

# Digital Privacy Agreement Audit

Data 6550

William Holt, Vaishnavi Paniki, Sebastian Segura

*AI Disclaimer: The structure and formatting of this report were done with assistance from ChatGPT to save time and provide suggestions on making the report more visually appealing. In addition to this, ChatGPT helped organize a preliminary 5-minute brief based on the report to ensure the scope of the presentation matched the requirements well. All analysis and thoughts were completed by Group 1 members and not by any artificial intelligence.*

## Introduction

This project analyzes how companies collect, share, and protect their users' data, and how their private policies line up with major regulatory bodies like GDPR, CCPA, and VCDPA. The eight platforms analyzed in this project represent a variety of company sizes and service types, specifically social media and e-reading platforms. This project highlights critical gaps in user protections which are often agreed to without reading in full. The average American has agreed to over 250 private policies without reading any of them. A typical privacy policy takes about 20 minutes to read and requires a very high reading level. This highlights a disconnect between the user agreements and those who are meant to read them. We aim to analyze agreements we have signed to compare their practices, assess regulation compliance, and evaluate what they do with their collected data.

## Overview of Services

Our analysis covers eight digital services from two categories:

### *Social Media*

1. Instagram – a social networking service owned by Meta
2. TikTok – a video hosting service owned by ByteDance
3. X – a microblogging service
4. Facebook – the largest social media platform owned by Meta

### *E-Reading*

5. Apple Books – Apple's e-book reading and store
6. Kindle – Amazon's e-book reader and marketplace
7. Nook – Barnes & Noble's e-reading platform
8. Kobo – Rakuten's e-reader and bookstore

This selection covers specific industries across varying company sizes and geographic regions to provide a broad view of privacy practices in the digital world.

## Key Findings from Comparison

### *Agreement Complexity and Readability*

All services analyzed employ privacy agreements which call for a college-level reading comprehension, with times ranging for 14 minutes (Instagram) to 33 minutes (X). This high reading level stops many users from attempting to read what they are agreeing to, specifically for companies like TikTok or Instagram which are geared towards younger users. As far as complexity goes, the social media platforms X and TikTok had the longest agreements with each containing over 7,000 words. The longest of the e-reader policies was Kindle, with 7,000 words and the rest coming in far below that tally.

### *Data Collection*

The social media platforms collect a wider variety of data than the e-reading services. E-reading devices primarily collect device information, purchase history, and reading behavior to enhance the user experience. The social media platforms collect extensive behavior, biometric, location, and interaction data, raising red flags for those with the ability to comprehend their agreements. The Meta companies collect the broadest range of data, including cross-platform activity across all Meta products. TikTok is not far behind, extensively collecting biometric and voice data. The e-reading platforms have more focused data collection which generally remains relevant to their core service. Apple Books collects data but integrates it only within Apple's services. Kobo's collection is limited to purchase history and reading preferences, making it the least invasive of the eight.

### *Data Sharing*

All the services analyzed share data with third parties to differing levels. Social media platforms share data much more broadly with advertisers, analytics firms, and partners. Meta services share data across their platforms to create a comprehensive user profile. Similarly, Amazon does the same with its collected Kindle data. Apple Books and Kobo gave the most transparent description of their data sharing practices, while TikTok and X stick to very ambiguous language regarding the extent of their data sharing.

### *User Rights*

All services provide access, deletion, and correction rights due to GDPR and CCPA requirements. However, Apple Books stands out as the easiest user controls while X and Amazon have very complex methods of opting out. Only Apple Books, Facebook, and

Instagram offer clear opt-out options for targeted advertising, while the other companies hide this option in settings or references to other external policies.

### *Regulatory Compliance*

All companies claim to follow GDPR, yet Apple Books and Kobo again stand out with strong compliance and clear, detailed data rights. Most services complied with basic CCPA requirements, but specific disclosures were often hard to locate or missing. For VCDPA and other emerging regulatory policies, there was minimal specific compliance, and these smaller policies were rarely mentioned if at all.

