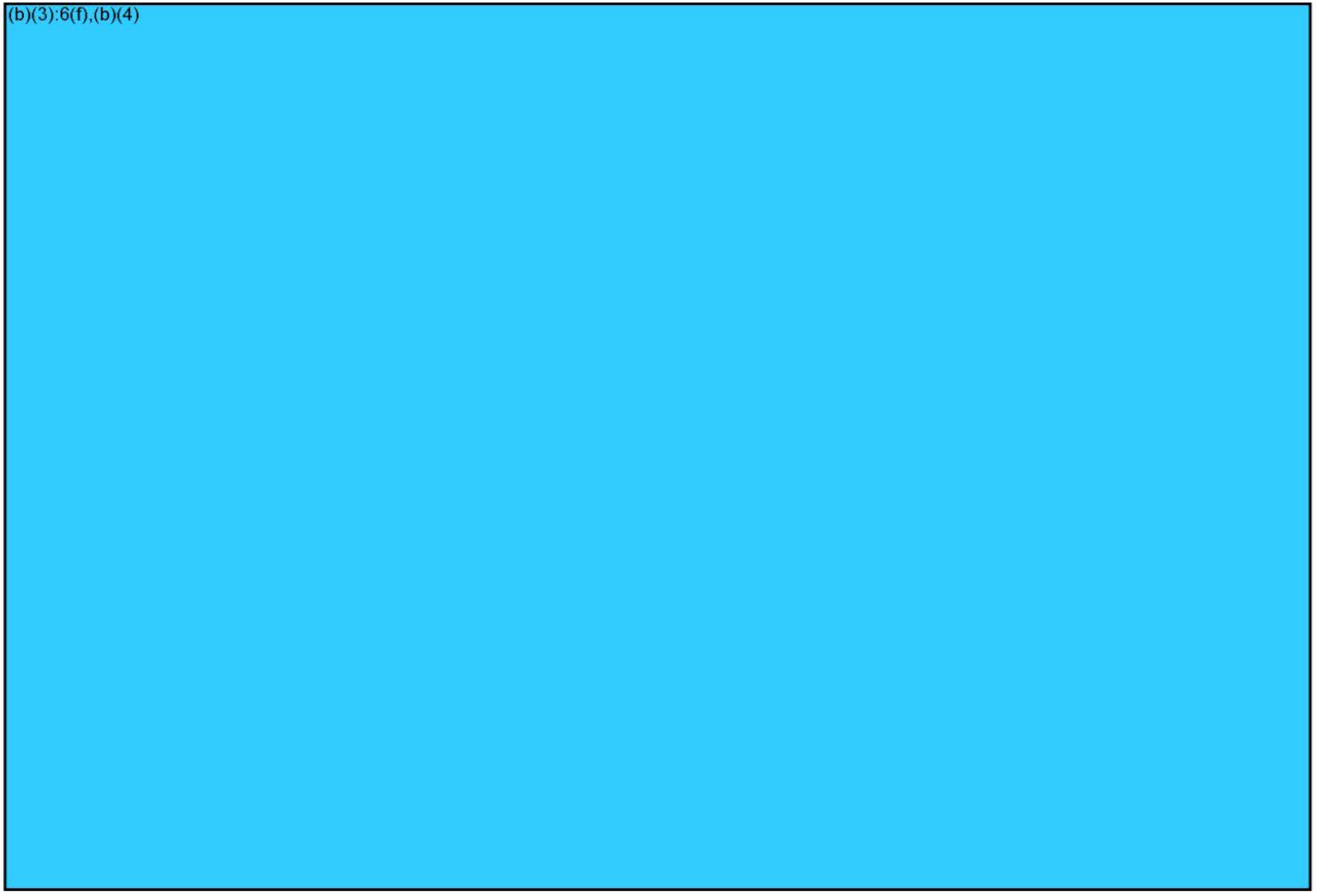

(b)(3):6(f),(b)(4)

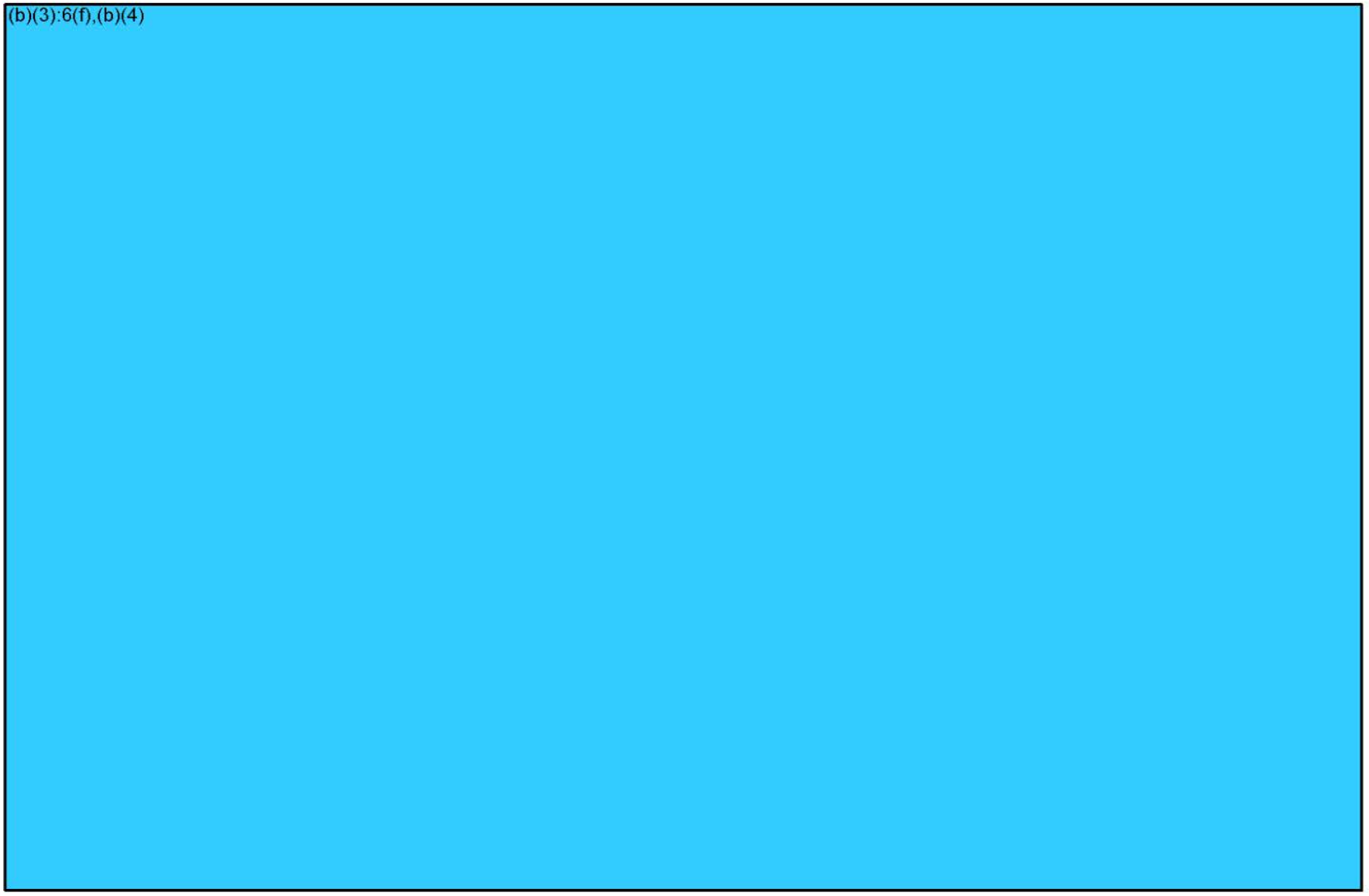

(b)(3):6(f),(b)(4)

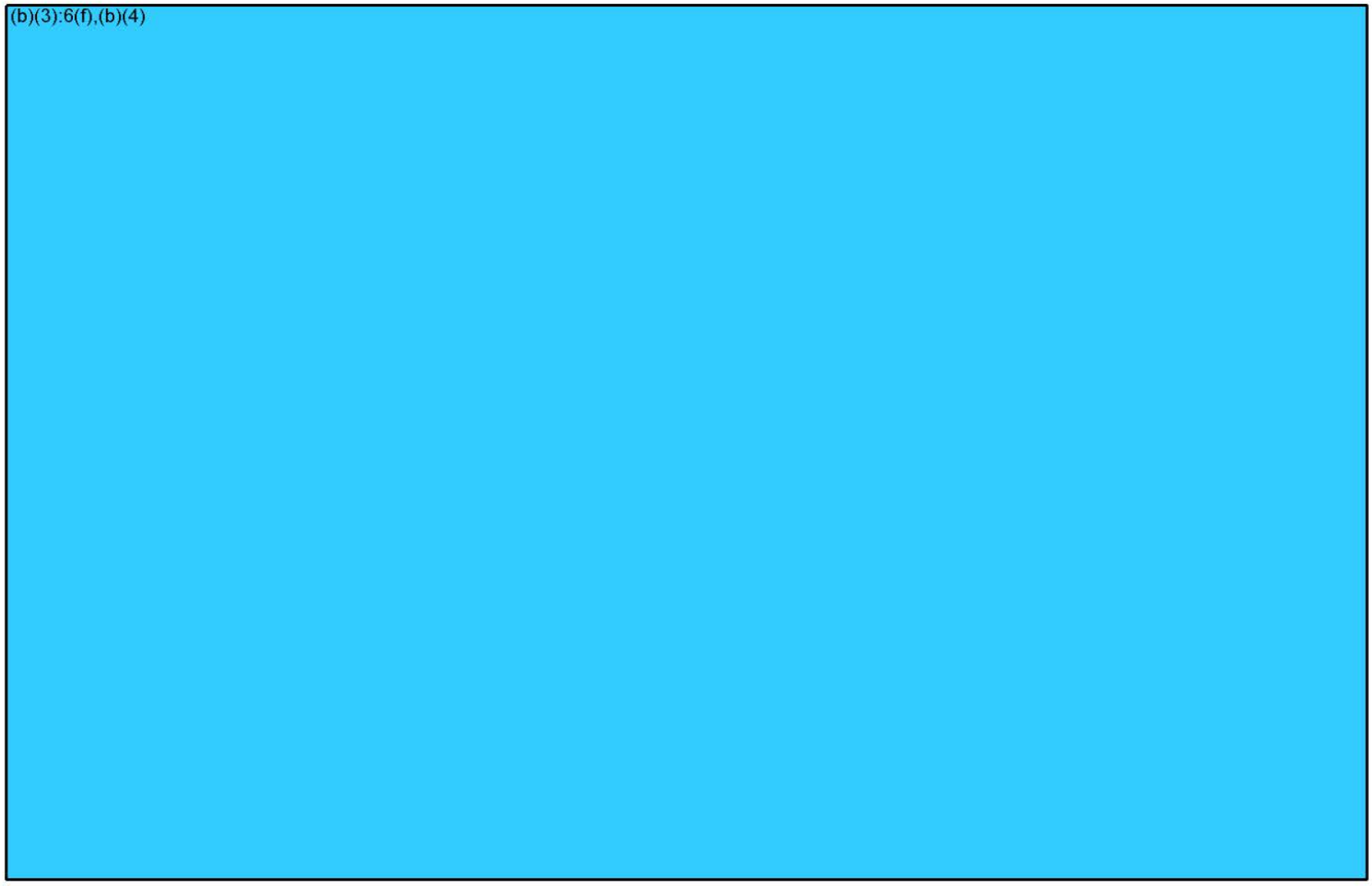

(b)(3):6(f),(b)(4)

