INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 9 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 9 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-10-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

X'S (FORMERLY AS TWITTER) TERMS & CONDITIONS AND ITS IMPACT ON THE DEBATE OF PRIVACY AND DATA OWNERSHIP

AUTHOR - SHERLYN ELIZEBETH SANTHOSH, STUDENT AT AMITY LAW SCHOOL, AMITY UNIVERSITY, MUMBAI

BEST CITATION - SHERLYN ELIZEBETH SANTHOSH, BLEEDING BOUNDARIES : RELIGION , RIGHTS AND RESTRICTIONS, AND REMEDIES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (9) OF 2025, PG. 284-302, APIS – 3920 – 0001 & ISSN - 2583-2344.

This article is published in the collaborated special issue of Amity Law School, Amity University, Mumbai and the Institute of Legal Education (ILE), titled "Emerging Trends in Law: Exploring Recent Developments and Reforms" (ISBN: 978-81-986345-1-1).

Abstract

This research paper explores the evolution of X's (formerly Twitter) Terms and Conditions, specifically the 2024 revision, and discusses its implications for user privacy, ownership of data, and legal underpinnings of digital consent. The study explores the platform's evolution through a multi-layered analysis, evaluating recent policy changes critically as markers of broader patterns in surveillance capitalism and corporate data supremacy. It compares the viability of user consent in these models to the counterarguments made by platform proponents and the dominant behaviours of major tech companies. Additionally, it analyses the legal protections that are in place in India and around the world and looks at emerging data vulnerabilities such as chatbot flaws, AI training methods, and third-party access. In order to gather real concerns and awareness, it uses user replies and an impartial poll to gauge public opinion. In addition to analysis, this paper offers policy suggestions for redistributing power between platforms and users, including stronger transparency requirements, clearer consent procedures, and legislative adjustments to safeguard digital rights. Finally, the study demands for a digital governance approach that is more equitable and responsible.

Chapter 1: Introduction

In today's world, social media sites are playing an increasingly powerful role in communication, culture, and commerce. X (formerly Twitter) has come a long way from being a simple microblogging platform to a much more capable and comprehensive ecosystem all thanks to and under the guidance of Elon Musk. In 2023, Twitter rebranded to X and underwent a series of major policy changes, one of which included the implantation of its own chatbot Grok. For the development of Grok, X implemented new policies which allow user-generated data to be collected, which includes posts, replies, and media; and by 2024, the new revised Terms and Conditions change the whole trajectory by removing all the previous choice for users to opt out of participation. This change enraged significant public discussion around user consent, privacy rights, and ownership of digital information. There has been a global concern of the loss of individual control over personal information in online settings. X's evolving policies reflect this. The most challenging thing is the imposition of consent through one-sided terms, which raises any doubt on the voluntariness and validity of such transactions. India's recent passing of the Digital Personal Data Protection Act, 2023 aimed at protecting user data. But the effective gap still sustains, especially if we compare it to the global standards. The objective of this research study is to perform a critical assessment of the validity of user consent under the updated policies of X, the defenses available to corporations in data cases and the overall

impact on privacy law and digital rights, particularly in the context of India. This study intends to contribute to the ongoing discourse surrounding data protection, informed consent, as well as corporate accountability in the age of artificial intelligence through comparative legal analysis and user survey data.

The central questions guiding this paper will be: *Whether the consent given by the users for X's Terms and Conditions consensually? Which principles can be used by the companies as defense for data breach or dispute over the Terms and Conditions? What are the potential dangers of such data collection for Grok? Do the public feel threaten by the implementation of such policies?* and *What is India's current capability to stand against such data breach in comparison with statutes over the globe?*

Chapter 1.1: Background and Evolution of X (formerly known as Twitter)

Twitter, introduced in 2006, works as a microblogging site to allow users post short posts of 140 characters. Founders of Twitter: Noah Glass, Jack Dorsey, Biz Stone, and Evan Williams. Unlike other social media sites, Twitter differentiated itself with its emphasis on conciseness, immediacy, and interactivity. During events like the Arab Spring, it also was an important contributor to global events that aids information sharing.[440] (Britannica, 2025) Over time, through hashtags, retweets, threads, and moments, Twitter expanded its usage and became known as an excellent platform for news sharing, political conversation and public debate.

In a highly publicized and contested bargaining episode, entrepreneur Elon Musk acquired Twitter in 2022. Musk's leadership has seen much internal reorganization on Twitter including mass firers, changes in its content moderation practices, and new paid features like Twitter Blue. A milestone event happened in 2023 when Musk rebranded Twitter to "X," showing an intention to change the microblogging site to an overall "everything app" like China's WeChat. Rebranding includes changing the branding elements of the platform, algorithm functions, and business vision to integrate communication, payment, shopping, and artificial intelligence technologies under one roof.[441] (Britannica, 2025).

After the rebranding to X, the company added a whole suite of features aimed at transforming platform's functionalities beyond mere microblogging. One of the most valuable innovations till date was the launch of its own artificial intelligence chatbot Grok. Unlike conventional chatbots, which compel users to log into different apps or specialized interfaces for each interaction, Grok is more tightly integrated into X. Those using Twitter would be able to use Grok right from their timelines. Embedded prompts inside tweets, replies, and posts would help him communicate without leaving Twitter. For example, a Grok user can tell the AI to interpret a post, summarize a thread, or respond to a post by tagging or asking it in an existing thread. In addition, Grok had its presence on the home page, suggesting that X sought an interactive multi-utility experience. This easy integration was a huge change from how chatbots were normally linked in their own silos as AI support became a timely, natural part of the interaction.[442] (The Verge, 2024)

[440] "Twitter." Encyclopaedia Britannica. Available at: https://www.britannica.com/money/Twitter. (last accessed on 1st May 2025)

[441] Supra note 1

[442] Jay Peters, "X begins testing Grok, its ChatGPT-style AI chatbot, on some Twitter users," The Verge, available at: https://www.theverge.com/2024/1/9/24030261/grok-ai-chatbot-test-chatgpt-twitter-x (last accessed on 1st May 2025)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

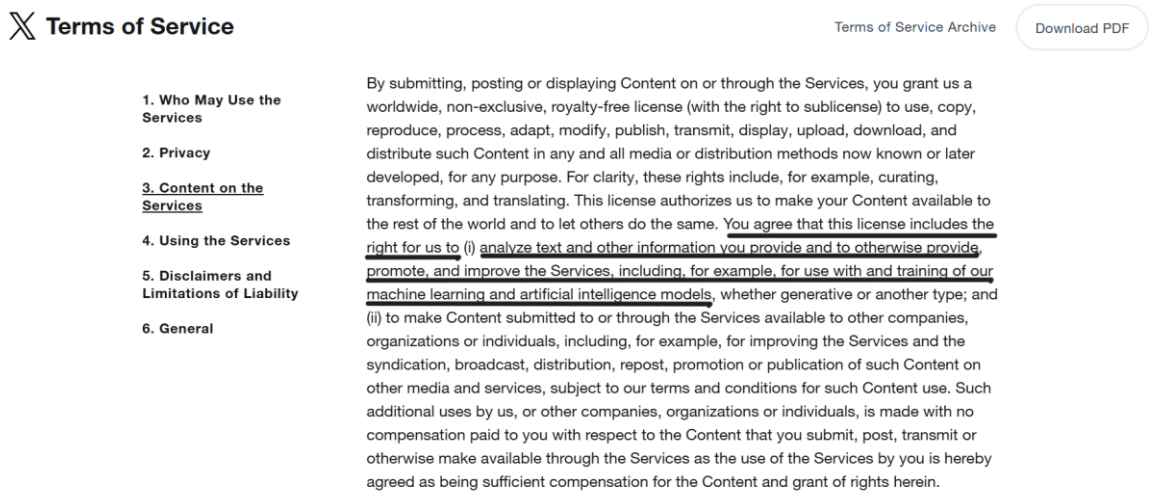
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Chapter 1.2: 2024 Terms and Conditions of X



