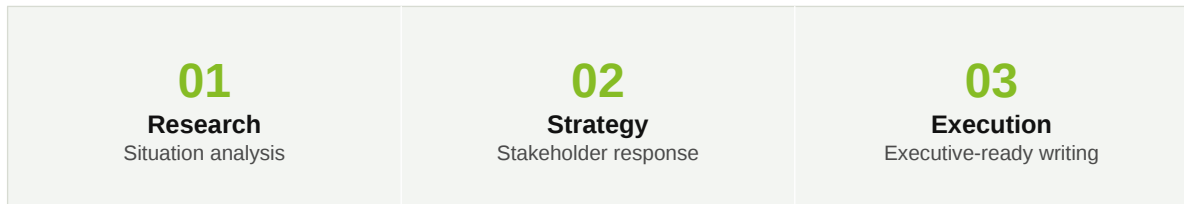


Meta Privacy Crisis

Strategic Communication & Crisis Response Case Study



Prepared by

Bisetsa Bienvenu

Writing samples reframed as professional case studies for communications, PR, marketing, and corporate affairs roles.

Portfolio Map

This document is organized like a consulting deliverable: the business issue first, the analysis second, then recommendations and supporting writing samples.

01 **Executive Summary**
A concise overview of the Meta privacy case and portfolio value.

02 **Situation Analysis**
Identity, reputation, legitimacy, stakeholder pressure, and business risk.

03 **Strategic Recommendations**
Clear actions to rebuild trust and reduce future crisis exposure.

04 **Communication Deliverables**
Executive-ready writing samples and message architecture.

05 **Appendices**
Original academic source documents preserved for reference.

Executive Summary

Objective

Analyze Meta's privacy crisis and recommend communication strategies to rebuild stakeholder trust, improve transparency, and reduce long-term legitimacy risk.

My Role

- Conducted strategic communication research and crisis analysis.
- Mapped major stakeholders including users, regulators, media, investors, and employees.
- Developed recommendations, executive messaging, and reputation repair strategy.
- Translated academic communication theory into practical business recommendations.

Skills Demonstrated

- Crisis communication
- Reputation management
- Strategic communications
- Executive writing
- Research synthesis
- Stakeholder analysis

Outcome

Developed a communication strategy addressing legitimacy, trust, transparency, and corrective action using crisis communication frameworks and organizational reputation analysis.

SECTION

Situation Analysis

Diagnosing the core communication problem before recommending action.

Business Problem

Meta positions itself as a privacy-conscious technology company focused on connection, safety, and innovation. The issue identified in this case study is the gap between that public identity and stakeholder perception after repeated privacy controversies involving user data, AI systems, smart glasses, and third-party contractors.

Communication Diagnosis

- The crisis is broader than a single reputational event; it is a legitimacy issue because stakeholders are questioning whether Meta can responsibly hold its current level of power over personal data.
- The image-identity gap is central: Meta says it values privacy, but stakeholders perceive recurring data practices as inconsistent with that message.
- Transparency is not only about publishing more documents. If users cannot understand the information, visibility increases while real accountability remains low.
- The crisis directly affects the business model because user trust is tied to consent, platform engagement, advertiser confidence, and regulatory permission.

Stakeholder Map

Stakeholder	Concern	Communication Need
Users	Privacy, consent, control over data	Plain-language explanations and stronger privacy controls
Regulators	Compliance, transparency, accountability	Evidence of oversight and corrective action
Media	Public narrative and scandal framing	Clear facts, consistent updates, and named reforms
Investors	Legal exposure and trust erosion	Risk reduction plan tied to operational changes
Employees/Contractors	Data access rules and ethical standards	Training, guardrails, and accountability structure

SECTION

Strategic Recommendations

A practical rebuild strategy focused on trust, accountability, and user control.

Recommendations

Recommendation	Action	Expected Impact
Clearer privacy communication	Rewrite privacy explanations in plain language and create user-facing summaries that explain what data is collected, why it is used, and how users can control it.	Improves credibility and reduces confusion caused by technical language or information overload.
Third-party oversight	Create stricter governance over contractors and vendors, including data-access limits, auditing, and leadership accountability.	Reduces preventable risk and shows stakeholders that corrective action is operational, not only rhetorical.
User data controls	Build stronger settings that let users choose what data they share and understand how those choices affect their experience.	Strengthens perceived control, supports informed consent, and signals user-centered design.

Response Strategy

Because the issue is preventable and tied to organizational responsibility, the recommended response uses a rebuild strategy: acknowledge the harm, apologize clearly, explain corrective action, and show measurable reform. Defensive messaging or generic reassurance would likely deepen mistrust because stakeholders are already skeptical of Meta's privacy claims.

SECTION

Communication Deliverables

Professional writing outputs that hiring managers can evaluate quickly.

