

Certain personal details from this document have been redacted for reasons of data protection.

# Facebook's Policy Advisory Opinion Request: Sharing Private Residential Information

<b>1. Issue Statement</b>	<b>2</b>
<b>2. Policy Advisory Opinion Request</b>	<b>2</b>
<b>3. Status Quo Policy Summary</b>	<b>2</b>
<b>4. Examples of Content Enforcement Based on the Status Quo Policy</b>	<b>4</b>
<b>5. Research</b>	<b>7</b>
<b>6. Human Rights Assessment</b>	<b>8</b>

## 1. Issue Statement

Access to residential addresses can be an important tool for journalism, civic activism, and other public discourse. Sharing such information has been used to raise awareness as part of campaigns to challenge disputed social and political issues. However, exposing this information without consent can also create a risk to residents' safety and infringe on an individual's privacy.

## 2. Policy Advisory Opinion Request

Facebook requests the Oversight Board's guidance on the following question related to its Privacy Violations and Image Privacy Rights policy:

Facebook does not allow users to post certain private information. See Community Standards, Section 11. In addition to the specific categories of private information that are described in the Community Standards, Facebook has internal guidance on how to determine whether information is private or has become publicly available and should no longer be removed. In this Policy Advisory Opinion Request, Facebook is asking for guidance on the following:

1. What information sources should render private information "publicly available"? (for instance, should we factor into our decision whether an image of a residence was already published by another publication?)
2. Should sources be excluded when they are not easily accessible or trustworthy (such as data aggregator websites, the dark web, or public records that cannot be digitally accessed from a remote location)?
3. If some sources should be excluded, how should Facebook determine the type of sources that won't be considered in making private information "publicly available"?
4. If an individual's private information is simultaneously posted to multiple places, including Facebook, should Facebook continue to treat it as private information or treat it as publicly available information?
5. Should Facebook remove personal information despite its public availability, for example in news media, government records, or the dark web? That is, does the availability on Facebook of publicly available but personal information create a heightened safety risk that compels Facebook to remove the information, which may include removing news articles that publish such information or individual posts of publicly available government records?

## 3. Status Quo Policy Summary

### **Privacy Violations and Image Privacy Rights Policy Rationale:**

Privacy and the protection of personal information are fundamentally important values for Facebook. Facebook works hard to safeguard personal identity and information in order to

protect people from potential physical or financial harm. Facebook does not allow people to post personal or confidential information about themselves or others.

Facebook removes content that shares, offers or solicits personally identifiable information or other private information that could lead to physical or financial harm, including financial, residential, and medical information, as well as private information obtained from illegal sources.

Facebook also provides people ways to report imagery that they believe to be in violation of their privacy rights.

See Community Standards, Section 11.

**Excerpt from Facebook’s Privacy Violations and Image Privacy Rights policy:**

Do not post:

Content that shares or solicits any of the following private information, either on Facebook or through external links:


Personally identifiable information about yourself or others: ...

- Personal contact information of others such as phone numbers, addresses and email addresses

Imagery that display the external view of private residences if all of the following conditions apply:

- The residence is a single-family home, or the resident's unit number is identified in the image/caption
- The city/neighborhood or GPS pins (for example, a pin from Google Maps) are identified
- The content identifies the resident(s)
- That same resident objects to the exposure of their private residence or there is context of organizing protests against the resident (this does not include embassies that also serve as residences)

Community Standards, Section 11.

  
In order to aid in the Oversight Board’s consideration of Facebook’s Policy Advisory Opinion Request, Facebook provides an excerpt of its Known Questions. Facebook’s Known Questions are used to provide definitions, guidance, and instruction to content reviewers when assessing potential violations of the Community Standards. Facebook regularly reviews and updates the Known Questions resource and is currently undergoing an audit of all Known Questions.

**Excerpt from Facebook’s Known Questions:**

What do we mean by ‘Publicly available’ information?