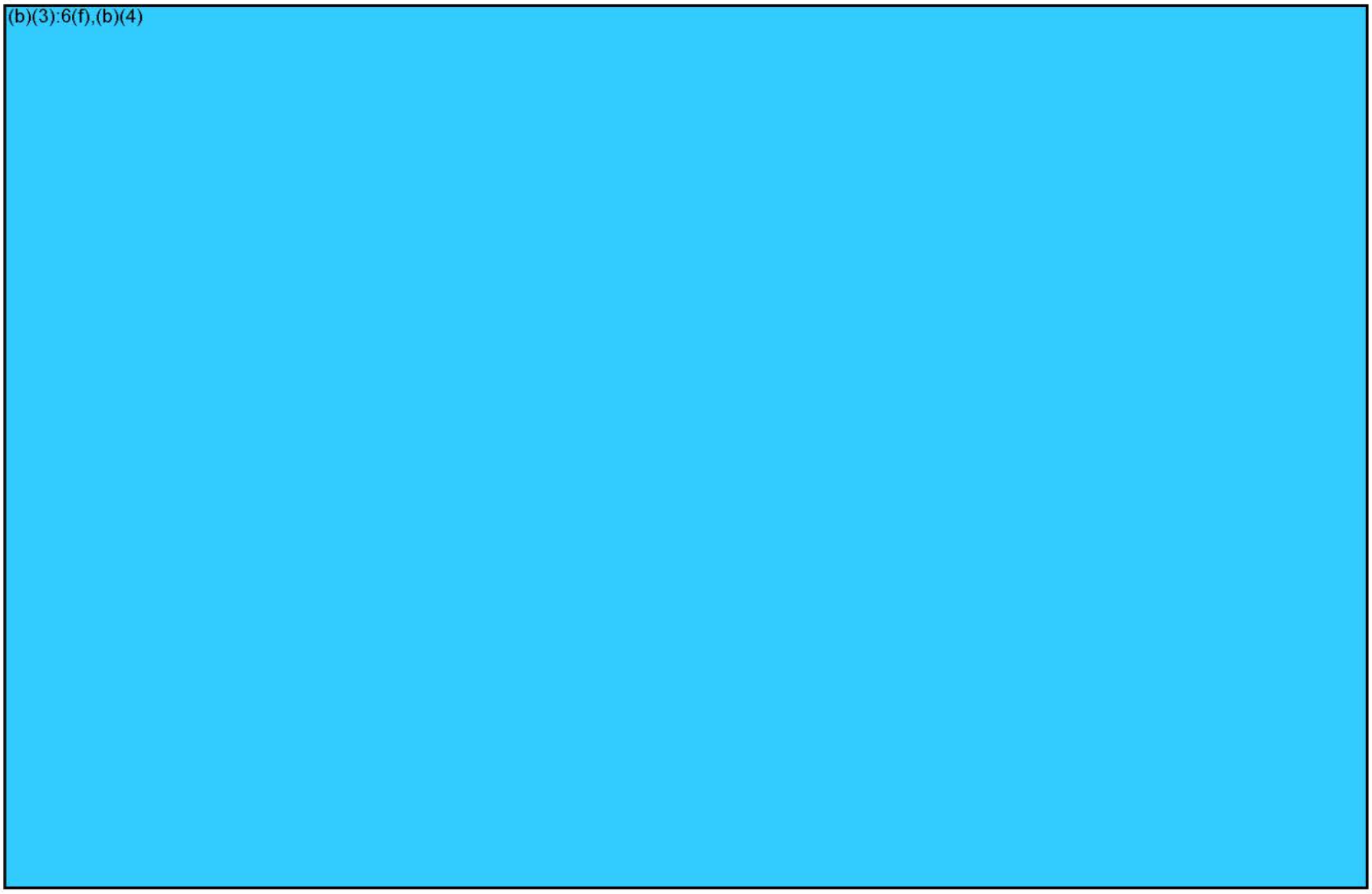

(b)(3):6(f),(b)(4)

