Facebook Privacy Policy

BDA 630: Legal & Ethical issues Affecting Big Data

Presented by:
Sahil Patel
Drashti Khatra

OVERVIEW

We'll be exploring Facebook's data practices, critically examining its Privacy Policy, Cookie Policy, and Terms of Service.

Scope: We will delve into Facebook's data collection methods, the purposes for which data is used, how data is shared, user rights and controls, data retention and deletion policies, and relevant legal frameworks (GDPR, CPRA).

Analytical Approach: We will employ a skeptical review, focusing on potential privacy issues, ambiguous language, and areas where the policies may fall short of established privacy principles and regulatory requirements.

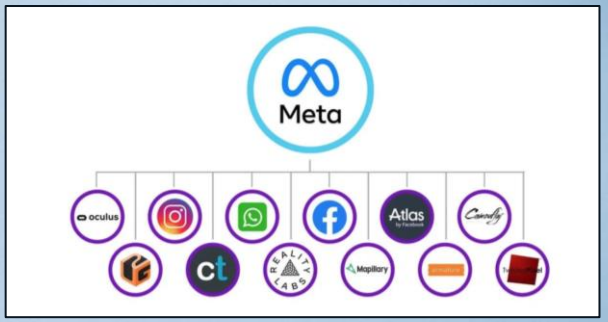
Objective: The goal is to provide a comprehensive understanding of Facebook's data practices and their implications for user privacy.

FACEBOOK(META) PRODUCTS

Meta **updated** their Privacy Policy on November 14, 2024.

The Policy describes the information that **Meta Platforms, Inc.**, process to provide **Meta Products** which includes:

- Facebook
- Messenger
- Instagram, including apps such as Threads and Boomerang
- Meta Platforms Technologies Products such as Meta Horizon Worlds or Meta Quest
- Meta Portal-branded devices
- Business products, such as ads, Meta Business Tools and Meta Business Suite
- Meta Audience Network
- Meta's commerce services platforms, features and products, including Meta checkout experiences and Meta Pay
- Meta Avatars
- Other features, apps, technologies, software or services offered by Meta Platforms, Inc. or Meta Platforms Ireland Limited.



FACEBOOK'S DATA COLLECTION: WHAT THEY SAY THEY COLLECT

"YOUR ACTIVITY AND INFORMATION THAT YOU PROVIDE"

Content: Posts, comments, audio, photos, videos. **Camera/Voice Data**: How you use these features, including information for applying masks/filters. **Messages**: Content (except end-to-end encrypted unless reported), metadata (time, date, type). **Commerce**: Purchase details, payment information. **Interactions:** Hashtags used, ads interacted with, apps and features used. **Sensitive Info**: Religious views, political opinions, health information (with "special protections").

"FRIENDS, FOLLOWERS AND OTHER CONNECTIONS"

Your connections: Friends, followers, groups, Pages you interact with. **Your contacts:** Names, emails, phone numbers (if you choose to upload/sync). **Inferences from others' activity:** Used for friend suggestions and group recommendations.

"APP, BROWSER AND DEVICE INFORMATION"

Your Devices: Type, operating system, hardware/software, identifiers (device IDs, Family Device IDs), signals (GPS, Bluetooth). **Your Usage:** What you do on your device (active app, mouse movements), device settings (location, camera access). **Your Network:** IP address (even when location services are off), connection details. **Performance:** How Meta products function on your device.

"INFORMATION FROM PARTNERS, VENDORS AND OTHER THIRD PARTIES"

Partners: Businesses using Meta's tools, including email addresses, cookies, and ad IDs. **Measurement Vendors:** Analyzing ad performance. **Marketing Vendors:** Supporting marketing campaigns. **Other Third Parties:** Including publicly available sources, industry peers, content providers, and law enforcement.

"INFORMATION FROM COOKIES AND SIMILAR TECHNOLOGIES"

Cookies: Stored on your browser or device. **Meta Pixel:** Tracking your activity across websites. **Social Plugins:** Integrating Meta features into other platforms. **Other Technologies:** Identifiers and software associated with your device.

META'S DATA COLLECTION: FIVE KEY CONCERNS

1. "YOUR ACTIVITY"

A Black Box of Implicit Collection: Meta's definition of "Your Activity" is overly broad ("all the things you can do"). While they mention explicit activities (posting, messaging, searching), the vagueness opens the door to collecting implicit data like mouse movements, scroll speed, and time spent on features without explicit user knowledge or consent, raising GDPR transparency and CCPA/CPRA notice (1798.100) issues.