- We want to protect users' private information. If their information is easily found elsewhere online or has been published through some media, it is no longer private information. For example:
  - Information published through legitimate news source or publications:
    - If the person or their company has publicly posted the content himself or herself somewhere online, we no longer consider it private info
    - If a phone number or email address belongs to an entire office or company (info@facebook.com), it is not considered private info.
  - Information shared by organizations related to their own organization or business:
    - Financial records or statements issued/shared by companies
  - Information shared by individuals related to their own private information
  - Information is searchable through local search engines
  - Documents of public record:
    - We do not protect information that is a matter of public record or intentionally becomes so via legal proceedings.
    - Example: Court files, including but not limited to case indexes, tax liens and judgements, bankruptcy files, criminal arrests and conviction records, warrants, and civil court recording.
    - Printed documents or electronic versions of records shared by government, law enforcement agencies or media with regard to a specific topic that requires PII. Examples of official records or public statements:
      - Property tax assessor files
      - Professional and business licenses
  - *Note: Private information does not become publicly available simply because one person has posted it in more than one location. For instance, if the person sharing the information on Facebook has also created a website to share that info, we do not consider it publicly available.*

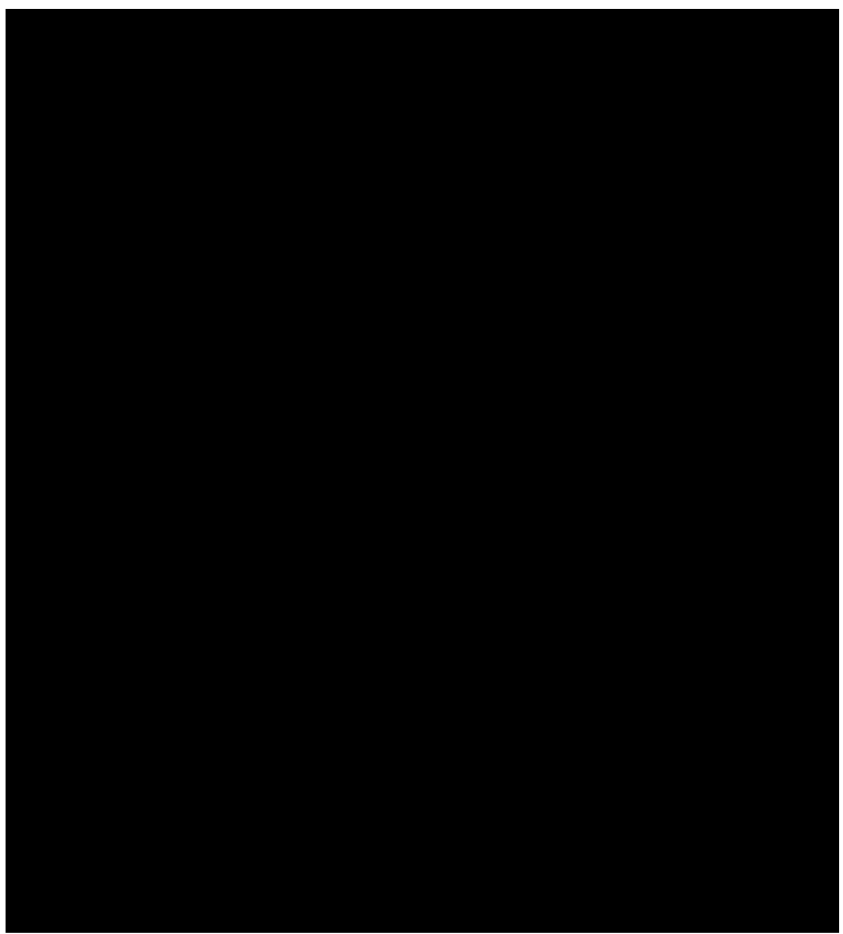
Allow: Documents/information or media reports that include personally identifiable information that is already publicly available through legitimate sources such as official records or public statements.