Terms of Service

Terms of Service Archive | Download PDF

1. Who May Use the Services
2. Privacy
3. Content on the Services
4. Using the Services
5. Disclaimers and Limitations of Liability
6. General

By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display, upload, download, and distribute such Content in any and all media or distribution methods now known or later developed, for any purpose. For clarity, these rights include, for example, curating, transforming, and translating. This license authorizes us to make your Content available to the rest of the world and to let others do the same. You agree that this license includes the right for us to (i) analyze text and other information you provide and to otherwise provide, promote, and improve the Services, including, for example, for use with and training of our machine learning and artificial intelligence models, whether generative or another type; and (ii) to make Content submitted to or through the Services available to other companies, organizations or individuals, including, for example, for improving the Services and the syndication, broadcast, distribution, repost, promotion or publication of such Content on other media and services, subject to our terms and conditions for such Content use. Such additional uses by us, or other companies, organizations or individuals, is made with no compensation paid to you with respect to the Content that you submit, post, transmit or otherwise make available through the Services as the use of the Services by you is hereby agreed as being sufficient compensation for the Content and grant of rights herein.

X's Terms of Service[443]

[443] "Terms of Service," X.com. Available at: https://x.com/en/tos (last accessed on 1st May 2025)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The 2024 rewrite of the Terms and Conditions for X was a break from previous user agreements and policy frameworks. Under Elon Musk, X made rule provisions that drastically changed the platform's bond with the users for the way user-generated data would be treated. One of the most controversial changes was the removal of the user's right to opt out of data collection for internal development processes, particularly to train its own AI system, Grok. With the new system, users are deemed to have automatically agreed to the use of their posts, responses, media uploads and other interactions on the site for training AI just by using the app.

This will change everything we've been told around digital consent and ownership of data. Prior to the 2024 overhaul, X had given varying degrees of control to users over their information. Opt out options were introduced in line with changing international standards on digital privacy, such as those contained in the European Union's GDPR. The new policy, on the other hand, took that freedom away and created a policy of "forced consent" wherein a user's continued use of the platform is a general consent to widespread use of their data. The T&Cs clearly stated that user content would be used to improve Grok's features thereby commodifying their actions which left the user with no real choices or real control options.

In addition to the mandatory use of data clause, the 2024 Terms and Conditions further extended the definition of "user data" and processing thereof. It is found that easy-to-track interactions is also considered as metadata but lacks the clarity of when, how often, and to what extent it is collected. Of course, deleted comments om the cache server is not excluded. Also, X had the right to share anonymized or aggregated information with third parties for other purposes that do not relate to platform optimization, including commercial uses. The extensive mention of this phenomenon caused anxiety among users, lawyers, and cyber rights activists, who felt that such a policy oversteps the boundary between user agreement and domination. This was very much the case where social media websites have become essential communication tools, and not voluntary services. The following chapters will conduct an empirical study on this issue with the assistance of statutory analysis, comparative approaches, and user survey results.

Chapter 2: Validity of User Consent

Chapter 2.1: User Consent deemed as consensual

According to the GDPR and India's Digital Personal Data Protection Act, 2023, consent, and particularly informed consent, is a fundamental legal and ethical concept in data protection regimes. As a matter of principle, the consent has to be freely given, specific, informed, and unambiguous. Users can find out exactly what information is being collected about them, why it's being collected, who is collecting it, how long it will be retained for, and on what terms it may be shared. These demands rely on rights under the Constitution, specifically the right to privacy, and seek to provide the ability to control their identities. The actual practice of users translating these principles into reality, nevertheless, is still seriously lacking.

Joergensen's (2014) empirical evidence shows how the users, particularly the teens, considers consent as a necessary hurdle rather than an informed decision. According to her research, the young people questioners take agreement on terms and conditions with platforms such as Facebook as means to get access and not as an informed decision. The resulting viewpoint turns the legal standard of voluntariness into a myth, where "consent" becomes more about functioning rather than freedom.[444] According to Luger, Moran, and Rodden (2013), terms and conditions are typically drafted in such a complex way that it is only marginally less than

[444] Rikke Frank Joergensen, "The unbearable lightness of user consent" 3 *Internet Policy Review 1-14* (2014).

a half of adults in the United Kingdom who are literate enough to understand them.[445]

As a remedy for such weaknesses, Oladele (2025) suggests replacing traditional models such as Dynamic Consent and Privacy Budgets, which center on transparency and concurrent user control. We will use these tools instead of strict one-time consent agreements, adding on iterative, revocable consent, that match changing data settings. This work emphasizes that good consent design requires a careful balancing act between legal compliance and user comprehension and empowerment.[446] When looked at together, these investigations reveal a systemic issue: consent today in a digital world is largely performative in the sense that it is shaped by law and platform design, and not an act of meaningful user autonomy.

Chapter 2.2: Comparison of different companies with their user consent

In evaluating the voluntariness and validity of user consent, one should look beyond X and explore how other big tech platforms handle data collection and user agency. While Facebook (Meta), Instagram, Google, TikTok, and others leverage user data to improve algorithmic personalization and innovate through artificial intelligence, they typically provide at least some mechanisms for opt-in or opt-out consent. TikTok offered settings that allowed the user to customize their permissions regarding the app's use of their content. Google allowed the user to adjust their activity logs and ad personalization. Meta provided switches for targeted ads and location tracking. These settings are often hidden away in submenus so that users must find their way there.

What sets those companies apart from X is not the less relaxing ethical commitment per se but positioning themselves on the scale on global benchmarks like the GDPR. The law states that consent must have four specific characteristics: free, specific, informed, and revocable. To meet this need, different platforms gave people finer-grained control over consent, a regular notice of policy, and controls allowing them to limit processing on dashboards. Some websites provide "reject all option" along with "accept all" option for the sake of user control. In contrast, X ignores the opt-out entirely. Instead, it hides mandatory consent for AI training and data use in its Terms of Service. This departure from best practices reflects an expanding disconnect between regulatory purpose and platform execution.