2. " DATA FROM THIRD PARTIES "

A Transparency Breakdown: Meta receives data from "partners," "vendors," "third parties," and cookies. The policy lacks transparency about who these entities are, what specific data they share, and the purposes of using this data. This raises GDPR and CCPA/CPRA (1798.100) concerns about user awareness and control over third-party data sharing. Data security risks associated with these transfers are also not adequately addressed.

3. " LOCATION DATA"

Always On? Meta collects location data even when location services are off, using IP addresses and Wi-Fi information. While they claim this is for "personalized experiences" and "safety and security," the policy doesn't justify the necessity or proportionality (GDPR Article 5) of continuous location tracking, raising concerns about user surveillance and potential chilling effects on free expression.

4. "DATA COLLECTED WITHOUT ACCOUNTS"

The Ghost in the Machine: Meta tracks non-users through browser/app logs, basic device info, and cookies from third-party sites using Meta's tools. This raises questions about the legitimacy of collecting data from individuals who haven't actively engaged with their services, the challenges of obtaining valid consent (GDPR), and the ethical implications of tracking non-users.

5. "SENSITIVE DATA":

Are "Special Protections" Sufficient? Meta collects sensitive personal data (health, religion, political views), promising "special protections." The policy fails to detail what these protections are. GDPR requires explicit consent for processing sensitive data (Article 9), and CCPA/CPRA provides a right to limit use (1798.121). The policy's language suggests a lower standard than required by law.

HOW FACEBOOK CLAIMS TO USE YOUR DATA

Meta's Privacy Policy states, "We use information we collect to..." :

1. **Provide, personalize, and improve Meta Products:** This includes personalizing features and content (like your Facebook Feed), making suggestions (friends, groups, topics), and developing new products.

2. **Show ads and other sponsored or commercial content**: Meta uses your information to target ads and show you commercial content they believe is relevant to you.

3. **Promote safety, security, and integrity:** This encompasses verifying accounts, investigating suspicious activity, preventing harmful behavior, and protecting Meta's services and users.

4. **Provide measurement, analytics, and business services:** Meta provides data to help partners understand how people use their products and services, measure the effectiveness of ads and content, and understand audience demographics.

5. **Communicate with you:** Meta uses your information to send you messages about their products, services, research, policies, and to respond to your inquiries.

6. **Research and innovate for social good:** Meta uses information for research on topics like social welfare, technological advancement, public interest, health, and well-being.

1. "PERSONALIZING YOUR EXPERIENCE": TOO VAGUE, TOO BROAD?

Meta's Privacy Policy states they use your information to **"provide a personalized experience to you, including ads."** This seemingly innocuous phrase, "personalized experience," warrants closer examination.
The policy doesn't explicitly define "personalization." This vagueness is problematic. What exactly constitutes a "personalized experience"? What data is used, and how? Without clear definitions, this broad term could encompass a vast range of data practices.

Examples of "Personalization" in Practice:

1. **Content Recommendations:** Suggesting posts, pages, groups, and products based on your activity, interests, and connections.
2. **Friend Suggestions:** Recommending potential friends based on mutual connections, shared interests, and other factors.
3. **Newsfeed Curation:** Filtering and prioritizing content in your newsfeed based on your inferred interests and interactions.
4. **Targeted Advertising:** Showing you ads based on your demographics, interests, activity, and other data.

Privacy Concerns:

Manipulation and Exploitation: Personalized content can be used to subtly influence your behavior, opinions, and even purchasing decisions, raising ethical concerns about manipulation and exploitation.
Lack of Transparency and Control: The opacity of Meta's personalization algorithms limits user understanding and control over how their data shapes their online experience.

2. TARGETED ADVERTISING: INSIDE THE MACHINE

Meta's targeted advertising system is a complex machinery fueled by user data that we discussed earlier. Meta's advertising system relies on algorithms and tracking technologies:

Algorithms: These algorithms determine the "most relevant" ads by considering factors like ad quality, advertiser's desired audience, your likelihood of reacting to the ad, and your activity on Meta Products. The lack of transparency about how these algorithms work is concerning.

Tracking Technologies (Cookie Policy): Meta uses cookies (like the "fr" cookie, Cookie Policy, used for "deliver, measure, and improve the relevancy of ads") and the Meta Pixel to track your activity across websites and apps, feeding data into their ad targeting system. This allows for cross-context behavioral advertising.