Deliverable Set

- Executive memo summarizing the crisis and leadership response priorities.
- Situation analysis identifying the legitimacy gap and stakeholder concerns.
- Strategic recommendations organized by business problem, action, and expected impact.
- Mock public statement explaining the issue, response, and planned corrective measures.
- Presentation materials translating the case into a concise visual briefing.

Employer-Facing Value

This case study demonstrates the ability to turn complex issues into executive-ready communication, diagnose stakeholder risk, and recommend practical actions for reputation repair. It is appropriate for roles in communications, public relations, corporate affairs, social media strategy, and marketing communications.

SECTION

Reflection

What this project shows about my communication approach.

Professional Reflection

This project strengthened my ability to analyze organizational legitimacy, evaluate stakeholder expectations, and build communication strategies grounded in both theory and practical business risk. It also shows my ability to write for multiple audiences: executives, users, media, regulators, and internal stakeholders.

SECTION

Original Supporting Work

The following pages preserve the original uploaded writing samples as appendices.

Appendix Index

Appendix A - Phase 1-Mata.pdf

Appendix B - Phase 3- Crisis or Issue Brief-Mata.pdf

Appendix C - From a strategic communication view-3 recommendations.pdf

Appendix D - Phase 4-Mata.pdf

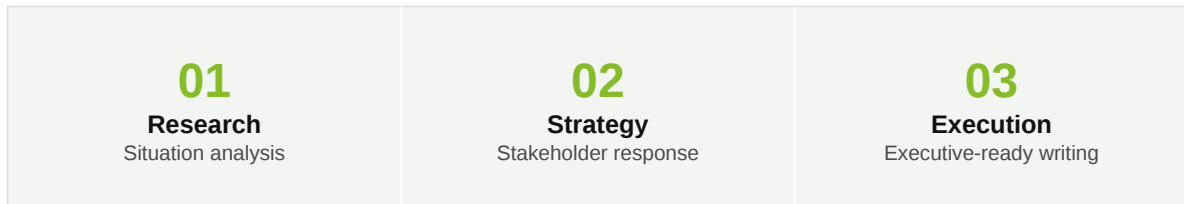
Appendix E - Meta Data Privacy Presentation.pdf

Original PDFs are attached after this divider to preserve the source work while giving employers a polished case study first.

ORIGINAL SUPPORTING WORK

Appendix A

Phase 1-Mata.pdf



Prepared by

Bisetsa Bienvenu

Writing samples reframed as professional case studies for communications, PR, marketing, and corporate affairs roles.

Organization overview:

Meta, formally named Facebook, is a technology conglomerate that includes notable digital platforms such as Facebook, Instagram, WhatsApp, Messenger, and Threads to connect individuals through social networking. The corporation focuses on the development, operation, and innovation of various digital media platforms as well as numerous VR technologies, AI models, and advertisements for businesses.

Why This Organization is interesting for Communication:

The appeal of studying Meta in a course for organizational identity, image, and reputation is because there is a legitimacy issue within the trust and credibility of the organization. Meta claims to protect data and private user information, however there has been evidence of data misuse and privacy breaches. There have been multiple situations of data leaks and of Meta allowing contractors to read users' conversations with AI chat bots. As these breaches and scandals keep happening, a legitimacy issue becomes prevalent. Users are starting to lose trust and the company's ethics are being questioned in the media. This organization also raises interesting communications questions because there is a gap between what the organization says and how it is perceived. Meta has claimed to prioritize user privacy and to protect personal data and information. Despite that, the public actually feels that Meta takes advantage of their data, has no transparency or visibility, and that they care more about money than their users. This gap in trust between Meta and its users has the public questioning intentions behind famous Meta products or platforms.

Early Signal of an Identity, Reputation, or legitimacy issue:

Despite claims of valuing privacy and data safety, Meta has faced multiple lawsuits regarding privacy concerns and data breaches of Meta users. Meta recently faced a multi-year lawsuit where they settled to pay \$50 million in civil penalties. Senior executives, including Mark Zuckerberg, were aware of privacy risks since 2012, but postponed action at the time to protect stock prices. Other lawsuits include major payouts, avoiding trial and public accountability. Meta also claims that their privacy policy standards are imbued into their product development, making sure their users are protected. However, we have yet to see this. They continue to have breaches of privacy that discount these claims. Meta has also had accusations about their contractors reading private sensitive information from users such as private photos, names, email addresses, locations, job information, and all unredacted information. Despite all this opposing evidence, Meta still claims to be protecting people's data through its policies.