#### 4. Examples of Content Enforcement Based on the Status Quo Policy



**Example 1** [REDACTED]



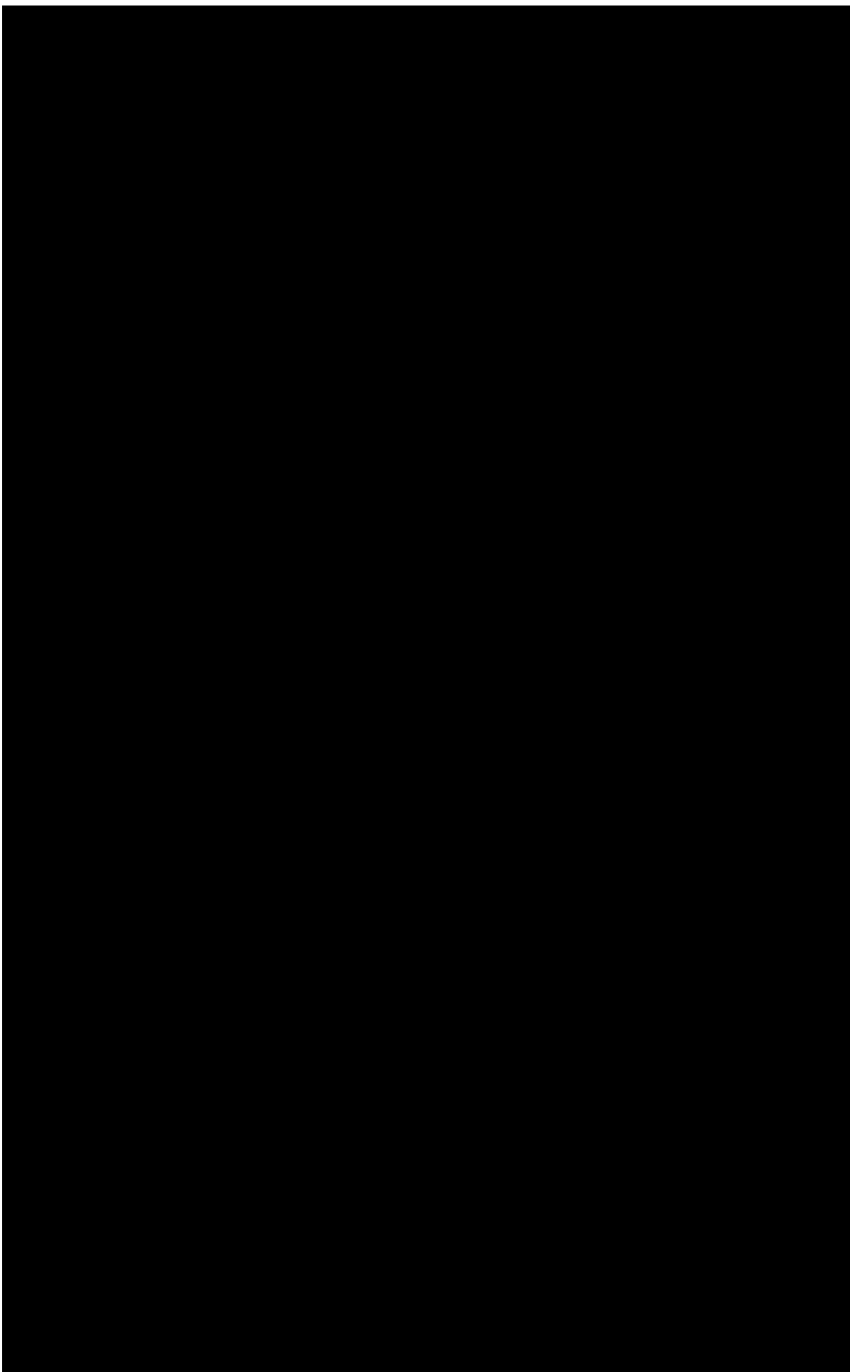


**Description:**

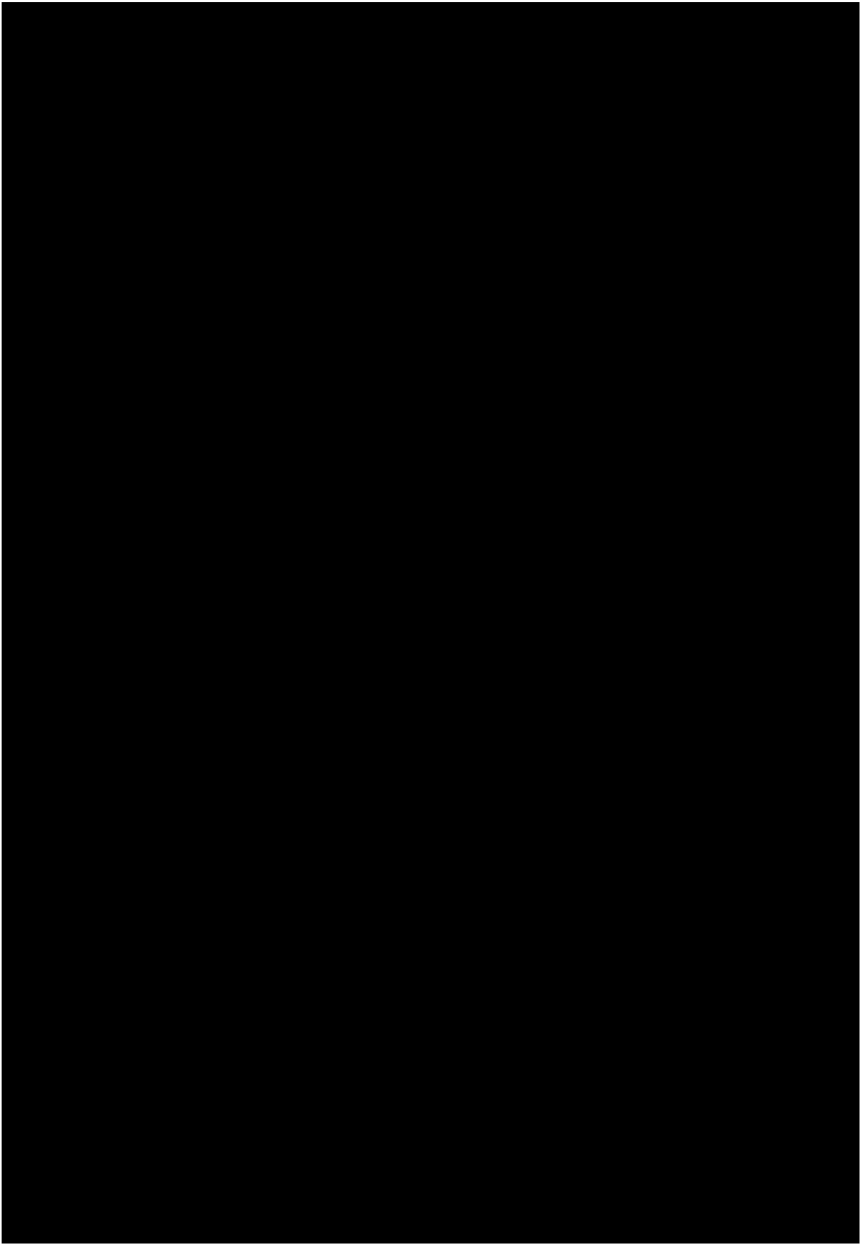
This example relates to a video filmed outside of a politician's home.

**Example 2:** [REDACTED]

**Description:**

This example relates to a post referring to a protest at the home address of a politician.

	
<b>Example 3:</b> 	<b>Description:</b>

	<p>This example relates to a post linking to an article disclosing the home address of an elected official.</p>
---	---



## 5. Research

To help inform the Oversight Board's policy advisory opinion, Facebook's internal research team reviewed a range of external research regarding potential harms associated with the disclosure of personal information, such as residential information. As part of Facebook's standard policy development process, Facebook relies on similar research to inform its



consideration of potential changes to the Community Standards.

## Research Summary

1. The disclosure of private information, such as a residential address, can be associated with a variety of offline harms.
2. Social media companies currently adopt policies similar to Facebook's status quo, but apply distinct rationales for permitting disclosures.