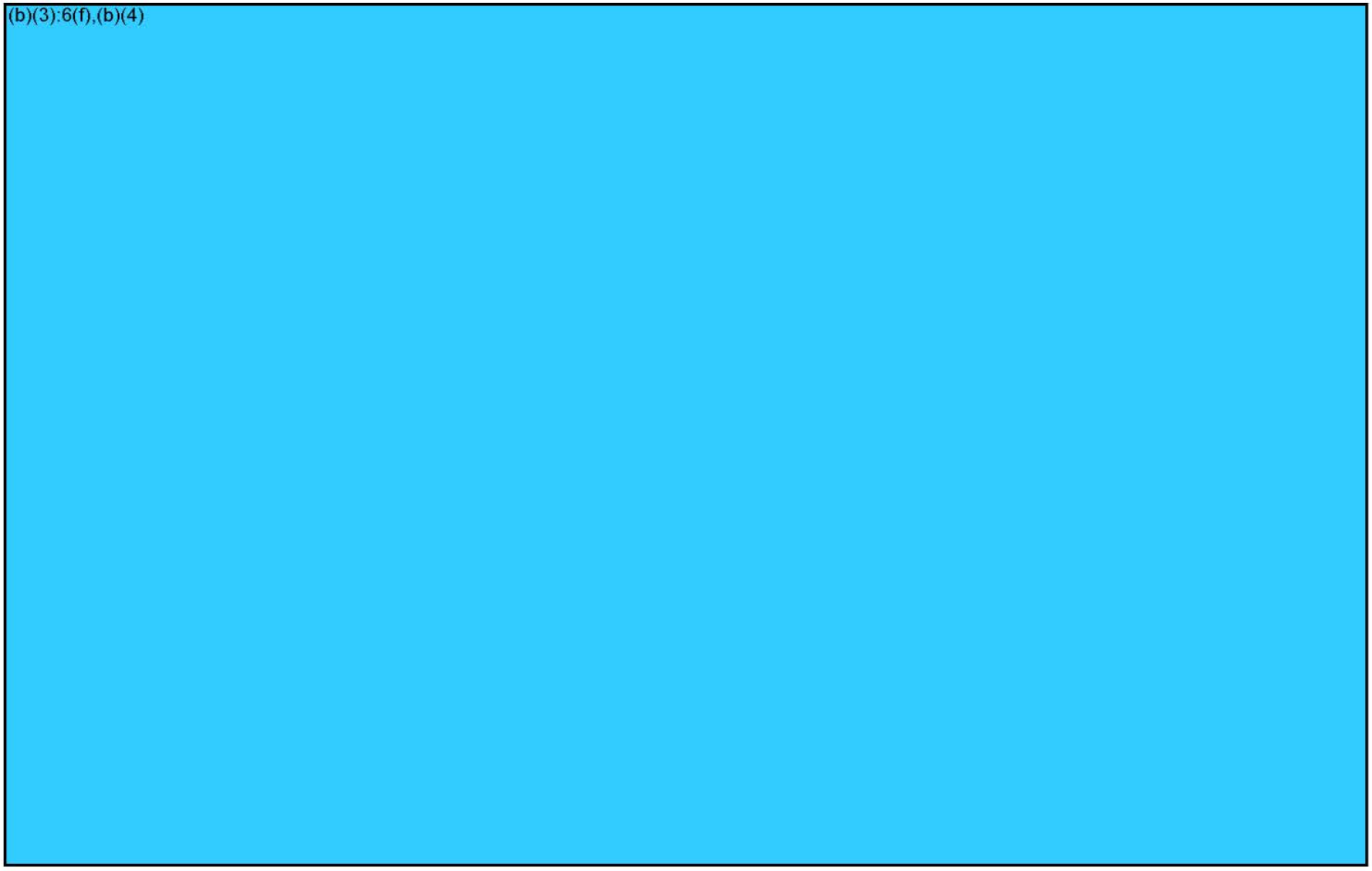
pwc

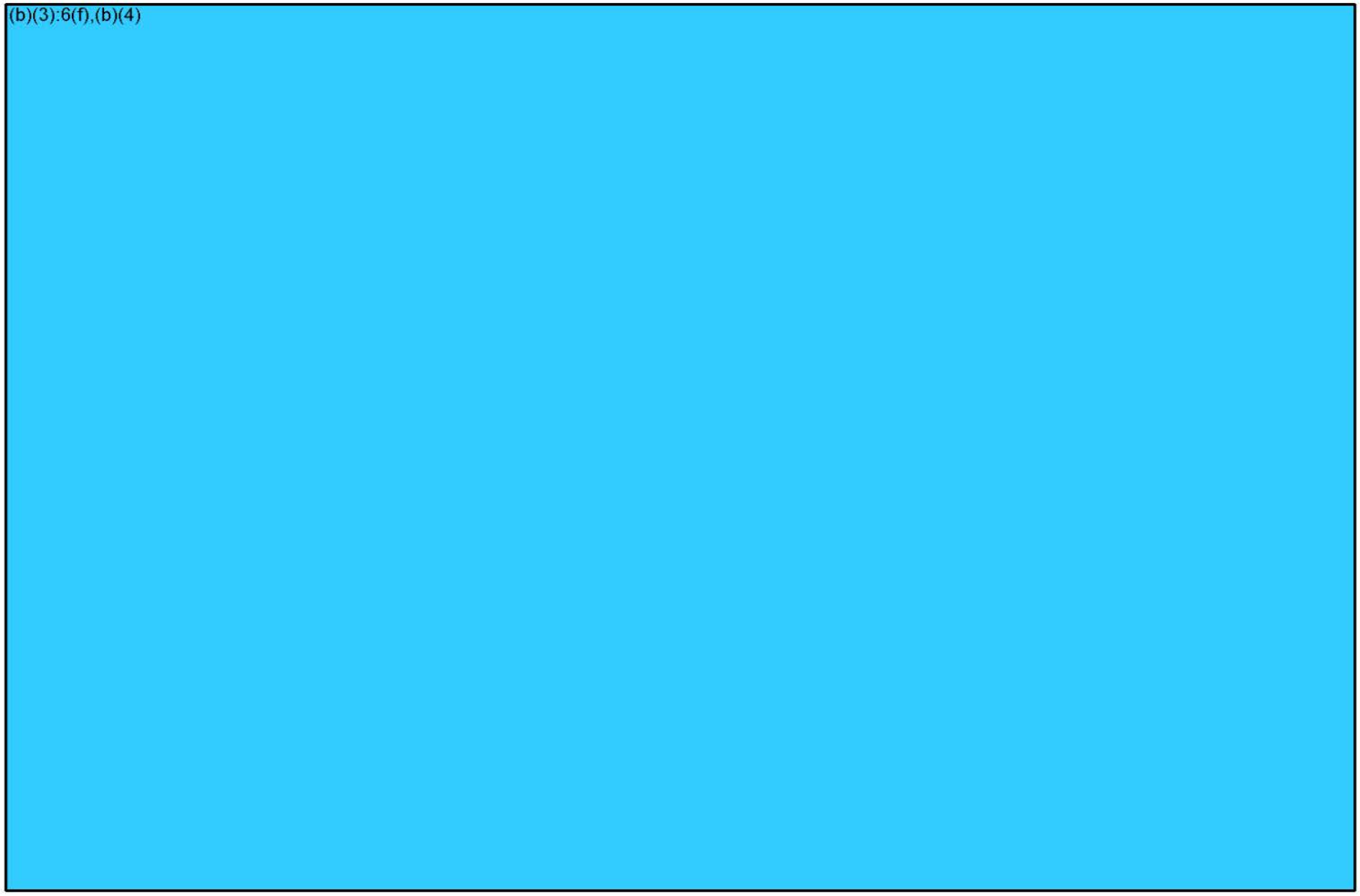


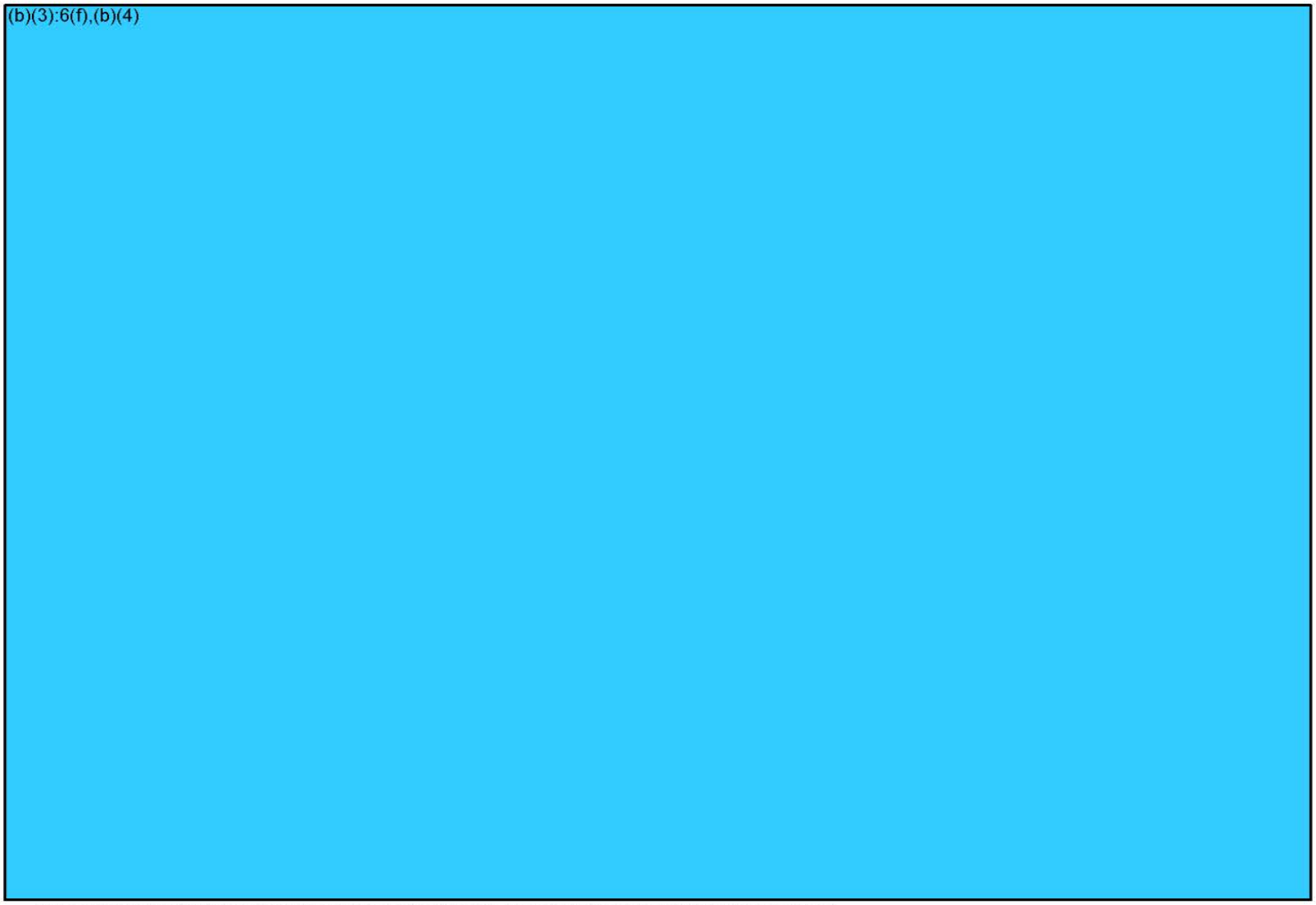

(b)(3):6(f),(b)(4)


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

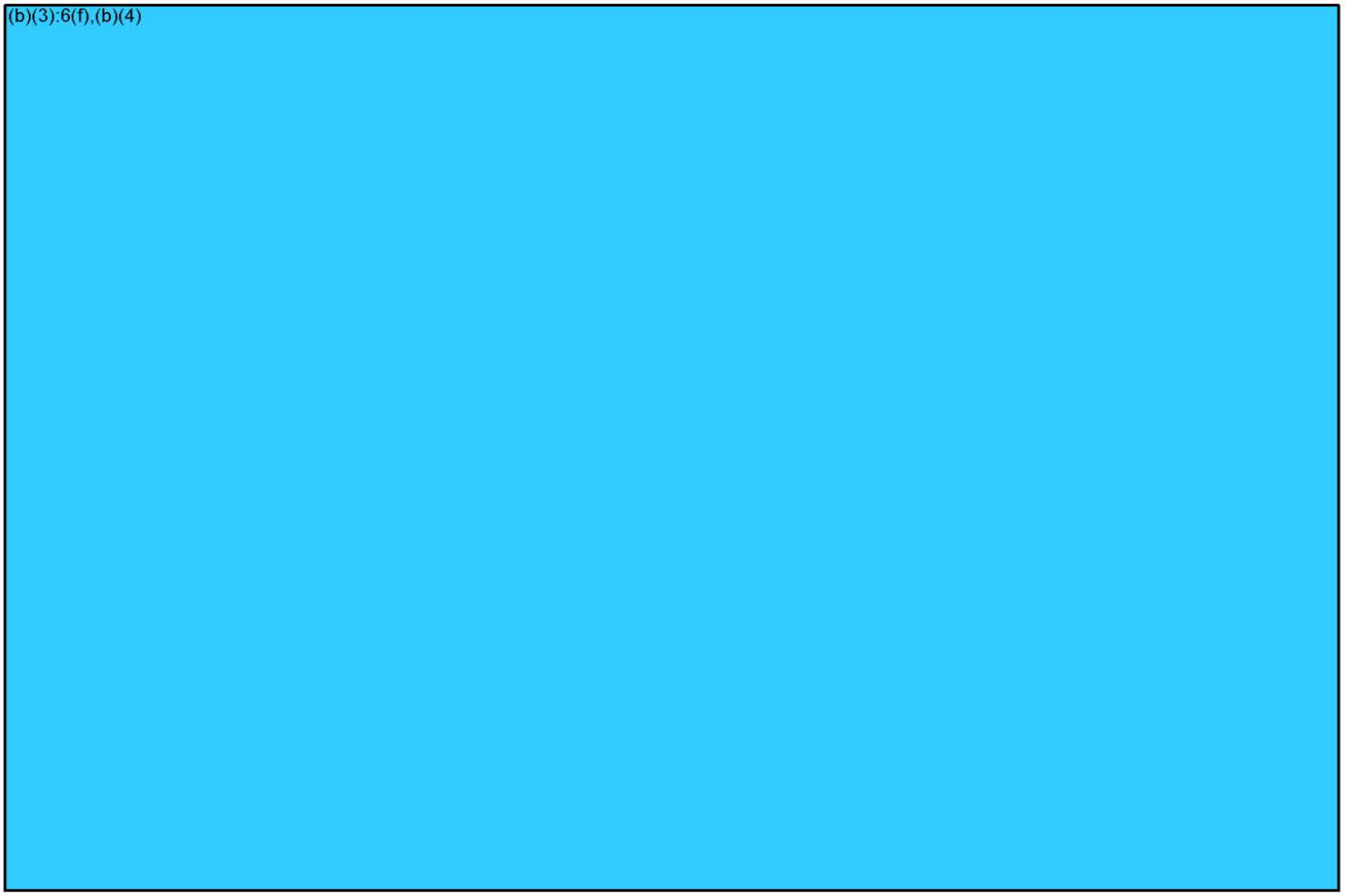

(b)(3):6(f),(b)(4)