User Control:

Meta offers some control over ad targeting through "ad preferences" such as:

- See why they're seeing a particular ad.
- Control the use of data collected by Meta for ad targeting.
- Manage settings related to the Meta Audience Network.
- Control whether data from third-party partners is used for ad targeting.

However, these controls are *limited:*

- Opt-out mechanisms are not always clear or easy to use. The language around opting out of "this type of use" for off-Meta ads is vague.
- Opting out of personalized ads doesn't stop data collection. Meta continues to collect your data, even if you opt-out of targeted advertising.
- Managing ad preferences is complex and time-consuming. Users are burdened with navigating intricate settings across multiple platforms.
- The "fr" cookie (Cookie Policy) has a lifespan of 90 days, meaning tracking continues even if you clear your browser cookies.

3. "SAFETY AND SECURITY": A JUSTIFICATION FOR INVASIVE MONITORING?

Meta's Privacy Policy and Terms of Service (ToS) frequently invoke "safety, security, and integrity" to justify various data practices.
This broad justification can be used to defend a wide range of potentially invasive practices, including:

Content Monitoring: Scanning user posts, messages, and other content for violations of community standards or illegal activity.
Account Restrictions: Suspending or disabling accounts for policy violations , often with limited transparency or due process.
Data Sharing with Law Enforcement: Providing user data to law enforcement in response to legal requests or based on "good faith belief". This can include content, location data, and other sensitive information.

Transparency and Accountability:

Users are not informed about:

- The specific algorithms or technologies used for content monitoring.
- The criteria for account restriction or suspension.
- The types of data shared with law enforcement and under what circumstances.

4. YOUR DATA AS A RESEARCH SUBJECT: ETHICAL CONSIDERATIONS

Meta's Privacy Policy states they use user data for "research and innovate for social good," including analyzing migration patterns, studying election impact, and improving internet access.

Ethical Concerns:

- **Lack of Explicit Informed Consent:** The policy doesn't clearly explain how users are informed about or consent to their data being used for research.
- **Transparency and Control:** The policy lacks transparency about the specific data used for research purposes and the types of research being conducted. Users have limited control over how their data is used in these contexts.
- **Potential for Harm:** Even anonymized data used in research can potentially reveal sensitive information or contribute to unintended harms (e.g., discriminatory outcomes based on biased algorithms).

Meta needs to be more transparent about its research activities, implement stronger anonymization techniques, and provide users with meaningful control over their data being used for research. Mere mention of **“social good" is insufficient** to justify ethically questionable data practices.

5. RESPONDING TO LEGAL REQUESTS: BALANCING OBLIGATIONS AND USER PRIVACY

Meta's Privacy Policy outlines their approach to legal requests for user data. They state they will access, preserve, use, and share information:

- "In response to legal requests, such as search warrants, court orders, production orders or subpoenas."
- "In accordance with applicable law."
- "To promote the safety, security and integrity of Meta Products, users, employees, property and the public."

Transparency:
While the policy mentions the types of legal requests (search warrants, etc.), it lacks transparency about:
The volume and nature of requests received: How many requests does Meta receive from law enforcement and other entities? What types of data are typically requested?

User Notification:
Meta's policy does not guarantee user notification when their data is requested. They state they may notify users **"unless doing so may expose us or others to legal liability"** or interfere with investigations. This lack of transparency and the broad exceptions raise concerns about user control and awareness.

Data Retention:
The policy is vague about data retention for legal purposes. While they mention preserving data for "an extended period of time", they don't provide specific timeframes or criteria for deletion after the legal obligation is fulfilled. This lack of specificity raises GDPR concerns (Articles 5, 13, and 14 – data minimization, purpose limitation, transparency) about potential indefinite data storage.

6. THE ALGORITHM KNOWS: TRANSPARENCY, BIAS, AND USER AUTONOMY

Meta's Privacy Policy reveals the pervasive use of algorithms across its platform for various purposes:

- **Content Ranking:** Algorithms determine what appears in your Facebook Feed, prioritizing certain posts based on factors like your interactions with friends, Pages you follow, and "topics that we think you may be interested in."
- **Ad Targeting:** Algorithms select the "most relevant" ads based on your profile, activity, inferences about your interests, and your likelihood of engaging with an ad.
- **Friend Suggestions**: Algorithms power the "People You May Know" feature, based on mutual connections, shared interests, and other factors.
- **Content Moderation:** Algorithms assist in detecting content that violates community standards. However, "manual review" is also used, raising questions about the consistency and criteria applied.
- **AI Integrations:** Meta uses AI-powered features, and while the policy mentions sharing some user data with third-party providers, it provides minimal transparency on how this data is used within AI systems.

