**Beat: Technology**

# Growing Concerns Mount Over Data Breaches Involving Meta and Facebook

## Rise of Privacy Concerns

San Francisco, 16.03.2024, 22:40 Time

**USPA NEWS -** Recent revelations of data breaches involving Meta Platforms, Inc. (formerly Facebook, Inc.) have sparked widespread concern and legal action, shining a spotlight on the tech giant's handling of user information. Among the most alarming developments are lawsuits alleging the unauthorized use of medical data by Facebook, leading to targeted advertisements without user consent.

These lawsuits add to a litany of privacy concerns facing Meta and Facebook, including big privacy lawsuits lodged against the companies in recent years. The company's wrong dealings started to gainnin attention when the Cambridge Analytica scandal, where personal data from millions of Facebook users was harvested without their consent for political profiling was first exposed. It started the first big example of the company's disregard for user privacy.

Amidst this mounting scrutiny, attention has turned to Mark Zuckerberg's wife, a doctor by profession, with calls for her to take a more active role in overseeing the handling of sensitive medical information on Facebook's platforms and it's consequences.

California, along with numerous other states, has filed lawsuits against Meta for purportedly causing harm to children's mental health through its platforms, including Facebook and Instagram. This legal action follows a whistleblower report by Frances Haugen, revealing that Facebook has been misleading the public regarding its efforts to combat hate speech, violence, and misinformation. Haugen's disclosures have sparked widespread concern and scrutiny, prompting federal law enforcement to investigate allegations raised by a former employee.

The unforgettable Facebook data breach scandal that happened during the 2016 elections. It stands as a watershed moment in the intersection of technology and politics. It came to light that Cambridge Analytica, a political consulting firm, illicitly harvested the personal data of millions of Facebook users without their consent. This breach was particularly alarming due to the use of the acquired data for targeted political advertising and manipulation of voter behavior.

The scandal raised serious concerns about the role of social media platforms in influencing democratic processes and highlighted the vulnerability of users' personal information to exploitation for political gain. In the aftermath of the breach, Facebook faced intense scrutiny from lawmakers, regulators, and the public, leading to calls for greater transparency, accountability, and regulation of tech companies. The incident underscored the need for stronger data protection measures and ethical standards to safeguard user privacy and preserve the integrity of democratic elections in the digital age.

Another Facebook data breach scandal marks the company's history of privacy controversies. In April 2019, it was revealed that millions of Facebook users' personal data, including passwords, had been stored in plaintext on internal servers. This meant that the data was easily accessible to thousands of Facebook employees, potentially exposing it to misuse or unauthorized access. The breach affected a large number of Facebook users, raising serious concerns about the company's data security practices and its ability to protect user information.

While Facebook stated that there was no evidence of abuse or misuse of the exposed data, the incident further eroded public trust in the platform's commitment to user privacy. It served as a stark reminder of the ongoing challenges posed by data security breaches and underscored the need for companies like Facebook to prioritize robust security measures and transparent communication with users to prevent future breaches.

The Facebook data breach of 2018 remains one of the most significant cybersecurity incidents in recent memory, impacting millions of users worldwide. The breach, which occurred in September 2018, compromised the personal data of approximately 87 million Facebook users. The vulnerability stemmed from a flaw in Facebook's "View As" feature, which allowed hackers to exploit access tokens and gain unauthorized entry to user accounts. This breach exposed a vast array of sensitive information, including users' names, email addresses, phone numbers, and in some cases, even private messages. The fallout from the breach was swift and severe, leading to widespread public outcry, regulatory scrutiny, and a significant loss of trust in Facebook's ability to safeguard data.