## Detailed Service Analysis

### *Social Media Platforms*

1. Instagram – This policy comes in at 3,512 words, approximately 15 minutes to read at a college level. They collect extensive user data including account information, behavioral data, location data, content, and advertising interactions. This data is shared across all Meta products. Third-party partners, advertisers, analytics firms, and law enforcement as needed. Instagram provides account deletion options but provides no control over specific data elements. Users may opt-out of targeted ads but are unable to opt-out of data collection or integration with other platforms. They protect your accounts behind encryption, access controls, and two-factor identification for login purposes. Instagram is partially compliant with CCPA and has not addressed VCDPA or CPA requirements. Notably, Instagram focuses on monetization of user data through its extensive cross-platform integration while maintaining much control to remove user content at will.
2. TikTok – TikTok’s policy is 7,051 words, which takes a college-reading leveled person 30 minutes to read. They collect personal identifiers, user content, behavioral data, device information, location data, and biometric/ and voice data which they share with the ByteDance corporate group, third-party service providers, advertisers, and law enforcement. TikTok offers data and account deletion options but with limited user controls, providing no general opt-out from data collection (exceptions being California minors). TikTok has dedicated security teams which provide encryption, anonymization of information, internal access controls, and audits for their systems. They do not follow state privacy regulations beyond basic CCPA provisions. Notably, TikTok does not disclose their AI training uses clearly while simultaneously extensively licensing user content.
3. X – Taking 33 minutes to read at 8,383 words, X’s policy is full of complex legal terminology. It outlines the collection of text, photos, videos, location data,

technical data, interaction data, and how it uses content for machine learning training. X shares its data with advertising partners, analytics services, law enforcement, and AI model developers and provides account deletion options without granular data controls for the user. X offers a bug bounty program alongside other extensive security measures and maintains minimal compliance with emerging state regulations. X uses user data to train AI models and imposes significant legal limitations on user rights.

4. Facebook – This user agreement is 6,500 words and estimated 25 minutes to read. Facebook collects profile information, connections, content interactions, device information, purchase activity, third-party integrated data, facial recognition, and off-platform activities and shares this data with all the Meta applications, advertising partners, measurement partners, vendors, service providers, researchers, and law enforcement. Facebook offers users the right to view their collected data, download personal information, and permanent account deletion, along with offering opt-outs for targeted advertising and facial recognition but limited controls for cross-platform data sharing. Facebook offers all the same security measures as the first three companies in addition to more enhanced suspicious activity detection. Facebook complies with GDPR and CCPA requirements but has not addressed newer state regulations. Notably, Facebook maintains extensive user profiles by combining on and off platform data and uses this data for AI training without in-depth disclosure or compensation.

#### *E-Reading Platforms*

5. Apple Books – Apple Book's agreement has 5,000 words and would take 20 minutes to read. It outlines collection of device information, purchase history, and browsing activity within the store platform which is shares across Apple's applications and services and to third-party advertisers. Apple provides user rights to access, correct, and delete their data through Apple's privacy dashboard and offers straightforward opt-out from targeted ads within the device. They are in firm compliance with GDPR and CCPA requirements. Apple is known for data sharing across iCloud and its other services but maintains transparent data practices compared to other platforms.
6. Kindle – The Kindle agreement is about 7,000 words and would take 25 minutes to read. It outlines the data collection of user purchase history, browsing data, device ID, location, and reading behavior to share with Amazon partners for marketing and service improvement. Kindle provides access, deletion, and opt-outs of targeted ads through difficult navigation of Amazon's settings. Kindle provides standard Amazon security protocols and maintains GDPR and CCPA basic requirements.

Amazon fully integrates Kindle data into its ecosystem to create consumer profiles across shopping and reading behaviors while maintaining ownership of the books on the user's device.

7. Nook – Barnes & Noble's Nook e-reader user agreement is 6,000 words and details collection of purchase history data, device data, browsing behavioral data, and how it is shared with Barnes & Noble affiliates for marketing purposes. Nook provides access, deletion, and correction options through their Barnes & Noble account settings and has no named opt-out method. They implement standard encryption and access controls along with basic compliance with GDPR and CCPA requirements. B&N combines digital reading data with physical store purchase data for marketing purposes.
8. Kobo – Kobo's agreement is 5,500 words long and details collecting account information, device details, purchase history, and reading patterns to share with Rakuten affiliates, analytics providers, and third-party partners. Kobo offers data deletion and control, opt-out from marketing communications, and basic controls over reading analytics, as well as secure user authentication and access limitations. Kobo follows GDPR and CCPA. Kobo is also the most transparent of the e-reading platforms about its reading analytics collection and provides clearer purpose statements for its data collection.