Bias and Discrimination:

The lack of transparency creates a high risk of algorithmic bias and discrimination. Potential examples include:

- Discriminatory Advertising: Ads for housing, employment, or financial services might be targeted based on protected characteristics like race, gender, or age, perpetuating societal inequalities.
- Bias in Content Moderation: Algorithms might disproportionately flag or remove content from certain groups or perspectives, limiting freedom of expression and reinforcing existing power imbalances.
- Reinforcement of Social Biases: Friend suggestions and content recommendations could reinforce existing social biases based on factors like location, ethnicity, or socioeconomic status.

BEYOND THE OBVIOUS: OTHER WAYS META USES YOUR DATA

In addition to the purposes previously discussed, Meta's Privacy Policy and Terms of Service reveal several other ways they utilize user data:

- **Data Analytics and Metrics**: Meta uses aggregated and anonymized user data for various internal analytics and business purposes.
- **Measuring product performance:** Understanding how people use their products (e.g., time spent on different features, frequency of usage).
- **Business intelligence:** Identifying trends, understanding user demographics, and informing product development.
- **Financial reporting:** Meta uses data (page 55, example of complying with accounting obligations) to comply with financial regulations and reporting requirements. This can include data about purchases and transactions.

These "**other purposes"** raise several privacy implications:

- Content monitoring for abuse and misinformation raises concerns about freedom of expression and potential overreach. The lack of transparency about Meta's content moderation algorithms and processes is problematic.

WHO DOES FACEBOOK SHARE YOUR DATA WITH?

Meta's Privacy Policy outlines several categories of data sharing:

- **Sharing on Meta Products:** Your information is shared with other users on Meta platforms based on your chosen audience and privacy settings ("Choosing an audience"). This includes posts, stories, messages, and other content you share. Meta highlights that even with specific audiences, resharing and screenshots by others are possible. Public content is accessible to anyone, on or off Meta's platforms.
- **Sharing with Third Parties:** Meta shares data with various third parties, including advertisers, measurement/marketing vendors , service providers (for infrastructure, customer support), researchers, and law enforcement.
- **Sharing within Meta Companies**: Meta shares data across its family of companies (Facebook, Instagram, WhatsApp, etc.) for purposes like providing features, verifying accounts, and "supporting innovation".

THE THIRD-PARTY DATA ECOSYSTEM: A TRANSPARENCY BREAKDOWN

Let's examine each third-party category:

- **Advertisers:** Meta shares reports with advertisers about user demographics and interests related to ad engagement. They also share information about which ads a user viewed before taking an action (e.g., downloading an app). While the policy states they don't share directly identifying information "unless you give us permission" , the extent of data shared for ad targeting raises privacy concerns.

- **Measurement/Marketing Vendors:** These vendors receive aggregated data on ad performance, user activity (online and in-app), and demographics. The lack of transparency about which specific vendors receive data and the details of their data usage agreements raises accountability concerns.

- **Researchers:** Meta shares data with researchers for studies on various topics. The policy claims user privacy is protected but lacks specifics about anonymization techniques and user consent practices.

- **Law Enforcement:** Data is shared in response to legal requests and for "preventing harm." The policy lacks transparency regarding the volume of requests, specific data shared, and user notification procedures.

- **Other Third Parties:** This includes content providers, service providers (beyond those directly supporting Meta's products), and publicly available sources. The policy lacks detail about the data shared and its purpose.

DATA SHARING WITHIN THE META EMPIRE: PRIVACY IMPLICATIONS

Meta shares data across its companies (Facebook, Instagram, WhatsApp, etc.) for:

- **Features and Integrations:** Enabling functionalities like using your Meta Pay account on WhatsApp or connecting your WhatsApp account with other Meta products.
- **Account Verification and Security:** Sharing data like your name and email address to verify accounts and monitor suspicious activity.
- **"Supporting Innovation" :** Using data (e.g., videos) to train AI systems for object recognition, content creation tools, and developing new features.
- **Lack of Granular Detail:** The policy lacks specifics about what data is shared for each purpose, raising concerns about data minimization (GDPR Article 5).
- **User Control:** While users can manage some connected experiences through Account Center (Privacy Policy), they have limited control over the underlying data sharing between Meta companies.