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

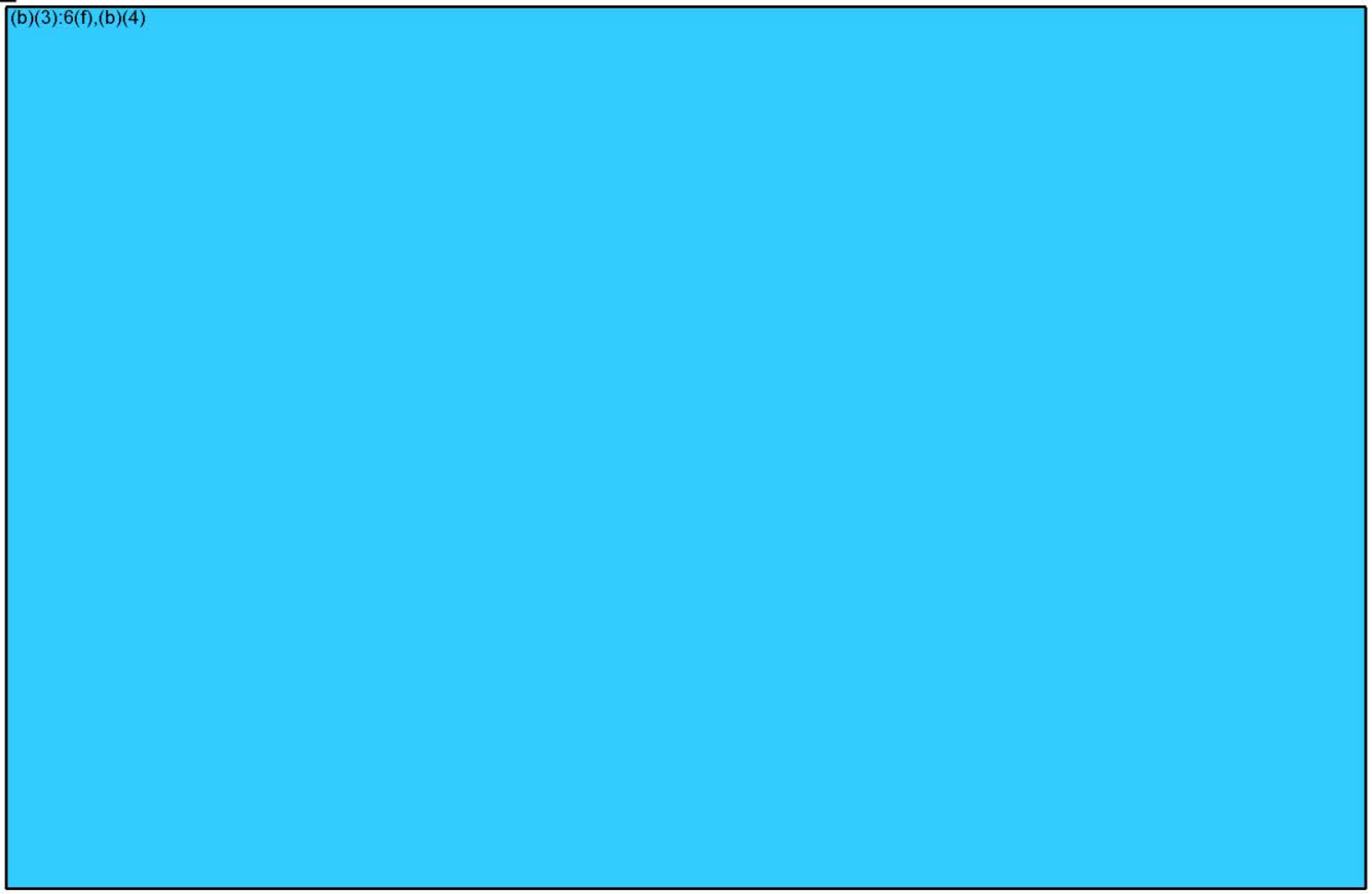


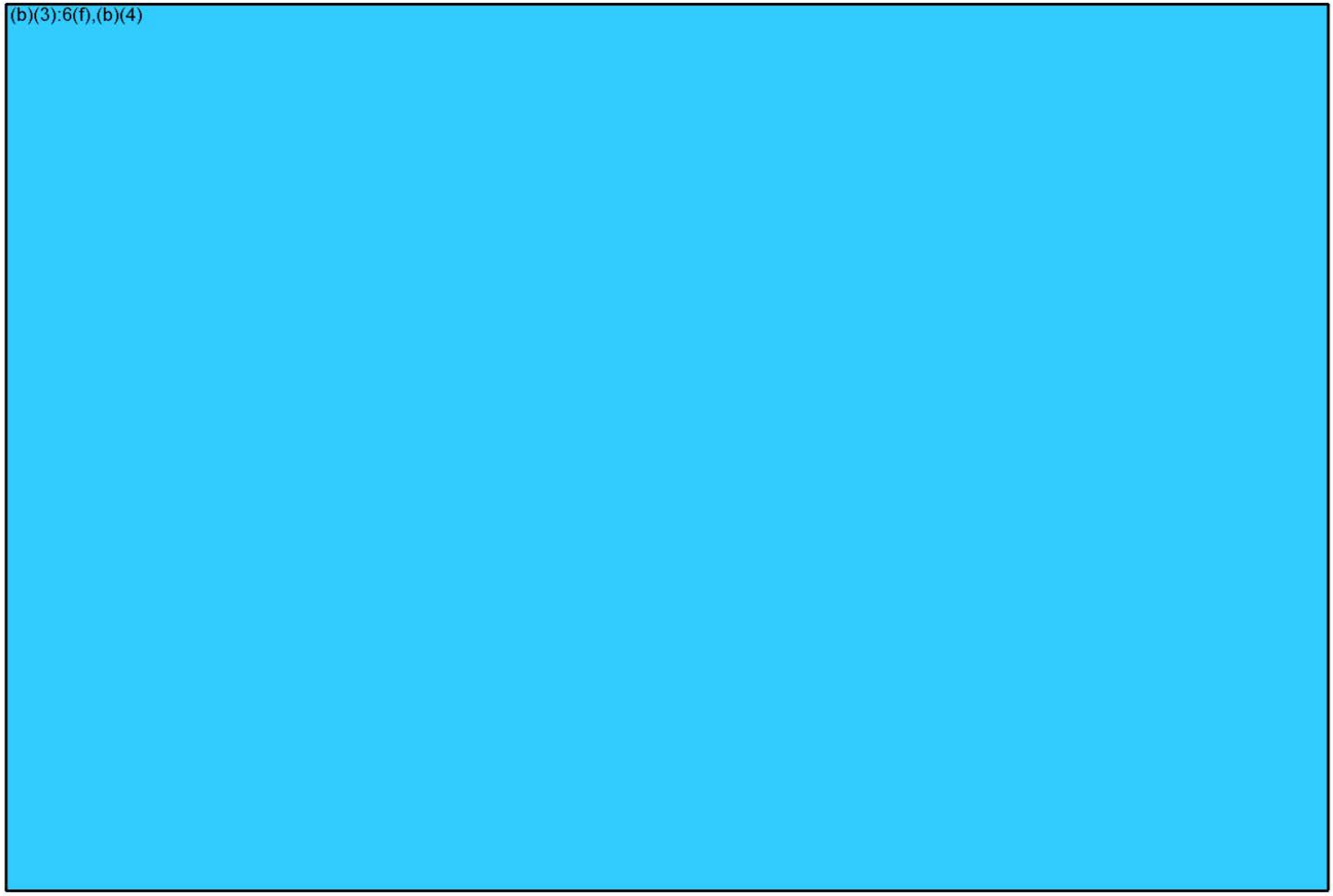

(b)(3):6(f),(b)(4)