## Regulatory Compliance Assessment

GDPR – All eight services claim compliance, although the extent to which they comply differs amongst them. Apple Books and Kobo are the most comprehensive with clear data subject rights, purpose and limitation statements, and transparent data processing practices. Facebook, Instagram, and Kindle meet basic requirements but have very complex user agreements with less transparency about their data sharing. TikTok, X, and Nook minimally comply thanks to their vague language around data purposes and international transfers. Across all platforms, there is predominantly vague and complex language surrounding their data usage.

US Privacy Law – Apple Books again stands as the most in compliance by including California-specific rights sections and straightforward opt-outs. The rest either don't mention California law or bury it within larger sections making the language hard to find. None of the services analyzed address any newer state regulations or emerging privacy laws. This is a signal for US privacy laws to continue to evolve in hopes of protecting their citizens data.

## Comparison Matrix

Company	Length	Time	Collection	Sharing	Rights	Opt-Out	GDPR	CCPA	Key
Instagram	3512	14 mins	Account info, behavioral data, location data, content, interactions	Meta apps, advertisers, analytics firms, law enforcement	Access, deletion	Targeted ads, account deletion	Partial	Partial	Cross-platform data used for monetization
TikTok	7051	28 mins	Personal info, content, behavioral data, biometric data, location data	ByteDance group, advertisers, law enforcement	Deletion of data and account	Opt-out for CA minors	Minimal	Minimal	Content licensing
X	8383	33 mins	Text, photos, videos, location data, interactions	Ad partners, analytics, law enforcement, AI developers	Account deletion	Limited controls	Minimal	Minimal	AI model training, no content liability
Facebook	6500	26 mins	Profile data, connections, interactions, off-platform activity	Meta ecosystem, ad partners, vendors, researchers	Access, download, deletion	Targeted ads, facial recognition	Moderate	Moderate	User profiles, AI training
Apple Books	5000	20 mins	Device info, purchase history, browsing activity	Apple ecosystem, third parties	Access, correction, deletion, portability	Clear opt-out for ads	Strong	Strong	Integration with all Apple Services
Kindle	7000	25 mins	Device info, purchase history, device ID, location, reading behavior	Amazon partners	Access, correction, deletion	Complex opt-out processes	Moderate	Moderate	Amazon ecosystem integration
Nook	6000	22 mins	Purchase history, browsing data, location data, reading patterns	B&N affiliates	Access, correction, deletion	No opt-out	Basic	Basic	Includes physical store data
Kobo	5500	21 mins	Account info, purchase history, reading patterns	Rakuten affiliates, analytics providers	Access, correction, deletion	Marketing opt-out	Good	Basic	Great transparency

## Recommendations for Improvement

Based on our analysis, we propose the following recommendations to improve privacy agreement practices:

1. Improve readability and accessibility by simplifying language, including visual elements, and detailing age-appropriate versions for teens or younger users.
2. Increase transparency by listing specific data elements collected, specify use limitations and purposes behind each collected data point, and name the third-party data partners and their usage purposes.
3. Enhance user controls by centralizing privacy dashboards, allow selective consent by users, and simplify opt-out mechanisms by making them easy to find and use.

## Lessons Learned

Our analysis revealed many important insights about the ethics of data privacy. First, there is a massive gap between the complexity of the agreements and the average user's reading skills. This creates a disconnect between actual informed consent and presumed understanding. Second, the patchwork approach of US state laws is making it difficult for companies to comply with global privacy demands. If the US wants to have as much of an impact at GDPR, it must find a way to unite the needs of its people. Finally, the privacy paradox remains an increasing problem despite an increase in awareness on the subject. Users will continue to accept agreements without reading them, which highlights the need for structural solutions, rather than individual ones.

## Conclusion

Our analysis shows that digital privacy regulations have failed to significantly alter the underlying issues driving ethical data usage. While they may have improved practices overall, there remains a significant gap between legal compliance and actual user understanding. This distance is explained by understanding the business models and decisions which shape private policies, rather than a code of ethics. Advertising revenue takes the front seat and is protected by ambiguous and complex language, while genuine and informed consent takes a back seat. Hopefully soon, privacy policies will be seen as tools of education for users and not just another annoying checkbox to initial before you can get on your Kindle.