Preliminary Sources

Lee, D. (2026, February 16). *Meta is wrong to try to sneak into facial recognition with Ray-Ban glasses. Bloomberg Opinion.* <https://www.bloomberg.com/opinion/articles/2026-02-16/meta-is-wrong-to-try-to-sneak-into-facial-recognition-with-ray-ban-glasses>

Goel, S., & Webb, E. (2025, August 6). *Contractors training Meta's AI say they read intimate talks with its chatbot — and see data that identifies users*. *Business Insider*. <https://www.businessinsider.com/meta-ai-chatbot-privacy-user-names-data-contractors-scale-alignerr-2025-8>

McArthur, V. (2024, September 23). *Meta's AI-powered smart glasses raise concerns about privacy and user data*. *The Conversation*. <https://theconversation.com/metas-ai-powered-smart-glasses-raise-concerns-about-privacy-and-user-data-238191>

Halleman, S. (2022, June 23). *Meta hit with class action suit alleging it mined providers' patient data*. *Healthcare Dive*. <https://www.healthcaredive.com/news/Meta-class-action-suit-mined-patient-data/625943/>

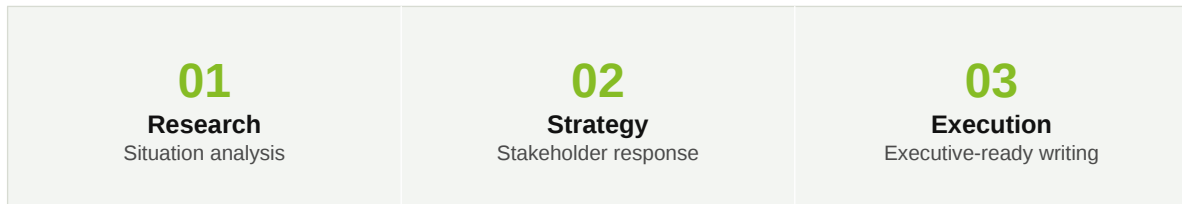
Harbath, K., & Fernekes, C. (2023, March 16). *History of the Cambridge Analytica controversy*. Bipartisan Policy Center. <https://bipartisanpolicy.org/article/cambridge-analytica-controversy/>

Hill, K., Huang, K., & Isaac, M. (2026, February 13). *Meta plans to add facial recognition technology to its smart glasses*. *The New York Times*. <https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html>

ORIGINAL SUPPORTING WORK

Appendix B

Phase 3- Crisis or Issue Brief-Mata.pdf



Prepared by

Bisetsa Bienvenu

Writing samples reframed as professional case studies for communications, PR, marketing, and corporate affairs roles.

The Issue or Crisis

Meta Platforms are currently facing issues with trust and legitimacy, according to Dowling it is different from reputation because it measures if an organization is seen as acceptable enough to operate outside of normal and formal rules and social expectations. Reports say that Meta Platforms have been breaching user privacy by having their Alchats being read by contractors on platforms like WhatsApp and Facebook, contractors also were hired to train their AI based on AI chats, recorded video and audio from their Rayban glasses in Kenya. Although AI training needs human review this recurrence of privacy breach shows a recurring pattern of not trust and legitimacy in the company among users. Even though Meta still claims to protect people's privacy, according to recent reports from [classaction.org](https://www.classaction.org) contractors accessed private conversations and personal information and allowed them to store and read the data that was linked to their Whatsapp account according to the class action lawsuit. These recurring issues about user privacy makes Meta look really untrustworthy, especially when they release reports to the public saying one thing while their actions take another step in the wrong direction. This creates a legitimacy and trust issue among users. The users expect privacy with end to end encryption not a human reviewing their chat logs, Rayban video and audio from the glasses.

The situation is damaging because it goes against all of Meta's core mission statement, principles and overall culture. Over time, when these recurring issues continue to happen it weakens trust within the organizations because you can't trust your employees, trust between shareholders & stakeholders and overall the general public. As a result of having weak trust among the public like Meta users, shareholders and stakeholders the organization's legitimacy can create an identity gap because what they claim to operate on doesn't seem to match up with the organization's identity. This creates tension with how the public sees them vs how they see themselves. For example, Meta promises that they're Rayban is "designed for privacy, controlled by you" yet users feel like they don't have control of their privacy nor data due to the fact that Meta Platforms were handing off their data to contractors and third parties for them to review. This repeated privacy breach also makes the stakeholders begin questioning their trust in the organizations which leads into the organizations identity being questioned and challenged since there is always controversy regarding your users. Current and future investors will fallout because they don't have trust in the organization nor in its legitimacy to the public. Another example that ties in with the legitimacy issue is Meta's leadership within the organization, which is transformational vs the public sees which is laissez-faire. Transformational leadership promotes innovation, and tech that empowers employees and a there's always a shared vision or goal, but it can leave room for human errors to occur like if or when goals are too big or ambitious, like the kanyan contractors, this type of leadership has made the public think Meta's leadership is laissez-faire which is very hands off, relying on trust and

small interventions, delegating and like handing off important work to third parties and such.