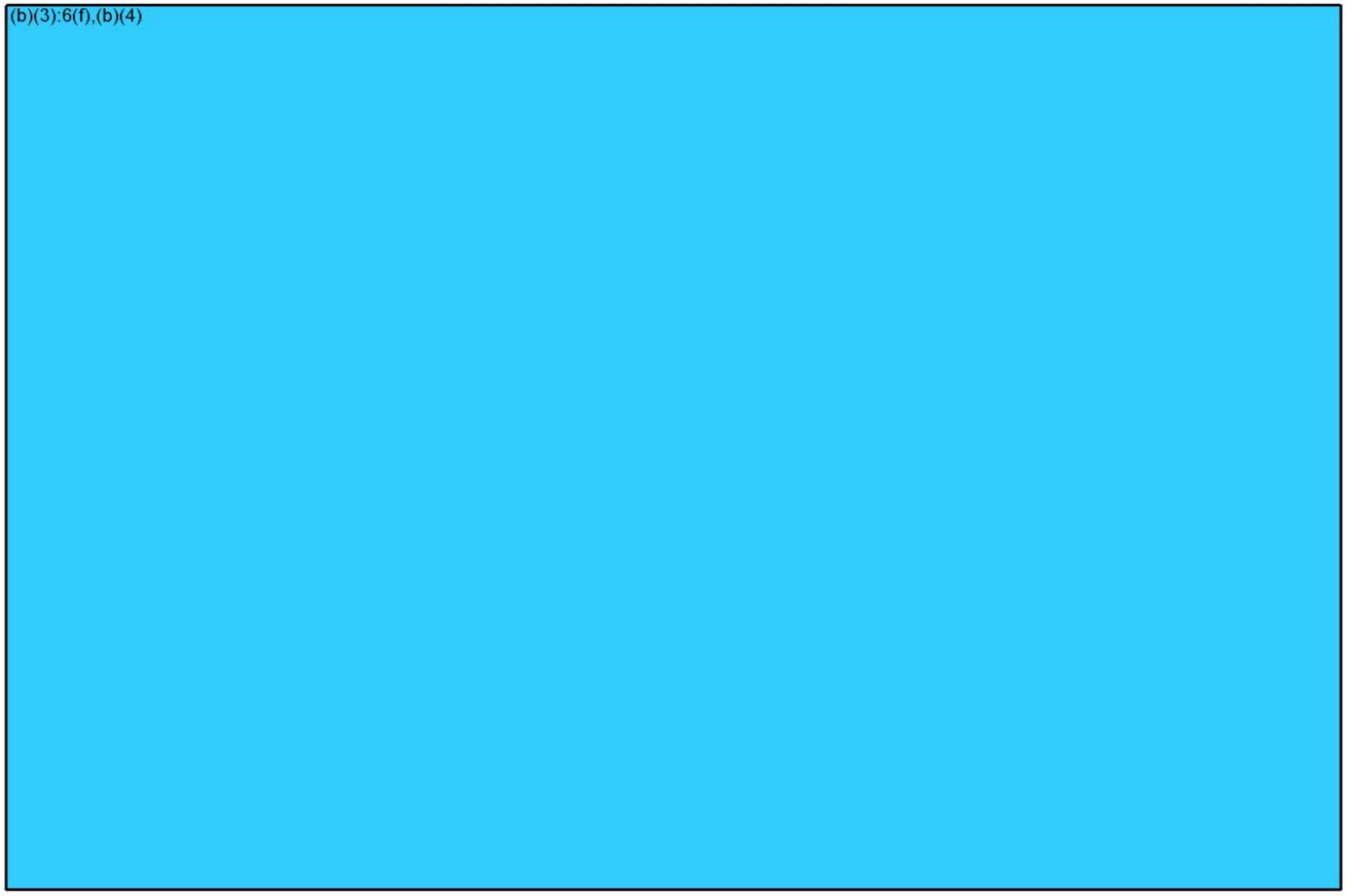
pwc

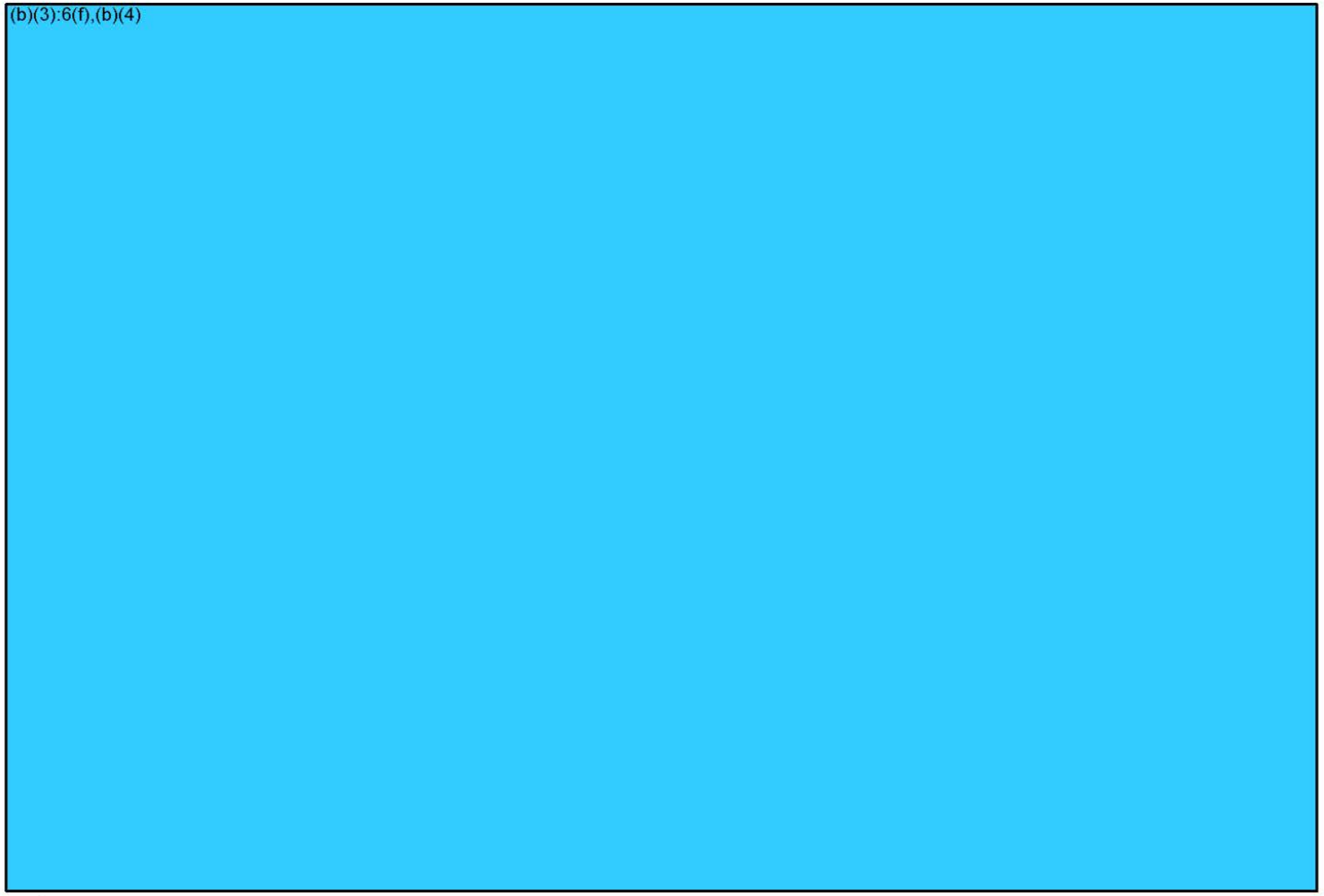


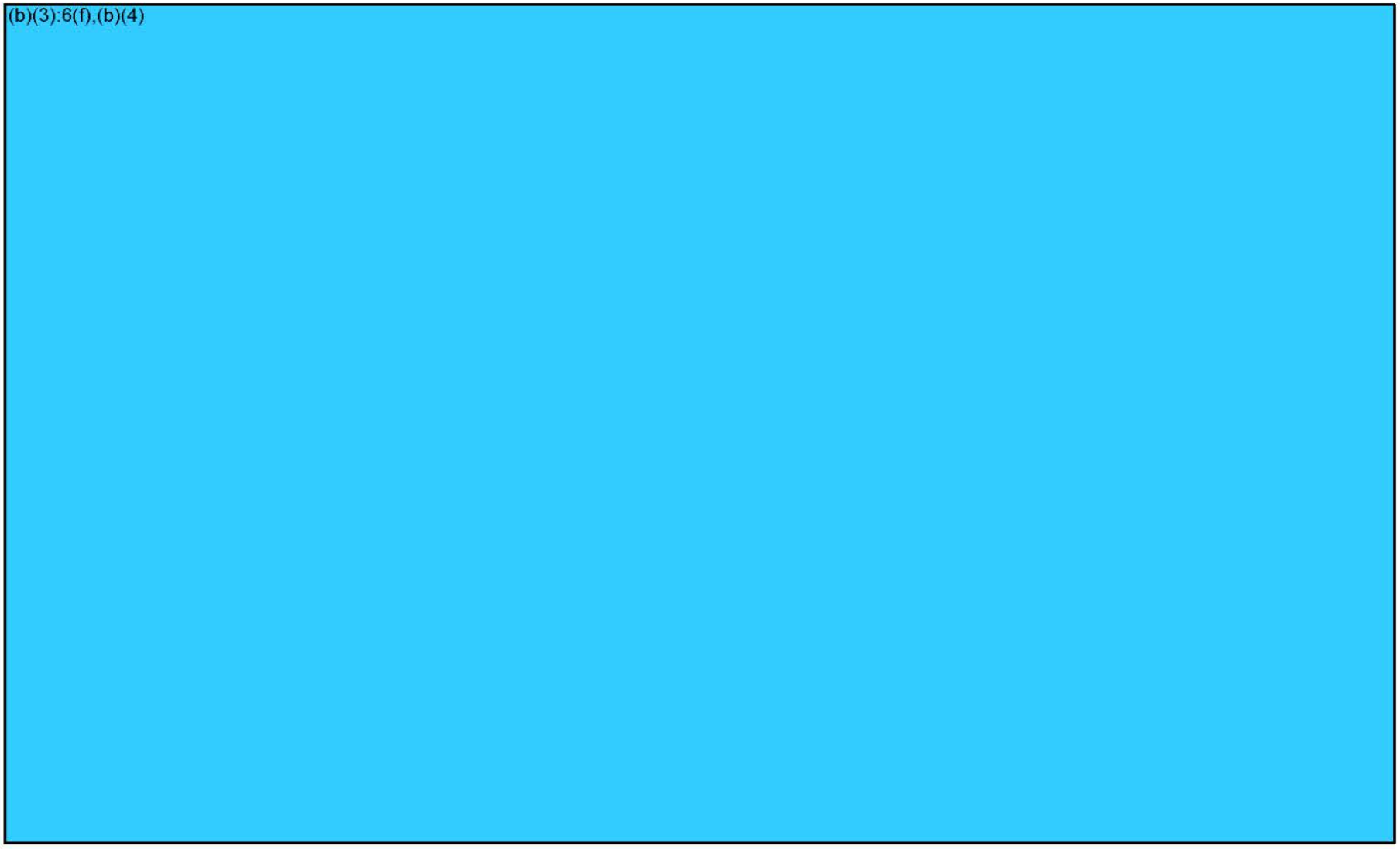
pwc



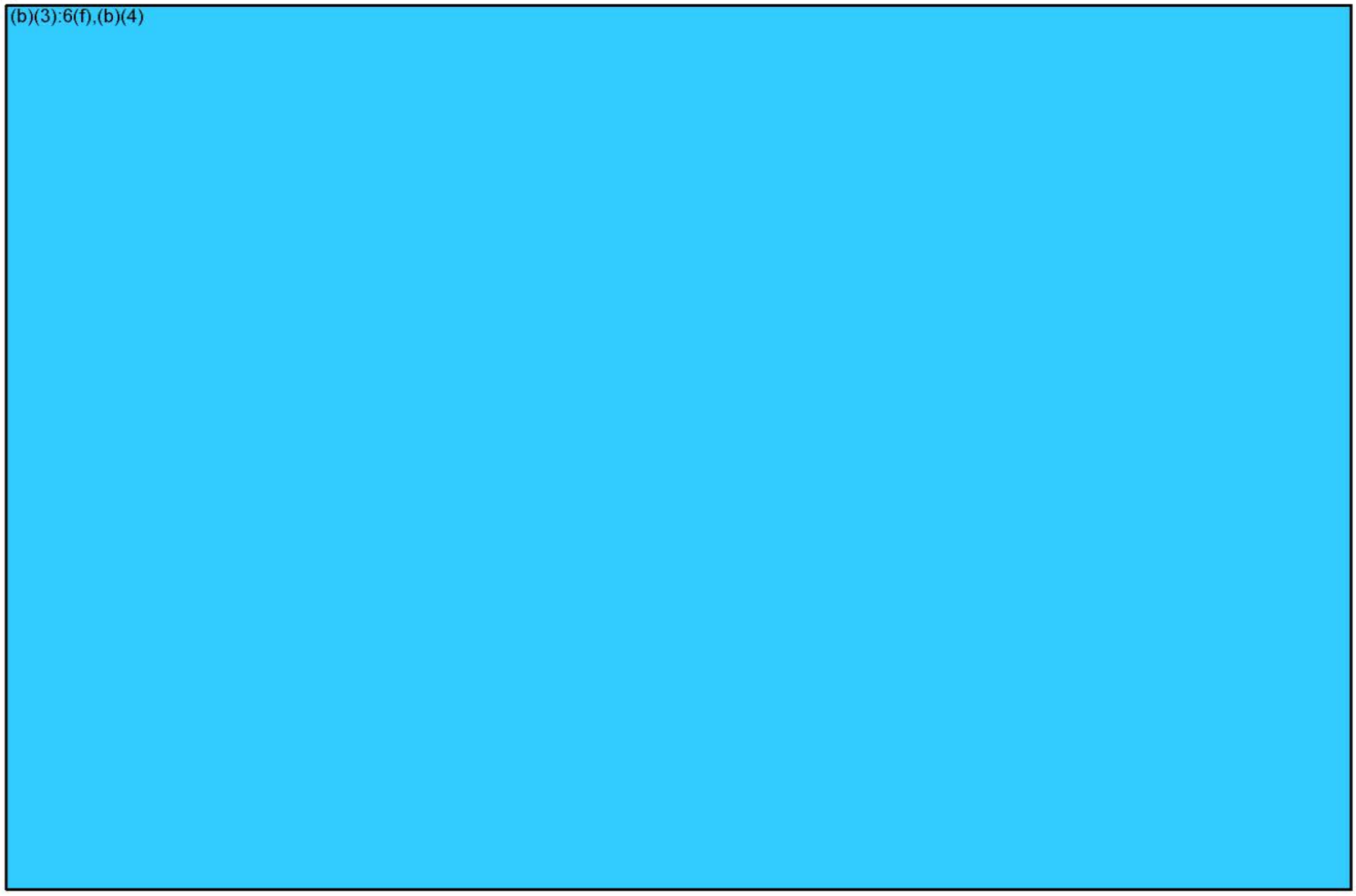

(b)(3):6(f),(b)(4)

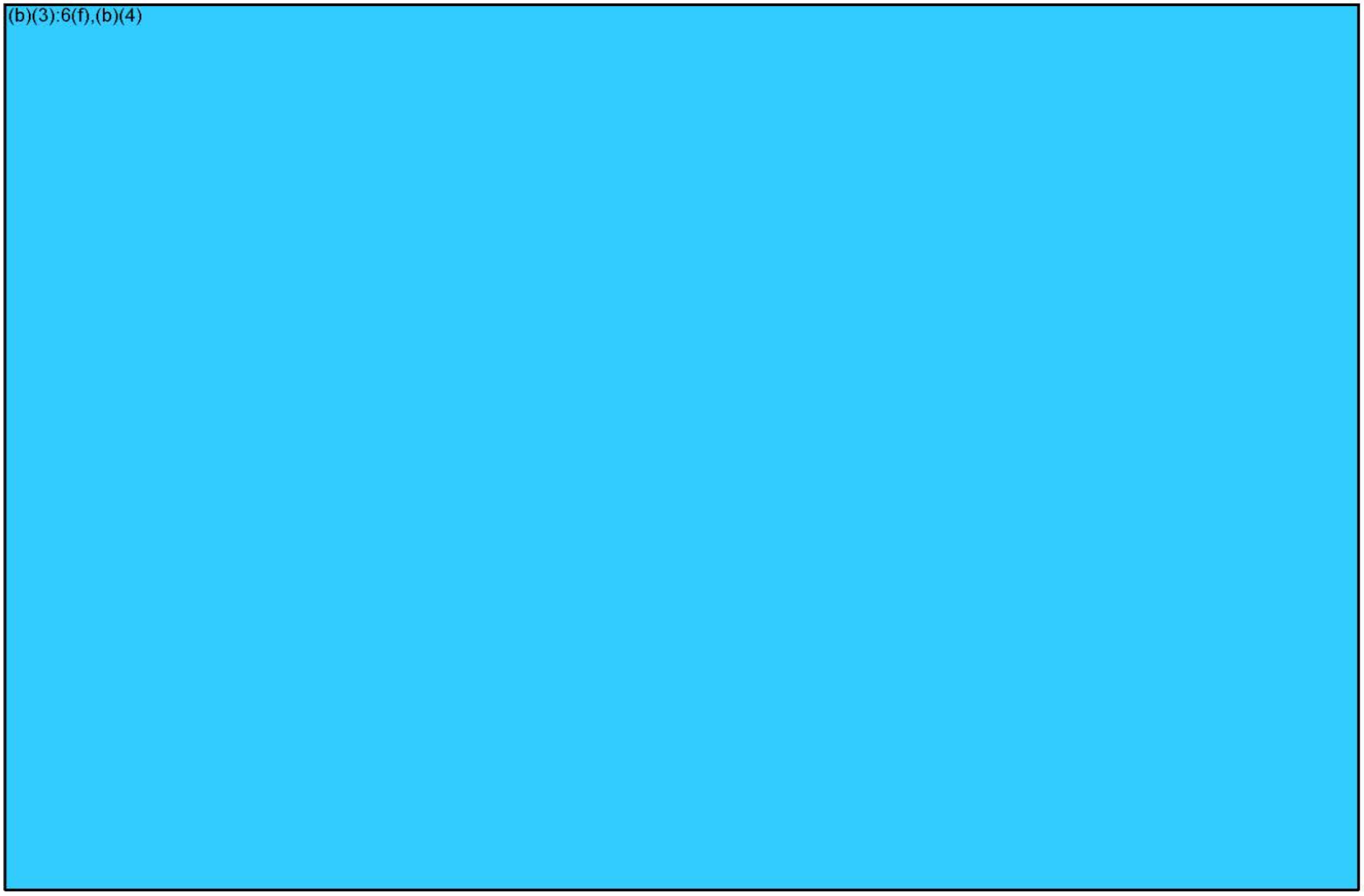

(b)(3):6(f),(b)(4)