[445] Ewa Luger, Stuart Moran, and Tom Rodden, "Consent for all: revealing the hidden complexity of terms and conditions" *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13) 2687 2696* (2013)
[446] Sunday Author & Sunday Oladele "Exploring User Consent Mechanisms in Data-Driven Personalization" (2025)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

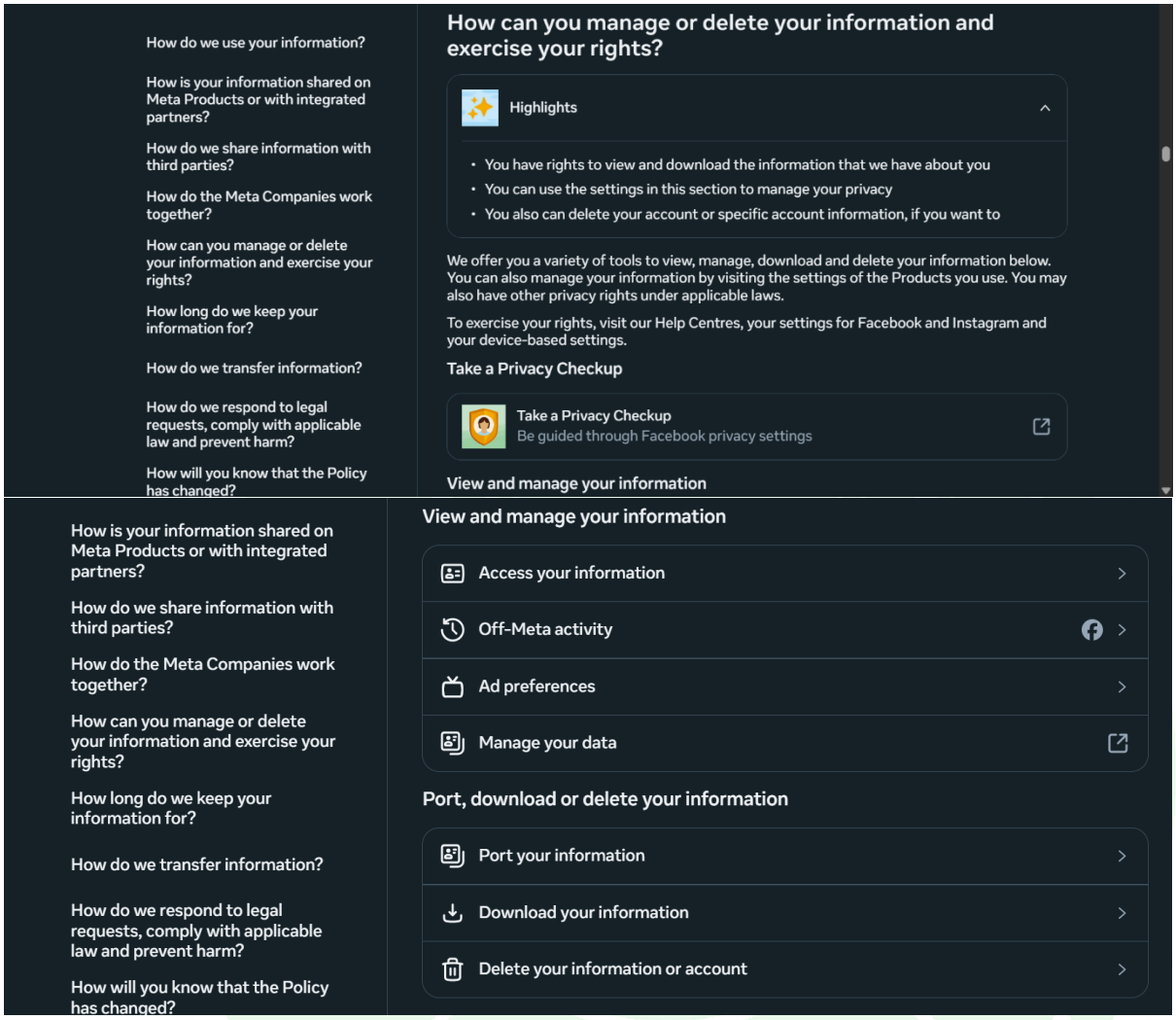
VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in



Meta's Privacy Policy[447]

[447] "Privacy Policy" Meta. Available on https://www.facebook.com/privacy/policy?section_id=6-HowCanYouManage (last accessed on 1st May 2025)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

X's Terms and Conditions for 2024 take an implied, irreversible consent model especially for training Grok, the AI chatbot. This move away from nascent best practices: specific opt-in structures towards a catch-all, non-negotiable provision is quite dramatic. Unlike Meta or Google, which at least provide roundabout ways of limiting data use, X requires full compliance as a condition of continued access. People must agree to the terms or lose the site. As opt-in mechanisms are abrogated, anxiety turns ever more acute, exposing an obvious divergence in expectations, as they become increasingly conditioned by rules and choices of people.

When we see how other companies are dealing with the criticism of using data for AI, the contrast is striking. Big names like OpenAI, Adobe and Meta introduced visible opt-outs. These features allow users to exclude their information from being used in AI-training pipelines. E.g. Adobe recently allowed for the disabling of training on cloud-stored content, and Google's Bard has data-use disclosures. Their decision not to put measures at this point after cutting out earlier possible options is ethically and regulatorily questionable. Their stance of "Take it or leave it" undermines data governance's consensual foundations, weakening consent to an ineffective technicality originating from an unviable user right. Consequently, an increasing visible gap is created, with most firms moving closer to organized openness, X rooted in a coercive compliance model.

Chapter 2.3: Defense by the opposition party

One of the main defenses the platform could rely on is the maxim 'volenti non-fit injuria', meaning that no injury is done to one who consents. This principle suggests if a user, after being made aware of the revised terms, continues to use the platform voluntarily, there is an implied consent on the user's part. According to the business themselves, the policy is available for consultation and use of the service amounts to a contract. Thus, users' choice to remain on these risks can be viewed as having accepted these risks by choice. As per Taylor and Paterson (2020), consent acts as a substantial justification for data processing, not merely a procedural one where the person has the option to object or withdraw consent.[448]

In addition, it may contend that it works within permissible limits of informed consent as envisaged under new data protection regimes. Even in the criticisms made by Abrusio (2024), which emphasizes the tension between fairness and consent in digital contracts, agreements can be presumed to be consented to when the terms are communicated and accessing the service is conditional upon acceptance.[449] The platform may argue that its disclosures are transparent, and that the user was neither deceived nor coerced to consent. Thus, the burden of vigilance is partially shifted on the user, and the burden of reading and understanding what the terms mean and what the implications might be is not a legal duty that the company must enforce but an onus the user is supposed to exercise instead.

Chapter 2.4: Case Study

A New York County Supreme Court case, O'Brien v. Trooper Fitness LLC, made it clear that a clickwrap agreement, where a user has to click "I agree" to a set of terms and conditions, is legally enforceable pursuant to contract law, even if one did not read and comprehend the conditions. The plaintiff suffered an injury while using a fitness company's workout app for which he sued the fitness company for negligence. The court held that the waiver of liability in the clickwrap contract was upheld. Hence, the court dismissed the lawsuit of the plaintiff.[450] This decision signals a growing judicial trend towards the importance of formality in a digital consent, regardless of the

[448] M.J. Taylor and J.M. Paterson, "Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection", 16(1) Art 4 *Indian Journal of Law and Technology*, (2020)

[449] 0 J. Abrusio, "The (In)Efficacy of Consent for the Processing of Personal Data", 6(1) *Humanities and Rights Global Network Journal*, (2024).

[450] **"Terms of Service: Clickwrap Agreement Sufficient to Bar Negligence Claim,"** *Ford Harrison LLP*, available at: https://fhnylaw.com/terms-service-clickwrap-agreement-sufficient-bar-negligence-claim/ (last visited 1 May 2025).

user's actual understanding where clear opportunities to read the terms were available.