This privacy breach situation gained quick attention from external stakeholders like users since it's their data and privacy that's being breached, media since they are amplifying the story even to non Meta users, regulators since data was being handed off to contractors and third parties like in Kenya, investors since they're putting money into the company whether that be ads or space, employees coming out and whistleblowing about how there's a backdoor in WhatsApps allowing others to see users' convos and data. Over time as the attention increased on the privacy breach from Meta products, trust, reputation which is according to Dowling is the stakeholders evaluation of an organization over time based on its past issues and consistency, it has nothing to do with the image but rather trust, legitimacy risk has expanded to a great extent that it has led to multiple class action lawsuits from users against Meta regarding privacy.

This issue shows more than a one time privacy issue but a recurring problem. Over time this recurring pattern in privacy breach among users on Meta Platform will lead to more class action lawsuits which can lead to losing users overtime. If Meta doesn't change how their leadership operates and is viewed then this problem will continue to happen because they can't seem to learn from their mistakes, effective leadership needs to happen so they can truly put the users first instead of chasing profits for the internal 1% shareholders inside that company, if they put the users first, the reputation on legitimacy and trust comes back to the company.

Communication Diagnosis

The main issue that Meta is dealing with is a gap between Meta's organizational identity, or how they view themselves, and their public image, or how the public views them. According to Hatch and Schulz (2002), this gap exists because external audiences are building Meta's image based on repeated privacy scandals. Meta's messaging and communication practices do not have influence on its image because of its constant issues. This issue has been made worse by Meta's poor crisis responses. Internally, Meta claims to be focused on giving their consumers top-notch privacy. On their website, Meta says, "Protecting users' data and privacy is essential to our business and our vision for the future" (Meta, n.d.). Meta outwardly communicates that it is committed to its users and visibility. Despite the identity Meta attempts to align itself with, the public interprets its image as entirely different. The general public perceives Meta as an exploiter of consumer data and as a company that does not care about its users as much as making a profit off of them. In 2023, it was found that 68 percent of American adults do not trust Meta with their data, which indicates growing public concerns regarding recent privacy breaches and other conspicuous scandals regarding user data (Socialeum, 2025). Meta's disconnect between identity and image reflects a credibility crisis within the organization.

Based on what we know about crisis communication, it is clear that Meta is experiencing an identity crisis and a breakdown of stakeholder trust, especially with

users and advocacy groups. Meta's most important stakeholders have been advocating for stronger protections and more attention to privacy. Stakeholders demand that Meta respond in real, transformative ways.

All of these breakdowns and crises have escalated Meta into facing a substantial legitimacy crisis. Legitimacy is the determining factor as to if an organization should be allowed to exist and function as it currently does. Meta's constant privacy scandals are making the organization feel untrustworthy, hence making its worthiness to exist as an organization feel questionable. The fact that these scandals have been happening time and time again for years indicates to stakeholders that there is a deep-rooted, ongoing, and preventable crisis within Meta. This is not just a reputational issue. Because these issues stem directly from how Meta makes a majority of their money, stakeholders are beginning to assume that Meta does not want to change their ways. This makes the threat to Meta's legitimacy a lot heavier.

The way Meta approaches transparency makes this issue even more complicated. When an organization provides the public with more transparency, sometimes we see the transparency paradox occur. If a company releases too much confusing and complex information, we often see the public become more confused by the information, which leads to skepticism. Meta has certainly utilized this 'info dump' technique to further confuse the public regarding their policies and stances on privacy. Meta's Transparency Center alone contains hundreds of documents over hundreds of categories, including but not limited to enforcement reports, human rights reports, data access reports, and quarterly transparency reports. The sheer volume of documents Meta releases is more of a deflection than honest and open transparency. Meta does have high visibility with their reports, documents, and data, however there is low transparency within this system, as people can't understand or track information efficiently. Visibility means Meta has proved that the information exists by publishing the data, but transparency means people would be able to understand the information to hold Meta accountable (Stohl, Stohl, Leonardi, 2016). It seems to stakeholders that Meta is just trying to protect and manage their image rather than truly hold themselves accountable.

"Meta's financial engine remains firmly rooted in advertising across its platforms —Facebook, Instagram, WhatsApp, and Messenger. With over three billion users globally, Meta has mastered the art of collecting user rich data, using AI to target ads more effectively, and monetizing attention at scale" (Dawgen Global, 2025). This information tells us that Meta's business model completely relies on advertising and data collection. These privacy scandals are not an accident. It is not a coincidence that these scandals are directly tied to how the company makes 99 percent of their money, according to Dawgen Global (2025). This supports the idea that this crisis is founded on how the organization operates and is embedded in the way Meta functions. The same data usage procedures that generate the most revenue for Meta are the same procedures that have been breaking down stakeholder trust for years.