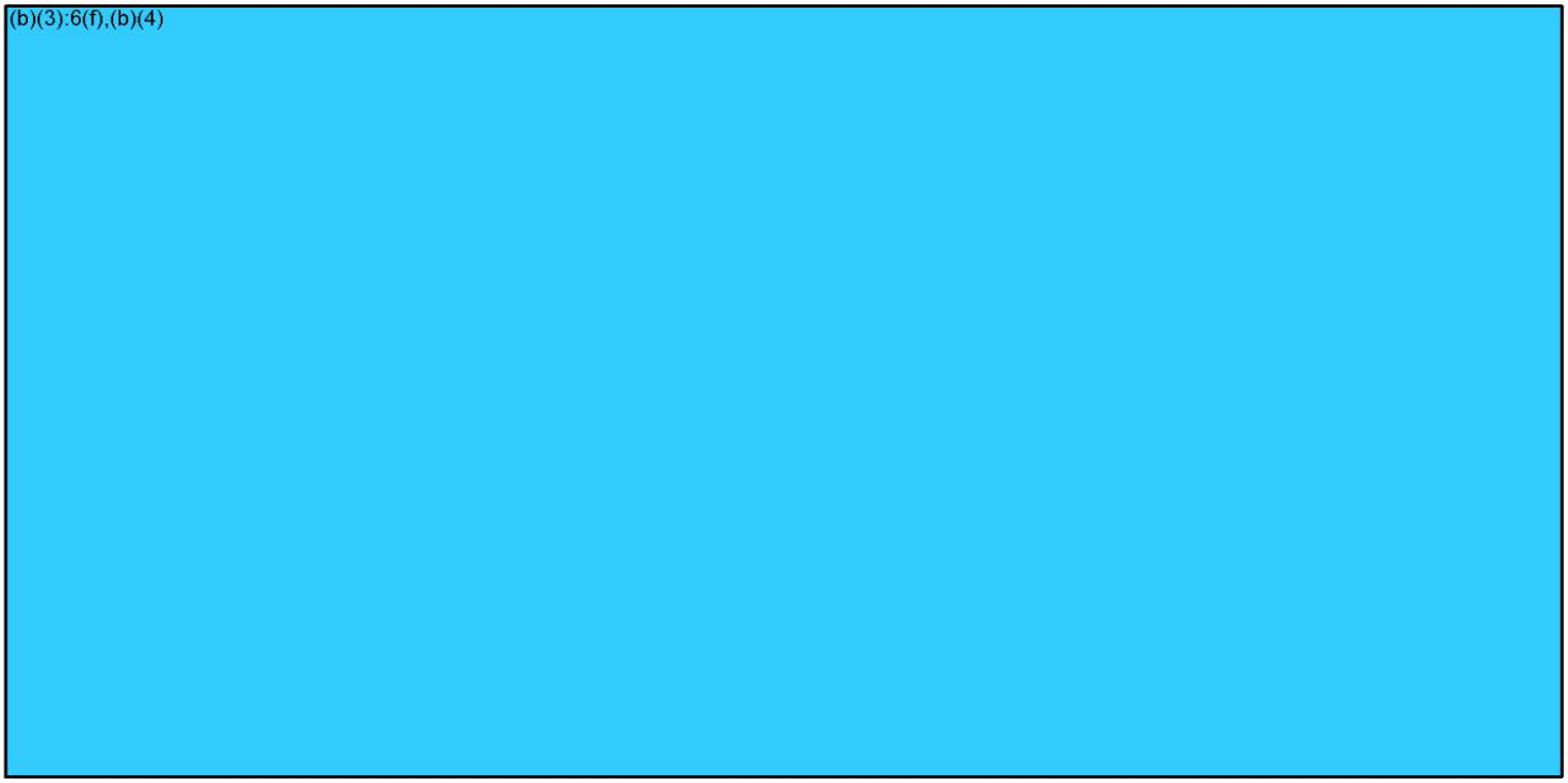

(b)(3):6(f),(b)(4)

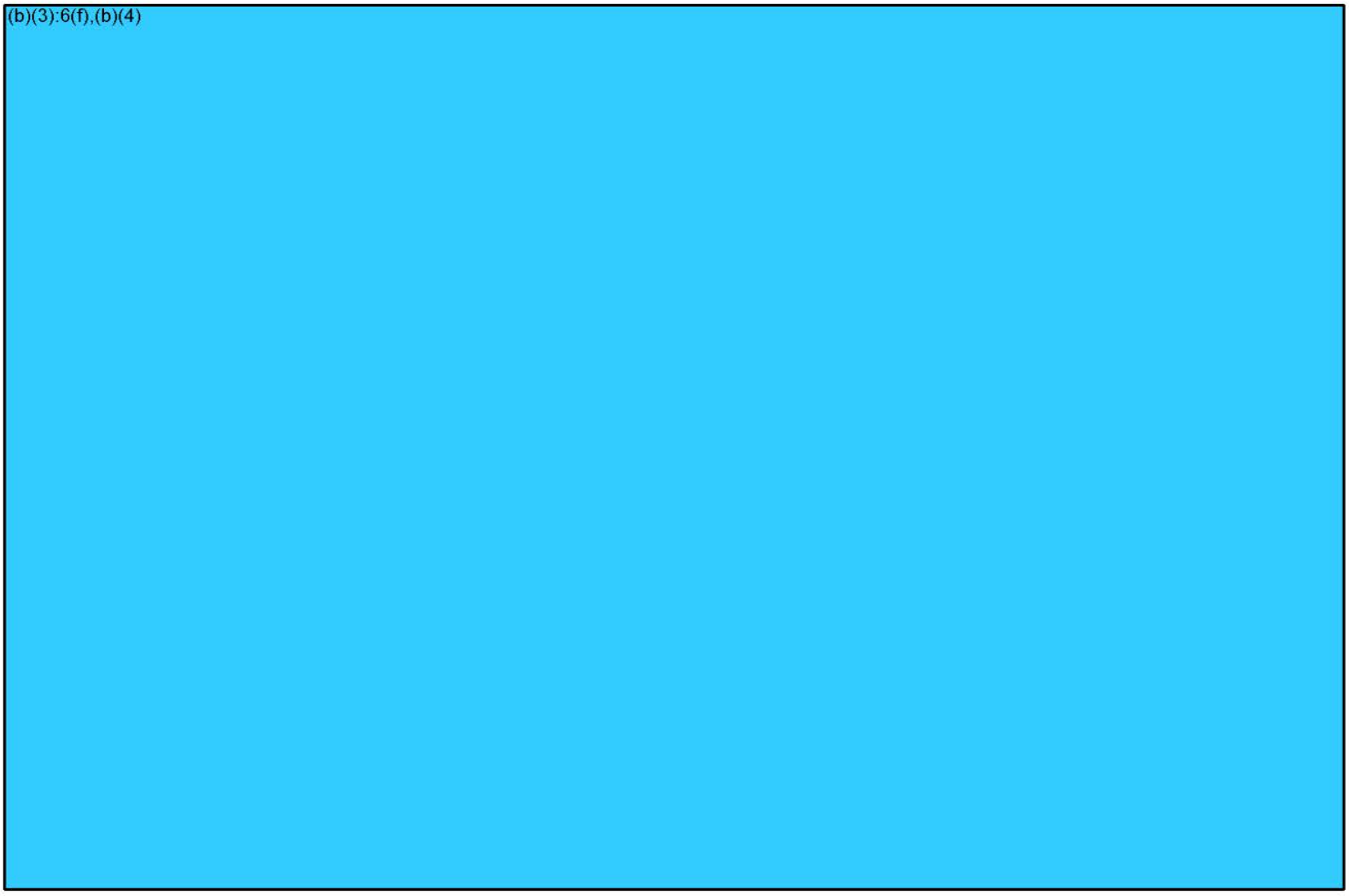

(b)(3):6(f),(b)(4)