According to the case, this would be a great precedent for companies like X who could use the argument of user acceptance for their broad data terms. In court, platforms can rely on the doctrines of volenti non-fit injuria (to a willing person, no harm is done) which means that because one continues to use a platform after accepting the terms, they assume the risk willingly. Courts have been treating clickwrap consent as a valid contractual defence, which means that clicking "agree" is sufficient enough in law even if the person isn't informed. This also shifts the burden away from businesses and on to users, further complicating the premise that digital consent is actually consent or just a tick box.

Chapter 3: Data threats and protections

Chapter 3.1: Data for AI development and training

AI systems like Grok rely predominantly on large datasets for training, testing and continuous refinement. Deep learning models applied to language generation, recommendation systems, or image classification rely on the dimension, scale, and statistical richness. According to Abadi et al. (2016), deep neural networks are fundamentally built using large and representative datasets.[451] This has led to progress in areas such as image recognition, natural language processing and strategic games. These datasets are often crowdsourced and capture users' rich, fluid behavior but may also include sensitive personal data. The rationale behind it is that neural networks have the ability to learn rich representations, but the risk of privacy invasion and unethical use is becoming more evident. This is especially true when there is large scale, vague or coerced consent to use.

The main process associated with dataset acquisition for AI is data mining which is not evil. Data mining has been used historically to extract useful patterns, associations and correlations from large sets of original data. This can be to assist decision-making in areas from marketing to health care (Coenen, 2011).[452] However, the transition of the discipline to AI training contexts presents new challenges. The ethical risk is heightened when non-tabular or personal type data mining is done, including SMS, images, and search histories. Unlike traditional mining for structured intelligence, new AI systems utilize this insight for prediction and personalization, often in ways that are apparent to users. Given their impenetrability, contemporary data's scale and nuance raise questions about whether data is being accumulated in the name of AI with proper governance or just retroactively justified by innovations. With the rising popularity of AI technology, these matters are not incidental, but rather essential issues which lie at the center of a society-wide conversation about how citizens manage their digital architecture.

Chapter 3.2: Cyber Attacks on Chatbots

AI chatbots that are based on advanced language models have become vulnerable to cyber-attacks. This is due to a well-crafted invasion on both the training data, and the model behavior. The most serious threats are data poisoning, prompt injection, and training data extraction. In data poisoning, the criminal adds false or malicious information to the training datasets that corrupt the model during fine-tuning. Prompt injection is a new kind of attack. In this kind of attack, the user input is deliberately designed to manipulate the action of the model. Moreover, it also causes the model to reveal unintended responses. However, what could be the most dangerous of all is training data leakage, whereby information or PII that the model picks up during training can be retrieved via misleading queries.

[451] Martín Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, Li Zhang, "Deep Learning with Differential Privacy" *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS)* 308-318 (2016)

[452] Frans Coenen, "Data mining: past, present and future" 26 *The Knowledge Engineering Review* 25-29 (2011)

Carlini et al. (2021) show how feasible such attacks can be. In their research they show that LLMs such as GPT-2 can memorize verbatim training data: names, phone numbers, and addresses that occur only once in the training corpus. The researchers present a "black-box" extraction technique. An attacker with no insider access to the model manages to get it to output seen training data via sampling.[453] This kind of memorization could reveal a fundamental weakness in AI systems today, posing a risk to users' personal data and regulations. As these models become larger and go into production, the need to create stronger defenses such as differential privacy, input sanitization, and auditing tools is also increasing to avoid risks of accidental data leakage.

Chapter 3.3: Third-party access to user data

Even though companies always say that they capture user data for internal machine learning training; this data never stays that way. User data is a business asset. It may be shared with partners, sold to advertisers, or used to improve cross-platform services, especially at scale. Even when they're anonymized, data is not safe. Re-identification techniques can find a match in other data sets for "anonymous" entries. This allows anyone to determine your identity, especially with location history, browsing patterns, or text entries. Consequently, it is not only overt abuse that poses a threat but rather security. Academic and legal circles are gradually debasing the notion that anonymized data is ethically or legally safe.

Matti Rossi et al. (2024) place these actions in the context of surveillance capitalism as shaped by Shoshana Zuboff, and further explored in Rossi's editorial. In this case, data of the user is not something you collect when offering your services but is the primary raw material that will be commodified, sold and further optimized and used for predicting behavior and manipulating behavior. The details of user activity, namely their information, data, behaviors, and habits, are quite valuable for most platforms today. As a result, platforms are rewarded to monitor, harvest, and monetize these details, frequently with no transparent disclosure or true consent. As computing systems get more complex and less comprehensible, the ethical costs increase: from disempowering marginalized groups to undermining digital agency and turning people into data-scooping vessels. AI model development insidiously transforms into a universal commodifying infrastructure that changes the basic social contract between users and platforms, in an environment devoid of meaningful regulation.

Chapter 3.4: Case study

A significant incident took place in March 2023, where a flaw in the open-source Redis library allowed hackers to take advantage of OpenAI's ChatGPT and steal users' data. Initially part of the bug, view other user's chat history titles and first lines were allowed. In addition to this, hackers temporarily leaked the payment data of some ChatGPT Plus subscribers, including email addresses and the last four digits of credit cards. OpenAI suspended the service, fixed the bug, and notified affected users promptly. However, the incident showed that without compartmentalization and sandboxing controls, the infrastructure of chatbots is vulnerable when handling sensitive data.[454]

When considering the less severe aspects of technology, prompt injection attacks are far more sinister in nature. These attacks happen when an adversary designs inputs with the intent of coercing the AI model to release confidential or restricted information. Recent studies show that even without external tools, ChatGPT-4 and GPT-4o can be coerced into revealing user information through stacked prompts, especially when running in memory

[453] Matti Rossi, Christy MK Cheung, Suprateek ("Supra") Sarker, and Jason B Thatcher, "Ethical issues and unintended consequences of digitalization and platformization" 39 Journal of Information Technology 390-391 (2024)

[454] Pluralsight Content Team, *All about ChatGPT's first data breach, and how it happened*, available at: https://www.pluralsight.com/resources/blog/ai-and-data/chatgpt-data-breach

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 9 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

mode. As AI models become more integrated and maintain context over time, the potential for attacks increases. And the implications are alarming: stored user inputs, even when anonymized, can be exploited and de-anonymized by exploiting such vulnerabilities. These threats do not stem from pure conjecture; they are binge-worthy surveillance, identity fraud, or administrative abuse.[455]

Chapter 4: Fight or Flight response to data concerns

Chapter 4.1: Data protection granted by Indian statutes

X's 2024 Terms and Conditions requiring that users irreversibly consent to data use for AI training in order to get access or mere enjoy the services of the platform. The forced consent or bundled consent is unacceptable in the Indian Digital Personal Data Protection Act, 2023. Section 6(1) of the Act states that consent ought to be "free, specific, informed, unambiguous and constitute an affirmative action on the part of the data subject." [456]It is of utmost importance the use of the word "unconditional" in this, as the consent is made conditional for the usage of the application. With X offering users a choice between two options: accept data collection for AI training or quit using the platform, it effectively negates any argument over providing freely given consent.