Response Strategy

As a tech conglomerate, users traditionally trust companies with their personal data through consent. Given this dynamic, Meta's response strategy must directly address that erosion, making accountability and visible corrective action non-negotiable components of any communication. Meta's continued privacy concerns can be analyzed through Coombs' Situational Crisis Communication Theory (SCCT), in which crises are categorized based on the perceived organizational responsibility. Within the SCCT framework, Meta's crisis of data privacy falls under the preventable crisis cluster where organizations are assigned a high responsibility level. Identifying under the preventable cluster connotes that a company knowingly created risk or violated rules (Coombs, 2007). Image Repair Theory (IRT) can be used in addition to SCCT to preserve Meta's reputation post-crisis. IRT has the power to shake the persuasive framing of the communication itself (Benoit, 2013). For this theory, it is imperative that perceptions matter more in comparison to objective truth. Meta's communication has to be one that can alter stakeholders emotionally as well as cognitively understand the crisis at hand. Preventable crises with high organizational responsibility call for a rebuild strategy in particular, mortification paired with corrective action (Coombs, 2007).

Using a rebuild response strategy is a good fit for this crisis due to its ability to allow an opportunity for relationship repair through clear action and accountability. In utilizing mortification in a response, it is vital that Meta offers a genuine apology that ensures responsibility on the company's behalf instead of deflecting from the crisis. Additionally, corrective action in a response requires communicating clear steps to avoid future data misuse such as breaches, and also expanding opt-out mechanisms that give users control over their personal data and usage. Combining the two strategies mentioned will address the identified goals of repairing stakeholder relationships and protect organizational reputation. It is important to signal to stakeholders and platform users alike that Meta is remorseful but dedicated to creating operational change.

Corrective action and mortification work together and would complement the SCCT principles utilized during the crisis. Mortification would help address the reputational damage by portraying genuine remorse while corrective action indicates actionable steps toward change. A strategy such as bolstering would not be appropriate in this crisis as it would deflect from the severity of the crisis alongside the frequency of Meta's data privacy breaches. Utilizing IRT can position Meta to follow the track of accountability and change, focuses on those affected by Meta's negligence, and gives clear steps forward on how they intend to change their policies and guidelines.

Together, these strategies will position Meta not as a company minimizing harm, but also actively working to earn trust. To be able to continue the growth across their platforms, Meta must protect their reputation as they handle users' sensitive and private information. Composing a statement including both IRT and SCCT principles,

acknowledging wrongdoing, apologizing outright and directly, and committing policy reform, offers the strongest path to reputational recovery. Additionally, this will reinforce that Meta's user protection is a core company value.



Mock Communication

FOR IMMEDIATE RELEASE

Meta Platforms Inc. Plans for Privacy Concerns

[Menlo Park, CA, April 13, 2026] Today, Meta Platforms Inc. announced an action plan to address user privacy and data concerns across its platforms, including Facebook, Instagram. And WhatsApp. As these reports surface, it's clear that the issue is not only about data practices but the communication around these practices. Meta claims that privacy is the priority, yet many users don't feel that their experience reflects that. This disconnect creates confusion about what user practices are in place and what users should expect from Meta platforms and devices.

Reports claim that Meta platforms are breaching user privacy agreements that protect user data containing AI chats and recorded audio/video from Meta AI devices, i.e. Rayban Meta glasses. In response to these ongoing claims, Meta reinforces their commitment to protect user data and privacy. Although, they acknowledge the change in public and stakeholder perception have changed.

To address the concerns Meta will plan to implement the following measures this year:

- Limiting human access to user data: Meta will implement more oversight of third-party contracts. Emphasizing what data can be accessed and how it can be used

- Improving user awareness: Clearer tools and settings will be introduced so users will better understand and manage how their data will be collected, stored, and used.
- Communication improvements: Clearer communication to the public about privacy will be readily available to users to limit confusion about their privacy while using Meta platforms.

Meta acknowledges these issues as preventable while perceiving them to be completely solvable. The company recognizes that rebuilding trust will take time and will require frequent policy updates. Moving forward, Meta will continue to review its systems and communication to users.

Sources

Meta. (n.d.). *Privacy Progress Update*. Meta.

<https://www.meta.com/actions/privacy-progress/>

User Trust in Facebook Privacy: Survey Stats. (2025, August 30). Socialeum.

<https://socialeum.com/user-trust-in-facebook-privacy-survey-stats/>

Brown, Dawkins. (2025, March 23). *Beyond the Ad: Meta's Business Model as a Blueprint for Entrepreneurial Success*. Dawgen Global.