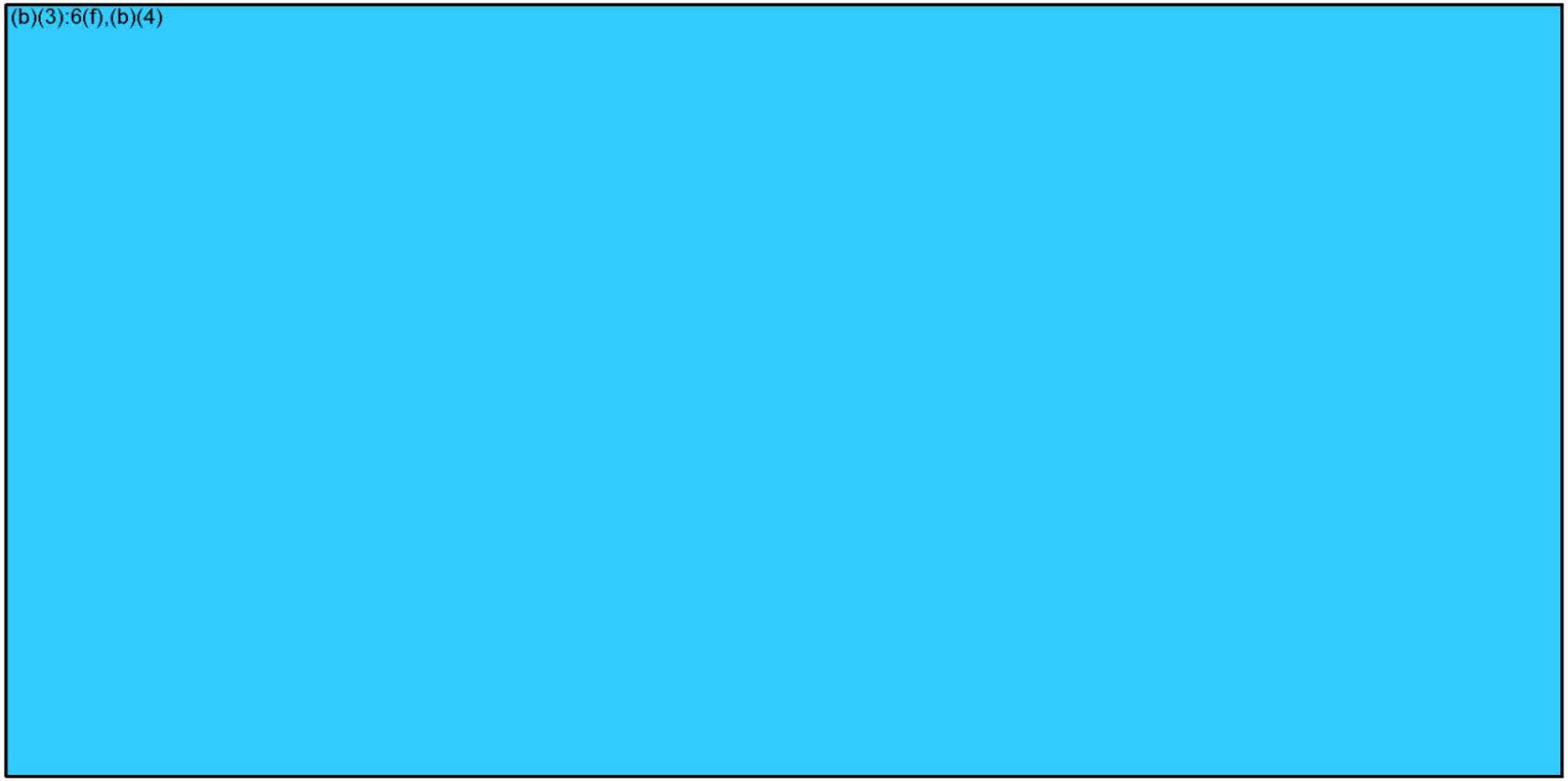
pwc

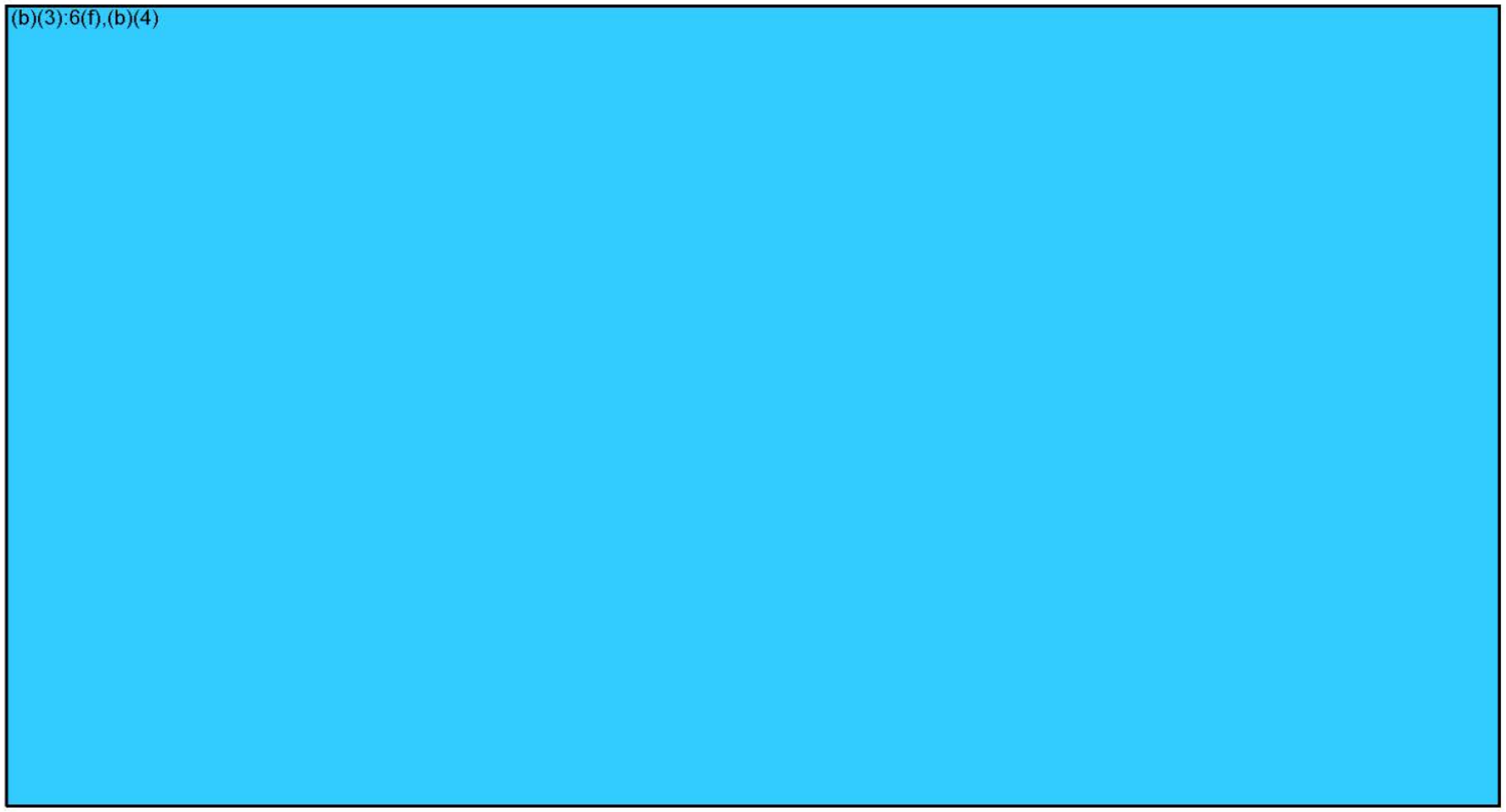


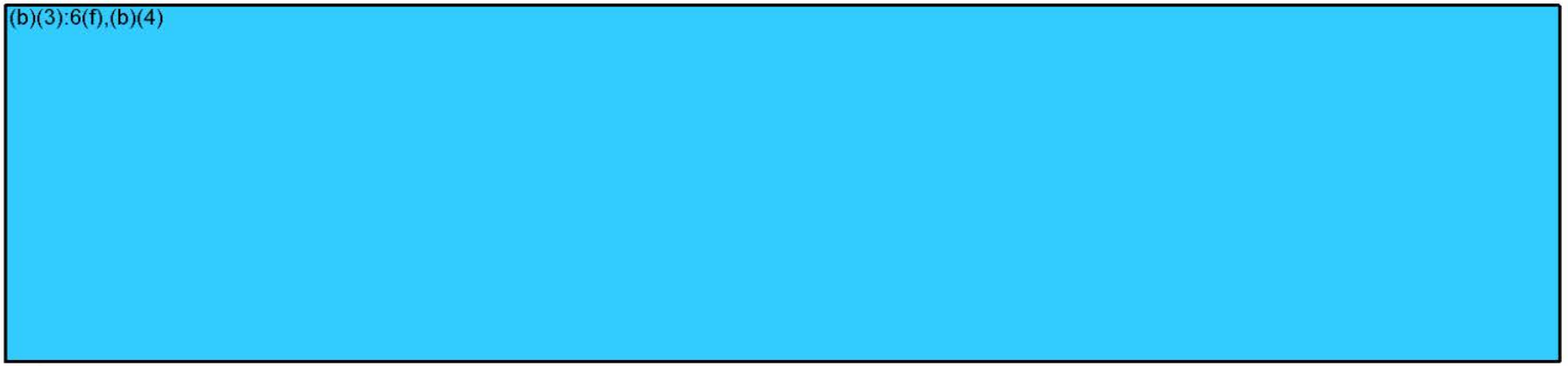

(b)(3):6(f),(b)(4)

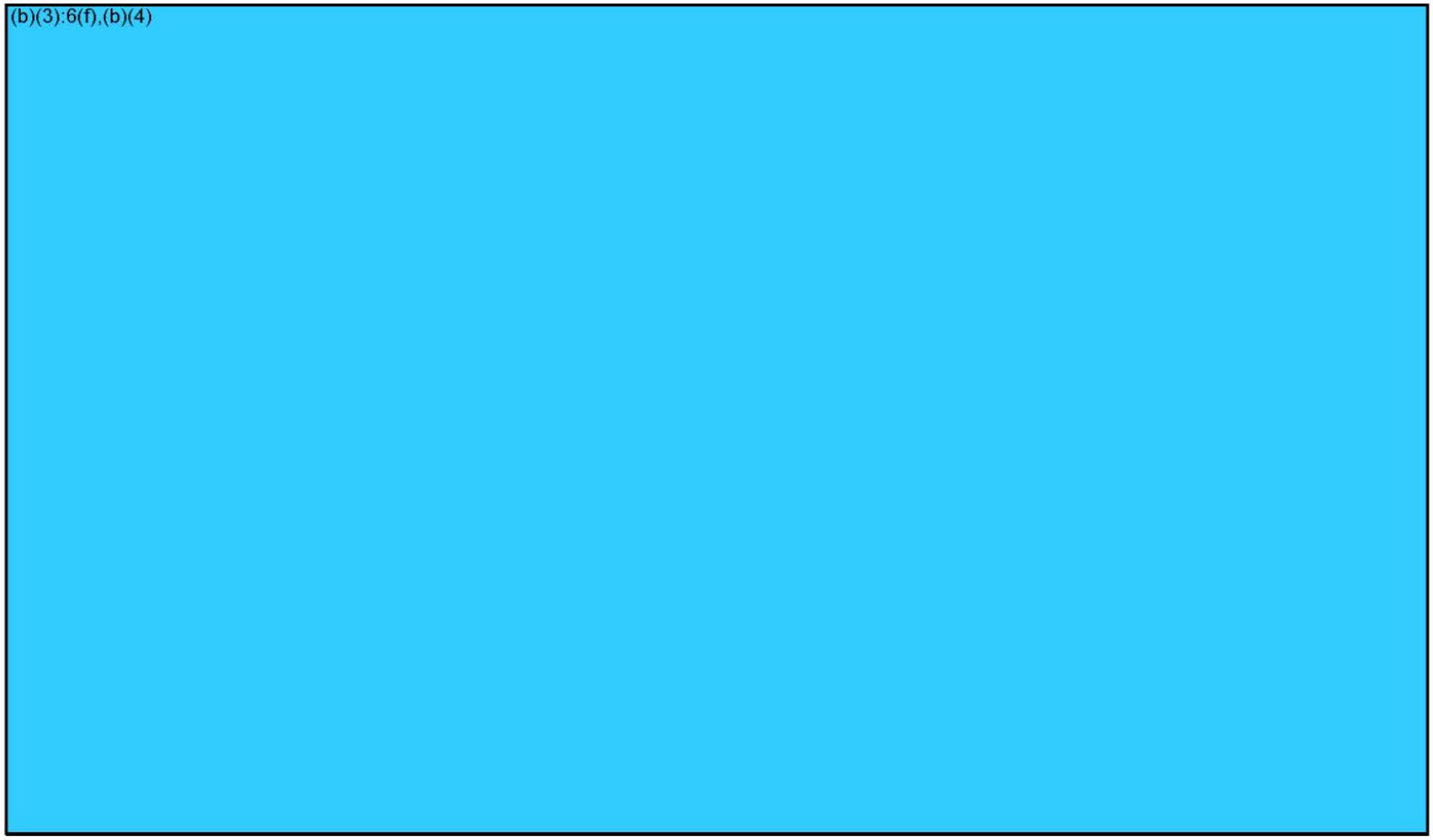

(b)(3):6(f),(b)(4)

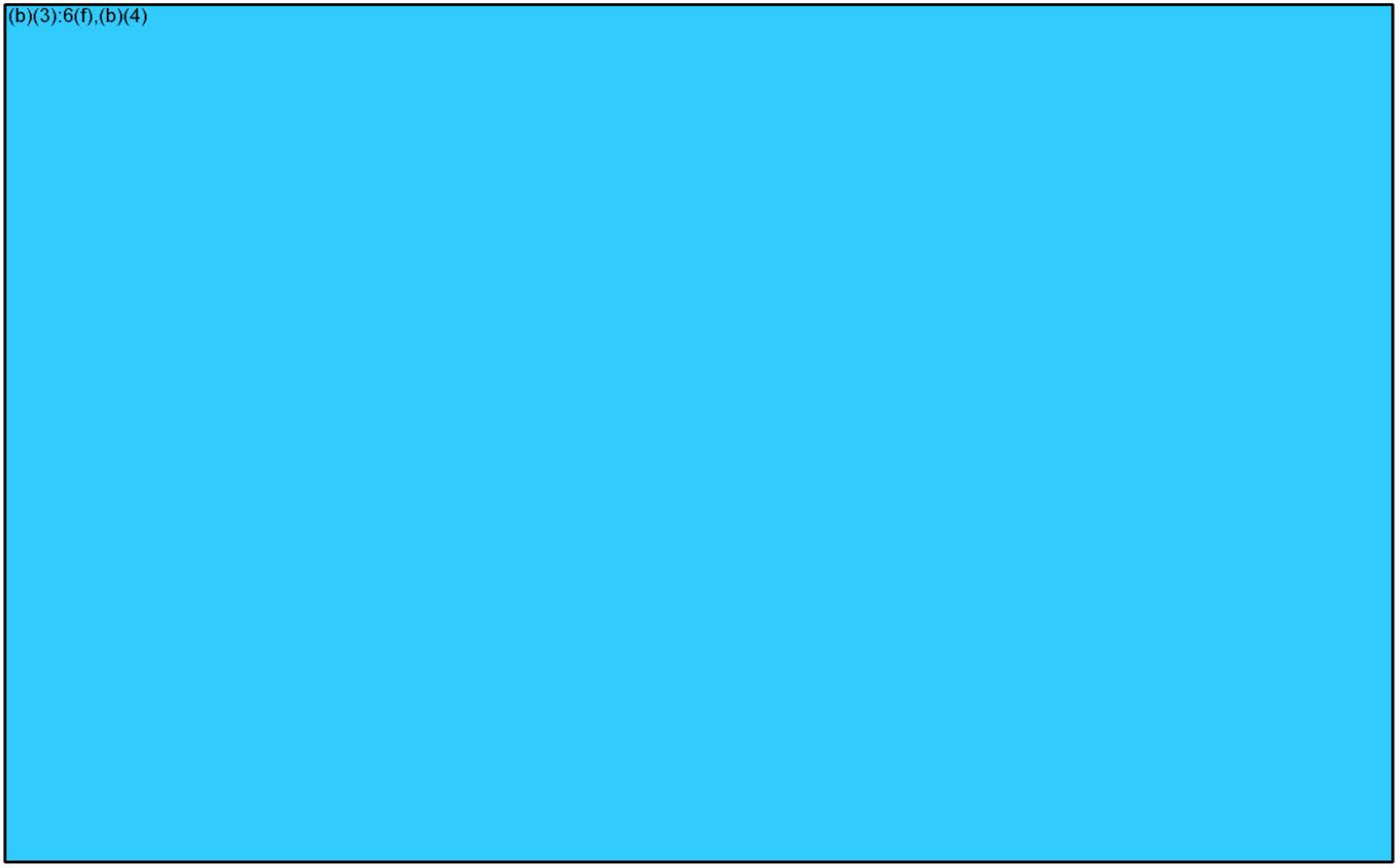

(b)(3):6(f),(b)(4)