It also recognises that consent is not fixed but dynamic, it is not static or one-way. By section 6(4) data users or "Data Principals" are given the right to withdraw their consent at any time and it should be "as easy" to withdraw as it was to give effect to their consent in the first place.[457] In contrast, model X offers no such off switch once you have consented, and the removal of existing privacy settings just cements the permanence of their approach. Further, as per Section 6(6), upon receipt of the request to withdraw consent, data fiduciaries are to discontinue processing personal data, and ensure that third parties delete or stop using it, too.[458] Along with complete data ownership and the idea of withdrawal not even being there in the design, we see that it's absolutely misplaced in connection to India's data rights framework. Rather than empower users to revoke access to their data, X operationalizes data access in open-ended, non-revocable terms. In cases where a user feels there is violation of their data rights, the DPDPA proposes a remedy under Section 13 which mandates a data fiduciary to establish a grievance redressal mechanism. This allows users to challenge abuse, denial of service, or malpractice.[459] Even if X has a global reach and can invoke jurisdictional limitations under Indian law, the processing of Indian users' data would remain subject to the regime under the DPDPA. Further, Section 8(7)(a) of the Act reinforces these rights ordering data to be deleted once it is no longer needed or consent is withdrawn.[460] If X were subject to DPDPA jurisdiction, its current policy of permanent data storage for AI uses, with no end in sight, would almost certainly be in violation of statute. The law is based on the idea that the world is digital, and decisions should be revocable, fair and informed.

Chapter 4.2: Global stands on data protection and privacy

The GDPR, which governs data protection in the EU, imposes a very high threshold for valid consent. The DPDPA of India closely follows the definition of consent being freely given specific informed and unambiguous as provided in Article 4(11) of GDPR.[461] The GDPR goes even further by stating that consent must also be "freely withdrawable" at any moment (Article 7(3)) and refusal or withdrawal must not cause detriment to the data subject.[462] X's "take-it-or-leave-it" approach runs counter to such principles. According to the Guidelines on

[455] Gregory Schwartzman, Exfiltration of Personal Information from ChatGPT via Prompt Injection (2024), available at: https://doi.org/10.48550/arXiv.2406.00199
[456] The Indian Digital Personal Data Protection Act, 2023, s. 6(1)
[457] The Indian Digital Personal Data Protection Act, 2023, s. 6(4)
[458] The Indian Digital Personal Data Protection Act, 2023, s. 6(6)
[459] The Indian Digital Personal Data Protection Act, 2023, s. 13
[460] The Indian Digital Personal Data Protection Act, 2023, s. 8(7)(a)
[461] General Data Protection Regulation 2016, art 4(1)
[462] General Data Protection Regulation 2016, art 7(3)

Consent of the European Data Protection Board (2020), conditionality (the provision of a service being conditional on consent to non-essential processing) conflicts with the requirement of freely given consent. Thus, X's revised policies breached the GDPR guidelines The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), an amendment of the CCPA, creates a business-oriented but still-protective consumer law, under U.S. law. Even though the CCPA does not explicitly use the term "consent" like GDPR does, it still requires businesses to give notice at or before the time data is collected (Cal. Civ. Code § 1798.100(b))[463], and to allow users to opt-out of sale or sharing of information (§ 1798.120(a)).[464] Moreover, consumers Have the Right to Request Deletion of Their Information per § 1798.105.[465] In this case, however, the most telling thing is the requirement for a "Do Not Sell My Personal Information" link on websites, which is a positive user choice that is utterly absent from X's interface. Even in California, which has a more lenient legal framework, law culture is focused on the consumer's ongoing agency. In other words, it does not view the consumer as having made one single act of unretractable deference.

Chapter 4.3: Suggested Measures for X

Faced with ever louder public complaints and heightened user unrest, primarily from artists and creators, X has to rethink the application of its newly changed policy in relation to the use of AI data. The reaction so far, as captured in tweets by users, is not just disappointment but a deep feeling of disbelief and a sense of frustration that many of them, whose original content is the lifeblood of the platform, may be betrayed. Users have criticized the fact that consent is made out as a mere formality, that an opt-out is weak coercion. To combat this, X should prioritize building a clear, affirmative opt-in system for AI development similar to GDPR's norm under Article 7, that a consent must be freely given, specific, informed, and unambiguous. Mere platform use consent undermines trust and breaches the voluntary nature.[466]

X may also bring in graduated consent controls so users can choose to opt in or out of different types of data processing, such as AI training. Such granularity would not only be consistent with Section 6(1) of India's DPDPA[467], which requires consent to be "specific and granular," but with best practices under the CCPA, as well, where consumers must have a right to opt out of the sale or sharing of personal data. X's current requirement, a one-size-fits-all clause with no real way to object or make an informed refusal, is out of step with changing global standards. Meanwhile, basic transparency reports clarifying how user data is being used to fuel AI growth who it's shared with, what training models it's used to develop, and what precautions are taken to safeguard them, would create some measure of accountability and aid in the rebuilding of trust.

Finally, given the especially visceral anger around artists and content creators, X should also adopt a creator-first data privacy policy. This might involve a different level of consent for video, audio, or text by users given that creative IP is unique, and that the creators of same are especially vulnerable to one-sided damage from un-permissioned AI use. Open dialog with the artist community (for example, with the help of stakeholder consultations and user forums) may help clarify fairer terms. Not only would these steps help counteract reputational damage, they would also signal a true commitment to respecting user freedom and input; no matter how you do the math, X will have to make if it is to remain a legitimate participant in an increasingly consent-aware era on the Internet.

[463] California Civil Code 2024, § 1798.100(b)
[464] California Civil Code 2024, § 1798.120(a)
[465] California Civil Code 2024, § 1798.105
[466] Supra note 23
[467] Supra note17