<https://www.dawgen.global/beyond-the-ad-metas-business-model-as-a-blueprint-for-entrepreneurial-success/>

Bagdonas, Tracy. (2026, April 1). *Despite Privacy Promises, Meta, Third Parties Read and Store WhatsApp Messages, Class Action Lawsuit Alleges*. Class Action.

<https://www.classaction.org/blog/despite-privacy-promises-meta-third-parties-read-and-store-whatsapp-messages-class-action-lawsuit-alleges>

Meta Faces Privacy Backlash over Ray-Ban Meta Glasses. (2026, April 26). Lets Data Science.

<https://letsdatascience.com/news/meta-faces-privacy-backlash-over-ray-ban-meta-glasses-199b90c9>

Hatch, M. J., & Schultz, M. (2002). *The dynamics of organizational identity*. Human Relations, 55(8), 989–1018. <https://doi.org/10.1177/0018726702055008181>

Coombs, W. Timothy. "Protecting Organization Reputations During a Crisis: The Development and Application of Situation Crisis Communication Theory." *Corporate Reputation Review*, vol.10, no.3, 2007, pp.163-176. <http://dx.doi.org/10.1057/palgrave.crr.1550049>

Benoit, William L. "Image Repair Theory and Corporate Reputation." *The Handbook of Communication and Corporate Reputation*, edited by Craig E. Carroll, Wiley, 2013, pp.213-221.

<https://onlinelibrary.wiley.com/doi/10.1002/9781118335529.ch19>

Dowling, Grahame R. *Winning the Reputation Game: Creating Stakeholder Value and Competitive Advantage*. The MIT Press, 2016.

https://uc.instructure.com/courses/1845598/files/202137317/download?download_frd=1

ORIGINAL SUPPORTING WORK

Appendix C

From a strategic communication view-3 recommendations.pdf

01 Research Situation analysis	02 Strategy Stakeholder response	03 Execution Executive-ready writing
--	--	--

Prepared by

Bisetsa Bienvenu

Writing samples reframed as professional case studies for communications, PR, marketing, and corporate affairs roles.

Bisetsa Bienvenu

From a strategic communication view we have 3 recommendations we would like to give Meta about how it should move forward since it has reached a class action lawsuit.

The first recommendation for leadership to do is to make more clear communication that normal people will understand regarding user privacy data. Having clear communication means not burying people in technical terms or leaving the audience in confusion about your legitimacy, credibility and image. Meta should be practicing what they preach when it comes to user data protection when communicating to stakeholders; By doing this, it will increase the stakeholders trust, which will fix the legitimacy if they practice what they preach when it comes to user data privacy. If they don't change their communication strategies, the inconsistencies in Meta's communications strategies will hurt the brands' credibility because what they believe vs their actions will continue to hurt Meta platforms.

The second recommendation, since the data privacy issue has escalated to a class action lawsuit, is to implement more oversight on third party contractors. The main issues with this class action lawsuit would be keeping the media under control, since they have loved sensationalizing stories, which will hurt our image and reputation if they get the control of the narrative. Another issue with the class action lawsuit is that there's gonna be regulators involved, so there will be heavy fines to pay. Since this involves other countries, international bodies and media will be involved. We can avoid future issues by implementing a leader with transformational leadership skills like empowering, motivating, and inspiring those third-party contractors not to read user data, to do what's correct in a manner that aligns with Meta's pillars on principles and moral. This transformational leader will have oversight of those third-party contractors, so they don't read/have sensitive private data that's supposed to be locked away. This will build more trust since users trust that we are handling their data and past concerns and issues consciously and securely.

The third recommendation would be creating more tools and settings for users to personalize, so they choose what kind of data they would like to share with Meta and have explanations under those settings, so they understand how their data is being shared, used, collected, and for training on AI models. Those explanations under those tools or settings should help the user understand how it might or not affect the user's experience and account when using Meta platforms. This strengthens the public stakeholder's perception that we listen to and care about our users that we are willing to create more tools for user safety.

We believe that this data privacy situation is a part of the ongoing issues that Meta has had before in the past and will continue to have if this data privacy issue is not addressed and contained. Meta needs to communicate better, so normal users don't get lost trying to understand technical terms. Leadership skills and implementation of more oversight need to happen because human errors still happen. Meta should be committed to making Meta platforms more personalization able on data. Meta should be also committed to protecting user data to which we cannot afford to mess up, because moving forward with the whole class action lawsuit, anything that contradicts Meta's image and identity will hurt its credibility as an organization which will lead to users and investors leaving Meta Platforms.

ORIGINAL SUPPORTING WORK

Appendix D

Phase 4-Mata.pdf

01 Research Situation analysis	02 Strategy Stakeholder response	03 Execution Executive-ready writing
--	--	--

Prepared by

Bisetsa Bienvenu

Writing samples reframed as professional case studies for communications, PR, marketing, and corporate affairs roles.