## Research Detail

The process of releasing personal information without consent—including residential addresses—is sometimes referred to as “doxing” (because it refers to the [release of documents](#), abbreviated as “dox”). Evidence from a quantitative analysis of [doxing incidents](#) suggests that “justice” and “revenge” are common motivations for doxing behavior. Experiencing doxing can lead to a range of [negative consequences](#), including [swatting](#) (a wrong-premises SWAT raid), being targeted for [harassment or stalking](#) (which may not have effective legal remedies), and other [kinds of harm](#).

One form of doxing involves the sharing of residential information. In the U.S., the degree to which residential address information is publicly available varies by state. For example, administrative data such as [voter files](#) provide a [public list](#) of all registered voters and, in most states, their home addresses. This kind of administrative information has been used for doxing in other contexts. For example, in Hong Kong, [a court ruled](#) that voter lists that were previously publicly available could be restricted to prevent [involuntary disclosures](#) targeting police officers.

Social media peers have adopted similar policy lines, though the degree to which they condition rules in this domain on public availability or public interest varies. On [Twitter](#), doxing rules address the sharing of residential addresses: users typically cannot share the “home address or physical location information, including street addresses, GPS coordinates or other identifying information related to locations that are considered private” without consent, unless it is publicly available and shared in a “non abusive manner.” [YouTube](#) also requires consent unless the information is *widely* publicly available. [TikTok](#) similarly prohibits sharing users' residential addresses without consent, while [Reddit](#) and [Snap](#) prohibit the unwanted disclosure of personal information in general. By contrast, [Google](#) prohibits the disclosure of personal contact information unless it is in the public interest (defined as professional contact information shared in the context of allegations of professional wrongdoing such as fraud; government records; criminal conduct; or content pertaining to topics such as active civic participation and public officials).

## 6. Human Rights Assessment

To help inform the Oversight Board's policy advisory opinion, Facebook's internal human rights team has provided information relevant to human rights that may be impacted by enforcement decisions made based on Facebook's current policy or based on possible changes to its policy. As part of Facebook's standard policy development process, Facebook

relies on similar assessments to inform its consideration of potential changes to the Community Standards.

The public disclosure of private information happens for many reasons. There may be inadvertent gaffes, poor editing practices, or different cultural expectations of privacy. As discussed above, public disclosure of private information is also (and perhaps most frequently) an adversarial tactic, such as “doxing,” which is used to harass, threaten, silence, or inconvenience others.

Doxing is a frequent but severe breach of the right to privacy as defined in Article 17 of the ICCPR, which provides no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence.

In particular, two highly relevant paragraphs of the [annual UN General Assembly resolution](#) on privacy state:

*Recognizing* that the promotion of and respect for the right to privacy are important to the prevention of violence, including gender-based violence, abuse and sexual harassment, in particular against women and children, as well as any form of discrimination, which can occur in digital and online spaces and includes cyberbullying and cyberstalking. . .

and

*Reaffirming* the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, and recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society.

[Human rights experts and advocates, as well as tech experts](#), indicate doxing and other online harassment strategies disproportionately impact women and girls, as well as other vulnerable users or users facing intersectional [vulnerabilities](#).

The real world disproportionate harassment of women and girls online means that even female politicians and political leaders are frequently targeted by, and grossly disproportionately impacted by, online harassment.

Guiding Principle 17 of the [Gender lens on the UNGPs](#) states:

Business enterprises should always regard sexual harassment and gender-based violence as risks of severe human rights impacts. They should have zero tolerance for such impacts throughout their operations.

Facebook welcomes the Oversight Board's guidance on how the company should define the standard of a "public record" when defining a policy violation, focused perhaps on the difference between government-mandated or verified information about certain citizens or all citizens, and the information shared or brokered by media outlets, paid providers, the dark web, or others. Facebook believes all human rights analysis, guidance, and reasoning indicates a narrow definition is the most proportionate and rights-respecting response.

Facebook asks that, in undertaking its consideration, that the Oversight Board keep cognizant of the fact that the mere imagery of a location or residence may in fact be as revealing as exact written address details - these are often only a few keystrokes away.