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

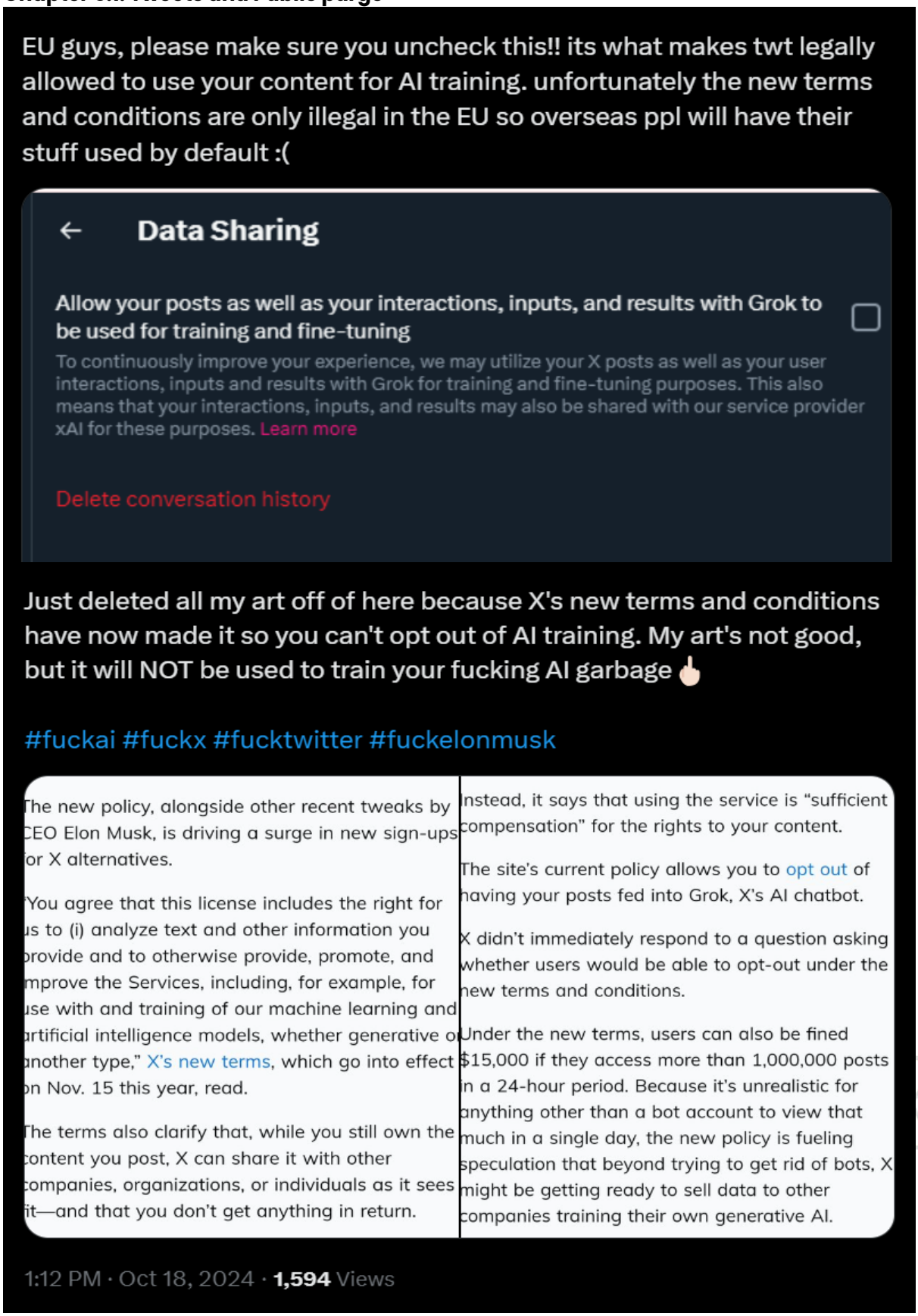
Published by

Institute of Legal Education

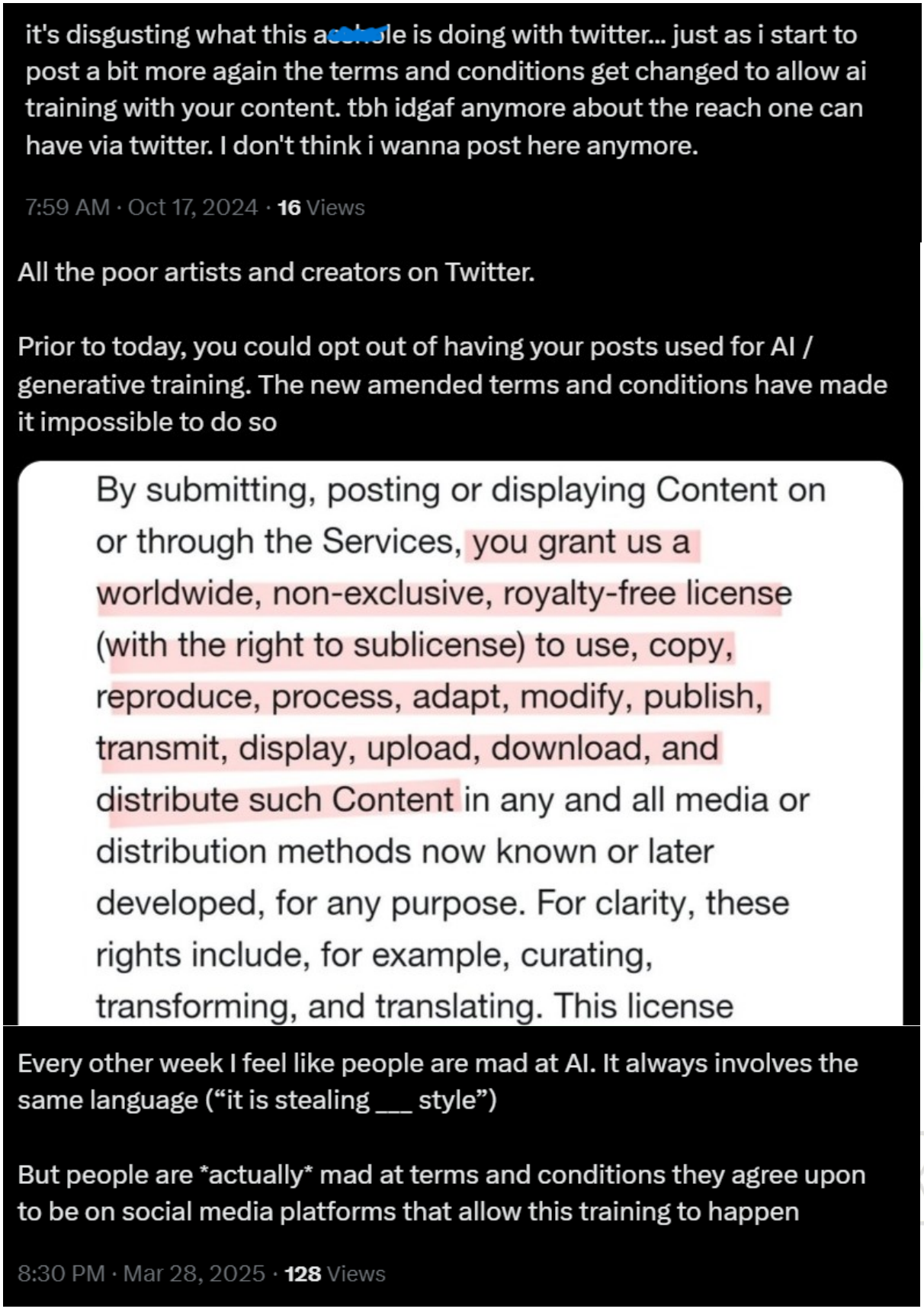
https://iledu.in

Chapter 5: Public opinions and views

Chapter 5.1: Tweets and Public purge



INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 9 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in



Public Tweets

Twitter's new 2024 Terms and Conditions have led to overwhelmingly negative reaction from the public, particularly regarding the section about allowing users' data to be collected in training artificial intelligence. Users across the site have issued forceful disapproval, such as in

multiple tweets showing amazement, frustration, and resistance. While one user responded with sarcasm regarding the company's integrity, another bluntly accused the corporation of exploiting their data. An important Tweet pointed out this harvesting was involuntary, which raises questions about the ethics of consent in the online environment. There were also tweets wherein users were actively seeking options to opt out, remove contents or even deactivate their accounts entirely. The public outrage indicates that people think the policy fails on purpose.

The negative reactions were strong especially in the creative communities. Certain tweets were specific about the threat that such terms pose to their practice since, the fear is, their creative output shared on Twitter in good faith may be re-used without attribution or control. Many digital artists worry about protecting their artworks online. People are scared of not just being stripped of their ownership, but having their artwork used to train algorithms that may replace human artwork in the future. Many artists view AI's expanding capabilities as an erasure of their creativity. Due to the ongoing debate surrounding the ethics of utilizing such data, a survey was conducted to investigate the issues and feelings of those affected by the policy change.