Bisetsa Bienvenu

Key Identity Insights

Meta claims to prioritize human connection and building community, innovators in their technology, and committed to privacy and safety for users. Leadership stresses focus on the future and an aim to connect people across the globe.

Meta's internal culture prioritizes high performance and innovation based on their efficient product development and risk-taking attitudes. Their business model is based on advertisement and user data collection, which generates 99% of their revenue (Dawkins, 2025). Although Meta claims a privacy-first business model, they care more about rapid growth and efficiency within their organization. A privacy and consumer-first identity is not prioritized.

Publicly, Meta emphasizes privacy, data protection, accountability, and ethical innovation. Their messaging frames Meta as transparent, privacy-focused, and passionate about its users.

Meta's identity contradicts its actions, specifically regarding privacy. Despite building their brand on user safety and confidentiality, the organization generates most of its revenue through data extraction and advertising. It promotes itself as an ethical tech company while operating as a surveillance-based advertiser.

Meta's identity is inconsistently perceived across stakeholders. Users do not trust Meta in regards to data practices, the media discusses persistent privacy scandals, investors are worried about its reputation, and regulators are pushing accountability. Additionally, Meta's privacy reporting demonstrates the transparency paradox—overloading stakeholders with mass information and providing no clear visibility. Meta's external image is defensive and underhanded.

This misalignment reflects what Hatch and Schultz (2002) describe as a breakdown in an organization's identity, internal culture, and image. They describe that inconsistencies between what an organization claims to be, how it behaves internally, and how stakeholders perceive these actions are what can contribute to a legitimacy crisis.

Core Communication Risks

Meta is facing a legitimacy crisis. Stakeholders are increasingly concerned whether Meta is trustworthy enough to operate in its current state. Meta's repeated privacy issues and inconsistent data protection practices have emphasized these concerns. This threatens Meta's status within public and regulatory viewpoints.

Meta has had a breakdown of trust, especially within users, due to data exploitation, chatbot data leaks, and scandals like Cambridge Analytica. Meta's attempts at reassuring its users are often deemed performative. Benoit (2013) describes an image repair theory, which states that when organizations rely on

messaging and putting out statements instead of taking corrective action, stakeholders are not likely to perceive the messaging as genuine. If users do not trust Meta to protect their data, they may revoke their consent for its use entirely, which will shatter Meta's core business model.

Other stakeholders, like regulators, have expressed their distrust in Meta. Lawsuits and regulatory action in relation to Meta's privacy issues have increased. Meta has faced class action lawsuits regarding user data misuse. These actions define public perception and Meta's external reputation.

These issues contribute to further magnifying Meta's image-identity gap. Meta positions themselves as being focused on privacy, safety, and connection, but its actions suggest the opposite. The public sees Meta as a profit-driven company that lacks transparency. Each scandal reinforces this perception. As Meta continues to promote its own trustworthiness and transparency without addressing root issues, the gap between its identity and the image grows.

Meta releases large amounts of transparency documents on their website. The information is too complex and unclear. Stakeholders might interpret Meta's effort to provide documentation and proof as trying to please them instead of actually being accountable and safe with user data.

Meta's primary communication risk is not solitary scandals; it is an escalating legitimacy crisis caused by privacy scandals, an image-identity gap, and ineffective transparency protocols.

Strategic Recommendations

From a strategic communication view we have 3 recommendations we would like to give Meta about how it should move forward.

The first recommendation for leadership to do is to make more clear communication that normal people will understand regarding user privacy data. Having clear communication means not burying people in technical terms or leaving the audience in confusion about your legitimacy, credibility and image. Meta should be practicing what they preach when it comes to user data protection when communicating to stakeholders; By doing this, it will increase the stakeholders trust, which will fix the legitimacy if they practice what they preach when it comes to user data privacy (Dowling). If they don't change their communication strategies, the inconsistencies in Meta's communications strategies will hurt the brands' credibility because what they believe vs their actions will continue to hurt Meta platforms.

The second recommendation, since the data privacy issue has escalated to a class action lawsuit, is to implement more oversight on third party contractors. The main issues with this class action lawsuit would be keeping the media under control, since they love sensationalizing stories, which will hurt our image and reputation if they get control of the narrative. Another issue with the class action lawsuit is that there are going to be regulators involved, so there will be heavy fines to pay. Since this involves

other countries, international bodies and media will be involved. We can avoid future issues by implementing a leader with transformational leadership skills like empowering, motivating, and inspiring those third-party contracts not to read user data, to do what's correct in a manner that aligns with Meta's pillars on principles and morals. This transformational leader will have oversight of those third-party contracts, so they don't read/have sensitive private data that's supposed to be locked away. This will build more trust since users trust that we are handling their data and past concerns and issues consciously and securely.