CROSSING BORDERS: INTERNATIONAL DATA TRANSFERS AND GDPR COMPLIANCE

Meta transfers user data globally to:

- Their infrastructure/data centers: Located in the US, Ireland, Denmark, Sweden, and "amongst others."
- Countries where Meta Products are available.
- Locations of partners, vendors, and service providers.
- Legal Mechanisms: Meta states they rely on "appropriate mechanisms", which includes SCCs (Standard Contractual Clauses), adequacy decisions, and other mechanisms under applicable law.
- GDPR Compliance (Article 44-49): The lack of specificity regarding which mechanism is used for which transfer raises compliance concerns. SCCs have limitations, and relying on them for all transfers might not meet GDPR's adequacy requirements, especially given concerns about US surveillance laws.
- Data Security: Meta claims they use safeguards like encryption for data in transit but provides minimal detail about other security measures.

"INTEGRATED PARTNERS": HIDDEN RISKS AND USER CONTROL?

"Integrated partners" are third-party apps, websites, and services that use technologies to connect with Meta Products (e.g., games using Facebook Login, websites with embedded "Like" buttons).

- **Data Sharing:** Integrated partners receive: Public data, data users choose to share via permissions (including potentially sensitive data), and activity data when interacting with other Meta users through the partner's platform.
- **Risks:** Integrating third-party services increases risks of data leaks, unauthorized access, and misuse of user information.
- **Transparency and User Control:** While Meta provides some control through app and website settings, the initial consent process for data sharing with integrated partners might lack transparency. Users might not fully understand the implications of granting permissions.

DATA SHARING CONTROLS: MANAGING YOUR DATA: THE ILLUSION OF CONTROL?

Meta offers various controls for managing some aspects of data sharing:

Account Settings:

- Privacy Checkup: Guides users through key privacy settings but lacks granular control over data sharing with third parties.
- Ad Preferences: Allows users to manage ad targeting preferences (e.g., interests, advertisers), but doesn't stop data collection for advertising purposes. Control over third-party data used for ad targeting is also limited.
- Off-Facebook Activity: Shows data shared by businesses with Meta but doesn't prevent this sharing from happening in the first place. Provides some control over future sharing by disconnecting activity from your account.
- Apps and Websites: Manages permissions for apps and websites connected to your Facebook account. However, the initial permission process for integrated partners might lack transparency.
- Location Settings: Controls location services for Meta apps but acknowledges ongoing location estimation even when services are off, using IP addresses and connection information.
- Audience Controls for Posts: Allows users to select the audience for their posts (Public, Friends, etc.) but doesn't prevent resharing or screenshots by others. Public content is always accessible.

- **Limitations:** Users have little control over core data sharing practices, such as sharing data within Meta companies, data used for "safety and security" , or data shared with measurement/marketing vendors. Control over data shared with integrated partners is limited after the initial permission grant.

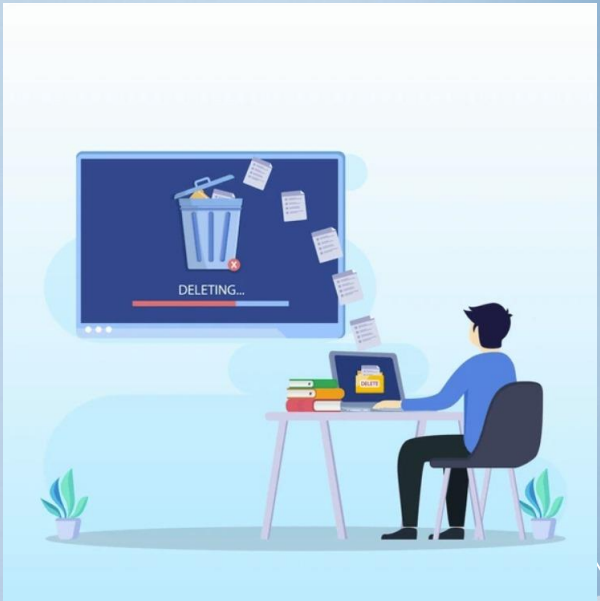
HOW LONG DOES FACEBOOK KEEP YOUR DATA?