Chapter 5.2: Survey limitations and area

To better understand what people, think about X's revised 2024 Terms and Conditions and particularly that data could be used for AI training purposes, a survey was done with various types of questions. The questionnaire consists of only multiple-choice questions so as to better measure the views, level of awareness and personal issues. The survey has been circulated through online media like messaging channels, social networks, personal chats, etc., A total of a little over 20 answers were received. Even though the total was smaller than anticipated, the replies did include a degree of shared opinion seen online.

However, the limitations of the survey must be recognized. The small sample size limits the extent to which the results can be generalized. In addition, the results may be heavily at risk of sampling bias. First, because a good portion of the people who were probably from the same socio-digital circles. The lack of geographic diversity and the limited method of outreach may have further reduced the possibility of representation. Most of the participants appear to know about or care for issues related to AI and data, meaning that the results might already tilt negative. The survey results may not represent the definitive view of the public as a whole. However, they do provide powerful qualitative evidence. Moreover, with the more general responses that have been evident across X and the like, they point strongly to the need for further research into public opinion and data ethics in an era of generative AI.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

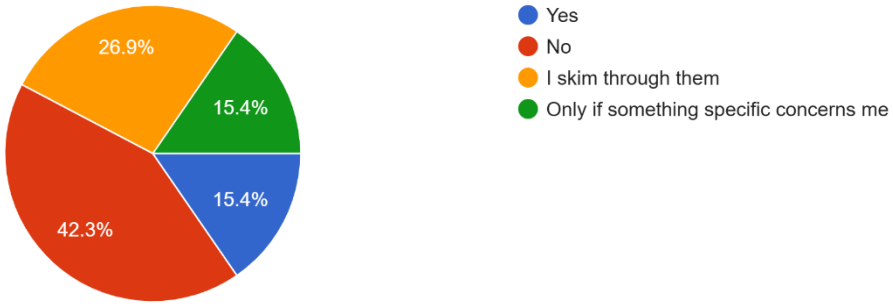
Institute of Legal Education

https://iledu.in

Chapter 5.3: Analysis and Takeaway from the Survey

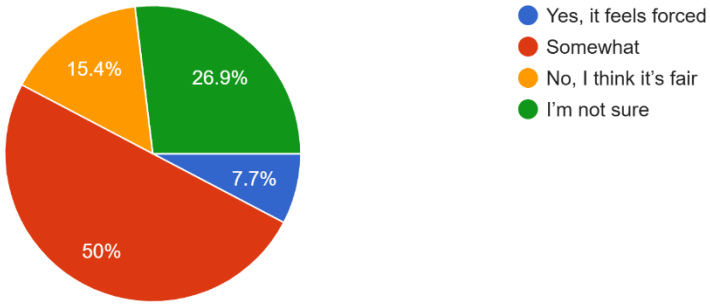
Before using X, do you read the Terms and Conditions in full?

26 responses



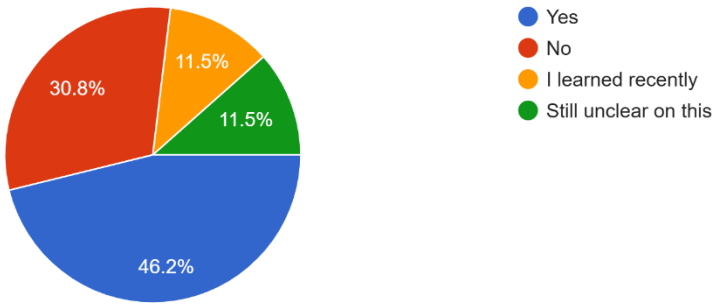
Do you feel that the current Terms and Conditions on X force you to consent to data use without real choice?

26 responses



Were you aware that your posts, replies, and media can be used to train Grok, X's AI chatbot?

26 responses



INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 9 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

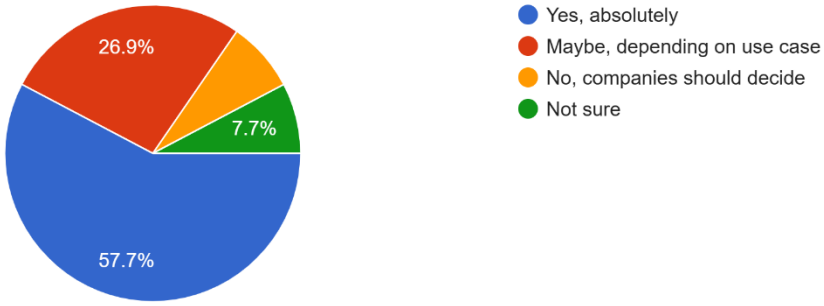
Published by

Institute of Legal Education

https://iledu.in

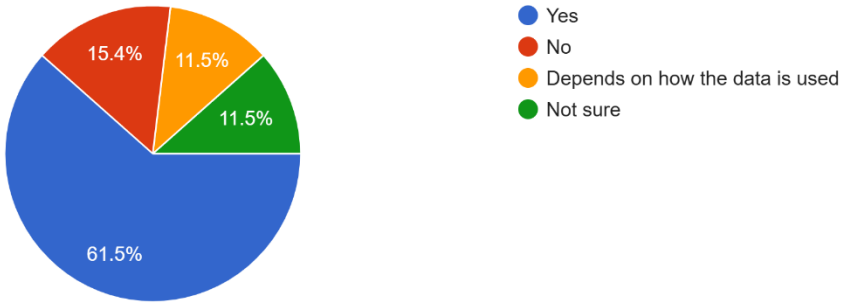
Do you think there should be legal regulations that require platforms to offer an opt-out for AI training?

26 responses



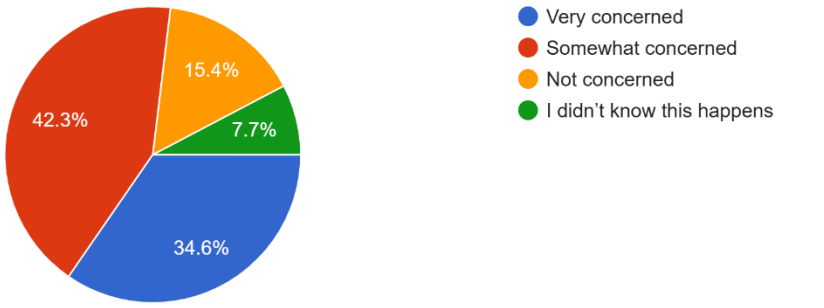
Do you believe platforms should obtain separate consent specifically for AI-related data use, apart from general Terms and Conditions?