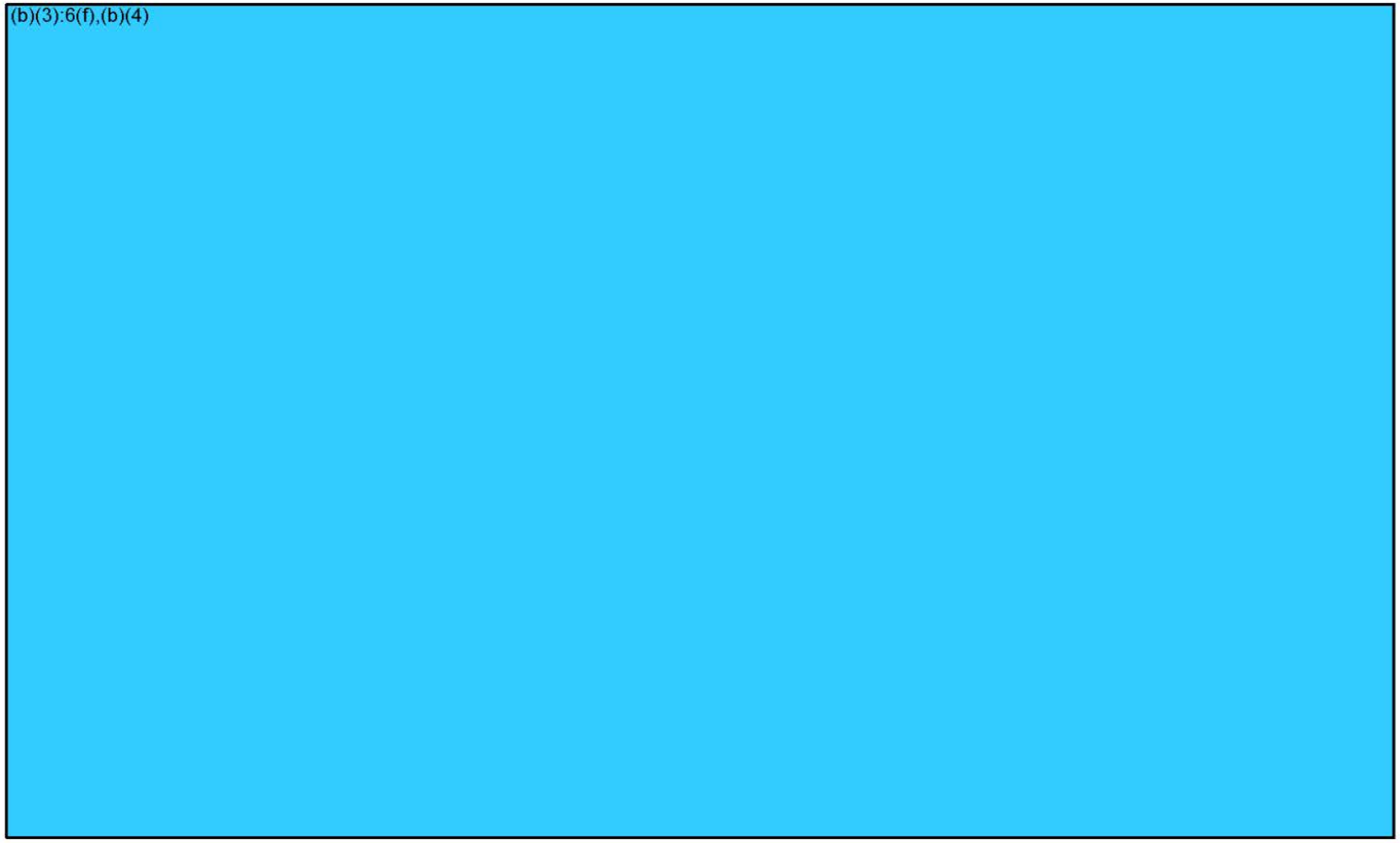

(b)(3):6(f),(b)(4)


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

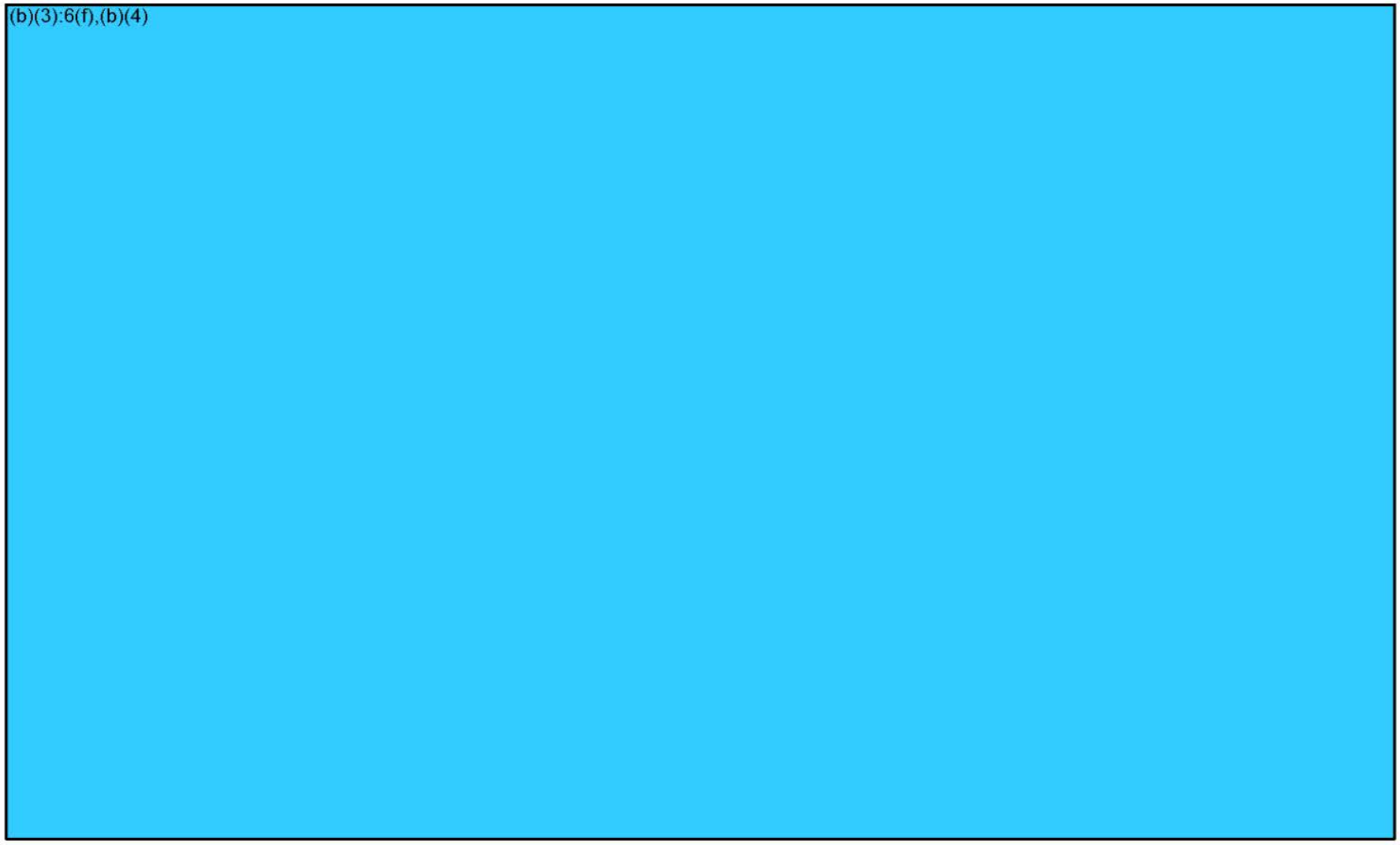

(b)(3):6(f),(b)(4)

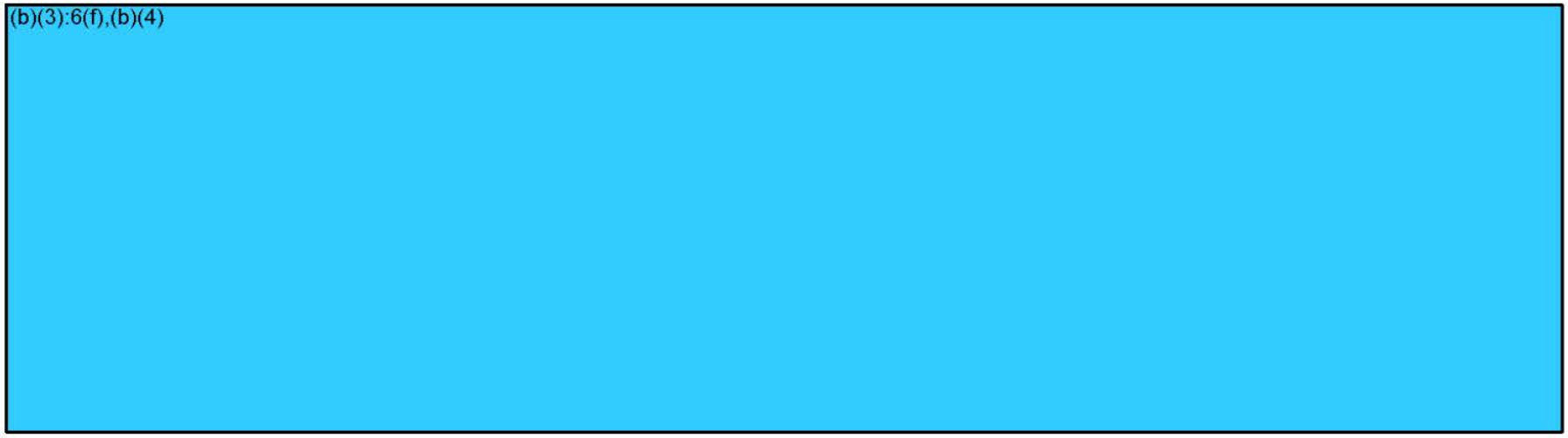

(b)(3):6(f),(b)(4)


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


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

pwc




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

facebook

Management's Assertion

The management of Facebook represents that for the two years ended February 11, 2017 ("the Reporting Period"), in accordance with Parts IV and V of the Agreement Containing Consent Order ("The Order"), with a service date of August 15, 2012, between Facebook, Inc. ("the Company") and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Privacy Program ("the Facebook Privacy Program"), based on Company specific criteria (described in paragraph two of this assertion); and the privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period. (b)(3):6(f)

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

The company specific criteria ("assertions") used as the basis for Facebook's Privacy Program are described below. The below assertions have corresponding controls on pages 22-51.

Assertion A - Responsibility for the Facebook Privacy Program, which is "Facebook has designated an employee or employees to coordinate and be responsible for the privacy program."

Assertion B - Privacy Risk Assessment, which is "Facebook has identified reasonably foreseeable, material risks, both internal and external, that could result in Facebook's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. This privacy risk assessment includes consideration of risks in areas of relevant operations, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research."

Assertion C - Privacy and Security Awareness, which is "Facebook has a privacy and security awareness program in place which is defined and documented in privacy and security for privacy policies. The extent of communications to employees is based on their role and responsibility and may include internal communications through various channels and training."

Assertion D – Transparency, Consent, Access, Use, and Deletion, which is "Facebook provides notices and other informational materials about its privacy policies and procedures, and about its terms of service. These materials explain the purposes for which covered information is collected, used, and deleted and describe the choices available to users.

Facebook obtains consent for such practices. Facebook has implemented controls, including a Privacy Cross-Functional ("XFN") process, to ensure that it only collects and uses covered information for the purposes identified in the notices and provides users with access to their covered information for review and update. Facebook retains covered information for as long as necessary to provide services or fulfil the stated purposes, or as required by law or regulations, and thereafter appropriately disposes of such information."

Assertion E - Security for Privacy, which is "Facebook protects covered information of users against unauthorized access."

Assertion F - Third-Party Developers, which is "Facebook discloses covered information to third-party developers only for the purposes identified in the notices and with the implicit or explicit consent of the individual."

Assertion G - Service Providers, which is "Facebook has developed and used reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from the Company and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information."

Assertion H - Ongoing Monitoring of the Privacy Program, which is "Facebook evaluates and adjusts the Company's privacy program in light of the results of monitoring activities, any material changes to the Company's operations or business arrangements, or any other circumstances that the Company knows or has reason to know may have a material impact on the effectiveness of its privacy program."

Furthermore, the Company represents that for the Reporting Period, Facebook's Privacy Program contains controls and procedures appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the covered information.

Facebook, Inc.

By: _____

Edward Palmieri

Director and Associate General Counsel, Privacy

Facebook, Inc.

1601 Willow Road, Menlo Park, California 94025
650.543.4800 – tel 650.543.4801 – fax

Appendix A – Assessment Interviews Summary

The primary Facebook individuals interviewed by PwC, as a part of the above Assessment procedures, include, but are not limited to, those individuals listed in the table below.

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