- Meta's Privacy Policy states, "We keep information for as long as we need it to provide our products, comply with legal obligations, or to protect our or others' interests." This core policy of retaining data "as long as needed" is central to the concerns about data retention.
- **"As Long as Needed":** A Recipe for Indefinite Data Retention?
- The phrase "as long as needed" is extremely vague.
- **Vagueness:** What constitutes "need"? The policy provides some factors (operating products, legal obligations, protecting interests), but these are broadly interpreted.
- **Lack of Specific Timeframes:** Meta provides no specific retention periods for different data categories. This contrasts sharply with GDPR's requirement (Article 5) for data minimization and purpose limitation, implying data should only be kept for as long as necessary for the specified purpose. CCPA/CPRA's emphasis on data minimization (1798.100(b)) raises similar concerns.
- **Risks:** Indefinite data retention increases the risks of data breaches, misuse, and unauthorized access. The longer data is kept, the greater the vulnerability.

DELETING YOUR DATA: IS IT TRULY GONE?

Meta's data deletion process raises several concerns:

- **Process:** Users can delete specific content (e.g., posts, photos) or permanently delete their entire account.
- **Timelines:** Even after account deletion, data may be retained for up to 90 days, and another 90 days for backups. *"Content you've posted"* may linger even longer if others have interacted with it.
- **Completeness:** Data might be retained indefinitely for legal purposes, safety and integrity, or litigation. This contradicts the idea of complete deletion. Backups further complicate matters, as data might exist in multiple locations.
- **Deactivation vs. Deletion:** Deactivation hides your profile but doesn't delete data. Deletion is intended to be permanent, but with the caveats mentioned above.



THE RIGHT TO BE FORGOTTEN(GDPR): DOES FACEBOOK COMPLY?

GDPR Article 17 grants the *"right to be forgotten"* – the right to have your personal data erased under certain circumstances (e.g., the data is no longer necessary for the purpose it was collected, you withdraw consent).

Facebook's Practices: Meta's long retention periods (up to 90 + 90 days, plus indefinite retention for other purposes) and the potential for residual data conflict with the spirit of the right to be forgotten.

Exceptions (GDPR Article 17(3)): The right to erasure is not absolute. Exceptions exist for freedom of expression, compliance with legal obligations, public interest, scientific/historical research, or legal claims. Meta's reliance on these exceptions, particularly "legal obligations" and "safety and integrity" , warrants further scrutiny to determine if their application is justified and proportionate in each case. Does "safety and integrity" justify indefinite retention of user data?

YOUR DATA RIGHTS: WHAT FACEBOOK SAYS YOU CAN DO

Meta's Privacy Policy outlines these user rights:

Access to your information: You can access and review the information Meta has about you.

Correction of your information: You can request corrections to inaccurate information.

Deletion of your information/account: You can delete specific information or your entire account. Note the limitations discussed later regarding data retention.

Portability of your information: You can request a copy of your data in a portable format.

Object to certain processing (GDPR – Article 21): This right is implied but not explicitly detailed in the policy. It's addressed indirectly through ad preferences and "Off-Facebook Activity" controls.

Withdraw consent (GDPR – Article 7): Similarly, withdrawing consent is not clearly explained, except for managing specific settings and deleting data.

USER RESPONSIBILITIES AND ACCOUNT LIMITATIONS

The ToS(Terms of Services) outlines user responsibilities and account limitations:

Data Privacy Responsibilities: Users are responsible for providing accurate information, not sharing their password, and using their account only for personal purposes.

Account Suspension/Termination: Meta can suspend/terminate accounts for violating ToS or Community Standards. Data may be deleted, but exceptions exist, creating uncertainty about the "right to be forgotten."

Content Removal: Meta can remove content that violates their policies. The process lacks transparency and has implications for freedom of expression.

FACEBOOK'S PRIVACY POLICY: SUMMARY OF KEY CONCERNS

Meta's Privacy Policy, Cookie Policy, and ToS, while using simplified language, raise significant privacy concerns:

Vague Language and Definitions: Broad terms like *"Your Activity," "partners,"* and *"as long as needed"* (for data retention) create ambiguity and provide Meta with excessive discretion.

Extensive Data Collection and Sharing: The scope of data collection, including implicit data, and widespread sharing with third parties and within Meta companies, is alarming.

Limited User Control: Users have limited control over key data practices, and the provided controls are often ineffective or lack transparency.

Inadequate Transparency: Despite some efforts toward simplification, Meta's overall approach lacks granular detail and clarity about specific data practices.

Questionable Compliance: Meta’s data practices raise doubts about full compliance with GDPR and CCPA/CPRA principles of data minimization, purpose limitation, transparency, and user control.

Thank you