26 responses

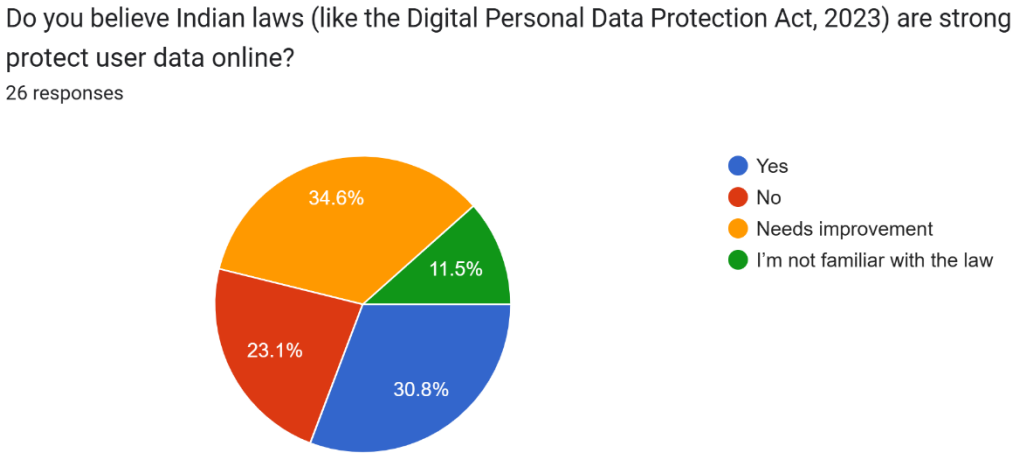


How concerned are you that your creative content (art, writing, etc.) may be used to train AI without your consent?

26 responses



INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 9 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in



Survey Response

The responses to the survey reveal a disturbing trend. Most people were either vaguely or partially aware that their information on sites like Twitter is collected for AI training. Some of the users are admitted that they have not read the new terms and conditions in full. Others, however, were shocked to find out that their tweets and media and activity will be used to train Grok. This ignorance highlights a bigger concern with digital platforms; the 'weird legal speak' and understated updates that usually go unseen by the average user. Among the respondents who claimed to be aware of the applications of personal data collection, there was a misunderstanding of the type of data that is collected and how it is used, especially for AI development.

The survey reflected emotions weighted heavily towards discomfort, distrust, and powerlessness. responses, varied in their experience of the policy. The tone of responses shifted from annoyance to resignation, with some reporting that they felt they had no choice but to agree to these terms in order to use the platform. Many expressed worries about creative theft and taking personal content, echoing frustrations already present in artist communities. These answers also indicate a growing worry about how AI models are being trained, particularly if that training is at the cost of transparency, personal control, and user orchestration.

The survey also showed us what the public feels with regard to consent and law. The majority of respondents support the requirement of affirmative consent to use their data for training AI. Many said they want opt-in procedures, not opt-out options buried deep in complicated legalese. The overwhelming opinion of respondents was that the existing laws on data protection legislation is obsolete or falls short to keep pace with the particular issues posed by the AI systems. Some interviewees indicated that besides legal reform, people also need more education regarding their digital rights such that the empowered user is the best defense against exploitation in times of algorithmic rule.

Chapter 6: Conclusion

The 2024 update of X's Terms & Conditions gives us a case study in the intensifying tussle between tech evolution and the ethical treatment of user rights over data. X has blurred the lines between acceptance and consent, by proposing that consent is an ongoing requirement rather than a one-time event. The policy change might meet the letter of the law in some places, but it violates the spirit of privacy models that value real control for users. The forceful design where platform denial raises an urgent question: can such consent be voluntary?

This consent illusion is not new. Dima Yarovinsky's conceptual work *"I Agree"* highlights the absurdity of today's digital contracts whose terms and conditions are written on colored rolls of paper similar to the ones used by large platforms. This art depicts that users do not and cannot read these terms, even less comprehend them. X is changing consent from an option to a performance in this scenario, to take advantage of users who have become comfortable and reliant on the platform to let everything through. In simpler terms, users are stuck in a system of rules they have not read or understood, and have definitely not agreed with, which makes any agreement they make meaningless from an ethical perspective.

In this context, creators, artists, and many ordinary users have taken to social media in outrage. What they are concerned about is neither the technology nor the AI itself, but it is the extractive conditions under which they are being mined for their presence, content as well as data. Artists have been particularly worrying about losing control over their work to generative models, sounding an alarm over loss of authorship in a machine-learning economy. Distrust is now so intense that people do not think about the platform as a user but a resource that it uses and extract.

Due to the seriousness of the matter, this paper sets forth a series of proposals calling on X to align its data policies with the changing needs of digital ethics. These include putting in place clear opt-in provisions for data use, establishing artist-specific data protection provisions, and increasing transparency in AI model training. A survey taken alongside this research will seek to provide further illumination regarding the depth and complexity of users' concerns rather than mere outraged surface-levels. What's revealed in this research is transparent: the future of AI is not to be constructed on soundless extraction, but rather starting with a fundamental reassertion of consent: transparent, knowing, and willing.

Reference

Books, Journals, and Conference Proceedings:

1. Rikke Frank Joergensen, "The unbearable lightness of user consent" (2014) 3 *Internet Policy Review* 1–14.
2. Ewa Luger, Stuart Moran, and Tom Rodden, "Consent for all: revealing the hidden complexity of terms and conditions" *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)* 2687–2696 (2013).
3. Sunday Author and Sunday Oladele, "Exploring User Consent Mechanisms in Data-Driven Personalization" (2025).
4. M.J. Taylor and J.M. Paterson, "Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection" (2020) 16(1) Art 4 *Indian Journal of Law and Technology*.
5. J. Abrusio, "The (In)Efficacy of Consent for the Processing of Personal Data" (2024) 6(1) *Humanities and Rights Global Network Journal*.
6. Martín Abadi et al., "Deep Learning with Differential Privacy" *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS)* 308–318 (2016).
7. Frans Coenen, "Data mining: past, present and future" (2011) 26 *The Knowledge Engineering Review* 25–29.
8. Matti Rossi, Christy MK Cheung, Suprateek ("Supra") Sarker and Jason B Thatcher, "Ethical issues and unintended consequences of digitalization and platformization" (2024) 39 *Journal of Information Technology* 390–391.

Web Sources:

1. *Twitter*, *Encyclopaedia Britannica*, available at: https://www.britannica.com/money/Twitter (last accessed on 1 May 2025).
2. Jay Peters, "X begins testing Grok, its ChatGPT-style AI chatbot, on some Twitter users", *The Verge*, available at: https://www.theverge.com/2024/1/9/24030261/grok-ai-chatbot-test-chatgpt-twitter-x (last accessed on 1 May 2025).
3. *Terms of Service*, X.com, available at: https://x.com/en/tos (last accessed on 1 May 2025).
4. *Privacy Policy*, Meta, available at: https://www.facebook.com/privacy/policy?section_id=6-HowCanYouManage (last accessed on 1 May 2025).
5. *Terms of Service: Clickwrap Agreement Sufficient to Bar Negligence Claim*, Ford Harrison LLP, available at: https://fhnylaw.com/terms-service-clickwrap-agreement-sufficient-bar-negligence-claim/ (last accessed on 1 May 2025).
6. Pluralsight Content Team, *All about ChatGPT's first data breach, and how it happened*, available at: https://www.pluralsight.com/resources/blog/ai-and-data/chatgpt-data-breach (last accessed on 1 May 2025).
7. Gregory Schwartzman, *Exfiltration of Personal Information from ChatGPT via Prompt Injection* (2024), available at: https://doi.org/10.48550/arXiv.2406.00199 (last accessed on 1 May 2025).

Statutes:

1. The Indian Digital Personal Data Protection Act, 2023
2. General Data Protection Regulation 2016
3. California Civil Code 2024