The third recommendation would be creating more tools and settings for users to personalize, so they chose what kind of data they would like to share with meta and have explanations under those settings, so they understand how their data is being shared, used, collected, and for training on ai models (Meta). Those explanations under those tools or settings should help the user understand how it might or not affect the user's experience and account when using Meta platforms. This strengthens the public stakeholder's perception that we listen to and care about our users and that we are willing to create more tools for user safety.

Why This Matters Going Forward

We believe that this data privacy situation is a part of the ongoing issues that Meta has had before in the past and will continue to have if this data privacy issue is not addressed and contained. Meta needs to communicate better, so normal users don't get lost trying to understand technical terms. Leadership skills and implementation of more oversight need to happen because human errors still happen. Meta should be committed to making Meta platforms more personalization able on data. Meta should also be committed to protecting user data to which we cannot afford to mess up, because moving forward with the class action lawsuit, anything that contradicts Meta's image and identity will hurt its credibility as an organization which will lead to users and investors leaving Meta Platforms.

References:

Hatch, M. J., & Schultz, M. (2002). *The dynamics of organizational identity*. Human Relations, 55(8), 989–1018. <https://doi.org/10.1177/0018726702055008181>
Benoit, William L. "Image Repair Theory and Corporate Reputation." *The Handbook of Communication and Corporate Reputation*, edited by Craig E. Carroll, Wiley, 2013, pp.213-221.
<https://onlinelibrary.wiley.com/doi/10.1002/9781118335529.ch19>

Brown, Dawkins. (2025, March 23). *Beyond the Ad: Meta's Business Model as a Blueprint for Entrepreneurial Success*. Dawgen Global.

<https://www.dawgen.global/beyond-the-ad-metas-business-model-as-a-blueprint-for-entrepreneurial-success/>

Bagdonas, Tracy. (2026, April 1). *Despite Privacy Promises, Meta, Third Parties Read and Store WhatsApp Messages, Class Action Lawsuit Alleges*. Class Action.

<https://www.classaction.org/blog/despite-privacy-promises-meta-third-parties-read-and-store-whatsapp-messages-class-action-lawsuit-alleges>

Dowling, Grahame R. *Winning the Reputation Game: Creating Stakeholder Value and Competitive Advantage*. The MIT Press, 2016.

https://uc.instructure.com/courses/1845598/files/202137317/download?download_frd=1

Meta. (n.d.). *Privacy Progress Update*. Meta.

<https://www.meta.com/actions/privacy-progress/>

Timeline for what was pasted in the document:

[From a strategic communication view we have 3 recommendations.docx](#)

ORIGINAL SUPPORTING WORK

Appendix E

Meta Data Privacy Presentation.pdf

01 Research Situation analysis	02 Strategy Stakeholder response	03 Execution Executive-ready writing
--	--	--

Prepared by

Bisetsa Bienvenu

Writing samples reframed as professional case studies for communications, PR, marketing, and corporate affairs roles.

Meta's privacy issue is bigger than just a bad reputation moment. It has turned into a legitimacy problem because people are starting to question whether the company can be trusted to handle user personal data responsibly. That matters because legitimacy is about whether stakeholders believe the company deserves to operate with the power it has.

The second issue is the gap between what Meta says and what Meta does. The company presents itself as privacy focused, but reports and lawsuits show that user data was accessed by contractors and third parties. That creates a disconnect between Metas' public image and stakeholder experience and expectations.

This problem also seems recurring instead of a one-time issue. Similar privacy concerns have come across several Meta Products like WhatsApp, Facebook, AI tools, and Ray Ban Glasses. Because of this, it starts to look like a deeper issue in the company's culture or leadership, not a one-time mistake.

Another reason this is serious is because multiple stakeholder groups are paying attention. Users are worried about their private data information; the media will amplify the story since they love sensationalizing stories. Regulators will step in since this involves international countries and user data information. Investors will see the company as a financial risk along with more whistleblowers coming out and adding more pressure.

- **This is more than a reputation issue**
 - Meta is facing a legitimacy crisis because stakeholders are questioning whether the company can still be trusted to operate responsibly and safely.
- **There is a gap between the company's pillars and actions**
 - Meta claims that it values and protects user privacy and data. Reports and class action lawsuits show that contractors in Kenya and third parties accessed user data
- **This issue looks like a recurrence of past privacy concerns & problems, not a random situation**
 - Past privacy issues and concerns have appeared across WhatsApp, Facebook, AI tools, and the RayBan glasses
- **Multiple stakeholders are paying attention to this issue**
 - Users, media, regulators, investors, and employees all have reasons to be concerned regarding the data privacy issue.
- **Long-term risk of losing trust and public support**
 - If Meta does not make changes, the company will face more lawsuits, weaker confidence from investors, and lose user trust.