Recent Facebook data breaches involving sensitive medical information have sparked significant concern over the privacy and security of individuals' health information. In a recent development, a proposed class action lawsuit alleges that a Seattle-area hospital permitted Facebook's online tracking tools to integrate with its website, resulting in the sharing of personal health data belonging to hundreds of thousands of individuals with Meta and other third parties. Furthermore, in 2023, five anonymous plaintiffs came forward in a consolidated lawsuit, accusing Meta of intercepting health information from individuals with Facebook accounts by installing the Meta "pixel" on patient portals of their healthcare providers. These plaintiffs claimed that Meta profited from the intercepted information by leveraging it to deliver targeted advertisements. These allegations highlight the potential risks associated with the unauthorized sharing and use of sensitive health data, raising serious concerns about the protection of individuals' privacy rights in the digital age.

Attorneys collaborating with ClassAction.org are investigating potential violations of the federal Video Privacy Protection Act (VPPA) by the operator of the Calm meditation website and app. They suspect that Calm.com may have unlawfully shared consumers' private information without consent, prompting consideration of legal action. Specifically, they allege that Calm.com and its associated app may be utilizing tracking tools to covertly transmit details about users and the videos they've watched to Facebook. This data linkage could potentially connect a user's watch history to their Facebook ID, a unique identifier that could be exploited to link the individual to their Facebook profile. These allegations raise significant concerns about user privacy and warrant thorough examination to ensure compliance with applicable laws and regulations.

Reports from KFF Health News reveal that trackers are collecting browsing- and purchase-related data on the websites of twelve of the largest drugstores in the United States, including grocery store chains with pharmacies. In the list; Walmart, CVS, Walgreens, Rite Aid, and Costco.

These trackers are then reportedly sharing the sensitive information they gather with companies such as Meta (formerly Facebook).

Cookies play a pivotal role in online tracking by sometimes linking individuals on a website to their corresponding account on a social media platform.

The tracking tools, commonly referred to as "pixels," operate discreetly while a website is in use, quietly collecting valuable information about user behavior and interactions. This data is then frequently transmitted to social media firms and utilized to target advertisements, either directly to the individual or to groups of users who share similar demographics or online habits. This targeted advertising approach relies on sophisticated algorithms to analyze and interpret the collected data, allowing advertisers to tailor their messages with remarkable precision. However, while these practices may enhance the effectiveness of advertising campaigns, they also raise significant privacy concerns, as individuals' online activities are monitored and their personal data potentially exploited for commercial purposes without their explicit consent.

These revelations surrounding Meta's corporate greed, where profit is prioritized over adherence to scientific guidelines, underscore the urgent need for accountability and ethical responsibility within the tech industry. By disregarding scientific guidelines and putting profit above all else, Meta risks undermining public trust, compromising user safety, and perpetuating harmful practices that have far-reaching consequences. As consumers demand greater transparency and ethical standards from tech giants like Meta, it is crucial for the company to reevaluate its priorities and commit to aligning its practices with scientific guidance, prioritizing the well-being of its users and communities above financial gains. Only through responsible and ethical conduct can Meta begin to restore trust and contribute positively to the broader societal landscape.

Every year, Facebook and Meta seem to find themselves embroiled in controversies that impact millions of people, yet accountability for these issues remains elusive. This recurring pattern of problems, ranging from privacy breaches to misinformation and algorithmic biases, underscores a fundamental lack of responsibility and oversight within the company. Despite facing widespread public outcry and regulatory scrutiny, Facebook and Meta have largely failed to address the root causes of these problems, allowing them to persist and even worsen over time. The gravity of these issues cannot be overstated, as they have far-reaching implications for user trust, societal well-being, and democratic processes. Without meaningful accountability and proactive measures to address these systemic issues, the cycle of problems plaguing Facebook and Meta is destined to repeat itself, perpetuating harm to millions of users worldwide.

**Article online:**
https://www.uspa24.com/bericht-24277/growing-concerns-mount-over-data-breaches-involving-meta-and-facebook.html

**Editorial office and responsibility:**
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Ricardo De Melo Matos



**Editorial program service of General News Agency:**
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619