Privacy Analysis

*Will Holt, Sebastian Segura, Vaishnavi Paniki*

Title (see page 2 for various notes)

Names

Class and date

Intro section*Introduction*

*Our analysis focuses on how these companies collect, share, and protect user data and how these privacy practices align with major regulations such as CCPA, GDPR, and VCPDA.  These platforms represent diverse cross-section of service types and company sizes which range from the big tech companies to the more traditional companies that offer retail-based digital offerings. The project aims to highlight the industry standards to identify gaps in user protection.*

Overview of each service analyzed

Key findings from each service

Regulatory compliance assessment

Recommendations for Improvement

Put ideas and notes here

Example table template:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Company | Agreement Length | Est. Reading Time | Data Collected | Data Sharing | User Rights | Opt-Out Options | GDPR | CCPA | Other Notes |
| Apple Books | ~5,000 words | ~20 mins. | Device information, purchase history, browsing activity | Apple’s ecosystem, third party ads and services | Access, correction, deletion, portability | Opt-out of targeted ads | yes | yes | Tracks data across all Apple servies (e.g. iCloud) |
| Kindle | ~7,000 words | ~25 mins. | Purchase history, bowsing data, device ID, location | Shared with Amazon partners for marketing and services | Access, deletion, data portability via Amazon account settings | Opt out of targeted ads | yes | yes | Full integration with Amazon’s broader data collection practices |
| Nook | ~6,000 words | ~22 mins. | Purchase history, device data, browsing behavior | Shared with Barnes & Noble affiliates for marketing | Access, deletion, corrections via B&N account settings | No named opt-out method, targeted marketing across B&N apps | yes | yes | May include physical store data collection in broader marketing |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sno** | **Company** | **Agrement Length** | **Estimated Reading Time** | **Data Collected** | **User Rights** | **Opt Out Options** | **Notable Observations** | **Data Shared** | **Security Measures** |
| 1 | Instagram | 3512 words | ~14 mins | Name  Username  Email  Phone  Posts liked  Accounts followed  Time spent  Device identifiers   IP address  Geolocation  Photos  Videos  Captions   Comments  Ads interactions | Account Deletion | Targeted Ads    Account Deletion | Cross-platform data use    Monetization    Platform powers to remove user posts | All Meta products,    Third-party partners,     Advertisers,     Analytics firms,    Law enforcement | Uses encryption and security protocols    Implemented access controls to access to user data.    Two-factor authentication (2FA) or users. |
| 2 | Tik Tok | 7051 words | ~28 mins | Name  Contact info  Videos  Sounds  Images  Likes   Shares  Interactions.  Device info  location info  Biometric  Audios   Voice data | Data Deletion    Account Deletion | Data Deletion    Account Deletion | Licenses User Content    Users can't opt from significant data processing | All the ByteDance corporate group,    Third-party service providers,    Advertisers,    Law enforcement | Uses data encryption and anonymization is used for sensitive user information.    Implemented Internal access control and security audits.    Has dedicated security teams to monitor threats and enforce compliance. |
| 3 | X Twitter: | 8383 words | ~33 mins | Text   Photos  Video  Location  Technical details  ML training with user content  Interactions with X services | Account Deletion | Account Deletion | User data to train Ai Models    Content Liability    Limited Legal Rights | Advertising partners,     Analytics services,    Law enforcement,     AI model developers | Organisational firewalls and access restrictions for user data.    Offers 2FA for user account protection.    Applied rate limits and abuse detection systems to prevent misuse.    Has a bug bounty program to identify vulnerabilities. |

Summary of my section:

I focused analysis on Apple Books, Nook, and Kindle to compare their user agreements, data practices, and regulatory compliance. These platforms all collect similar data, including device information, browsing data, and purchase history. The depth and specifics of their data collections differ between the three. Apple Books is integrated into Apple’s broad ecosystem, while Kindle and Nook focus more on reading-specific data. All of the services allow users to exercise their data protection rights, with Apple Books offering the most user-friendly opt-out methods, thanks to its larger integration into Apple’s systems.

Key Findings of my section:

Nook, Kindle, and Apple Books all collect purchase history, device information, and browsing data. While Apple Books focuses more on integration with its ecosystem (such as iCloud data), Kindle and Nook gather more specific usage data tied to books and reading habits. All three platforms allow users to exercise certain rights like access and deletion of their data through differing methods, with Appl Books having the easiest opt-out mechanism, as its settings are directly tied to your Apple account.

Regulatory Compliance Assessment of my part:

All three services comply with GDPR to varying degrees. They allow users to access, correct, and delete their data at will. For CCPA, all services are compliant. Amazon, however, is prone to make users jump through hoops to fully exercise their data rights compared to the much simpler Apple Books.

My contribution to Recommendation for Improvements section:

Simplify user rights to cultivate an environment where people know what they can do with their rights, unlike Amazon which often complicates the processes.

Improve opt-out laws to combat complicated or difficultly navigated application settings to make it easier for individuals to find out how to opt out of data sharing or targeted ads without jumping through hoops.

Lessons Learned for my section:

Many digital services are intentionally vague in communicating the extent of their privacy practices and often are too complicated for the common user to understand what they have signed up for. Transparency and more layman terminology should be employed to combat this. Global services have a much more complicated patchwork of international regulations to follow, making compliance a challenging and expensive task. Global corporations have a much more difficult time operating in compliance. Hardly anyone cares to read user agreements, and despite an increasing level of awareness related to invasive privacy issues, more and more users sign away their rights. This highlights the need for more education around privacy rights aside an increase in simpler user interfaces to help users make informed decisions.

Vaishnavi   
I did this according to the instructions , if there is anything wrong or add or edit please let me know.

**1. Instagram:**

1. Complexity of the Agreement:

1. This document is somewhat difficult to read. It does not feature very heavy legalese; however, it uses technical language and vague legal disclaimers.
2. The reading level estimation is approximately at the college-level. It would take a good bit of strain for most users, especially teenagers, who are the audience most heavily targeted by Instagram, to fully understand.
3. **Areas of concern:** Largely, this includes passive voice and abstract legal terms. These, in addition to long sentences and large blocks of text, contribute to less clarity. Many important rights or exceptions (such as data use, license to content) are embedded within long paragraphs.

2. Compliance with U.S. Data Privacy Laws:

|  |  |
| --- | --- |
| **Law** | **Observations** |
| **California Consumer Privacy Act (CCPA)** | Partially compliant. A general privacy policy is found on Meta, with opt-out options and access/delete rights, but not as fine-grained as CCPA might ideally want it to be. |
| **Virginia Consumer Data Protection Act (VCDPA)** | Ambiguously addressed. There is some consideration on the part of the user over his or her data - whether they can opt-out and delete it. “Opt-out of processing for targeted advertising” is missing in the former term though. |
| **Colorado Privacy Act (CPA)** | Somewhat addressed. It is similar to the above: a general compliance (delete, access, correction), without mentioning anything specific to rights under Colorado law or to the roles, controller/processor. |
| **Emerging State Regulations** | Inconsistently addressed. Specific laws such as Connecticut or Utah's regulations are not mentioned. Compliance seems to be based most on the overarching Meta Privacy Policy as opposed to this Terms doc alone. |

3. Types of User Data Collected

1. While there is detailed mention of data collected here, inferred data includes:
2. Account info: Name, Username, Email, Phone.
3. Behavioural data: Posts liked, Accounts followed, Time spent.
4. Device/location data: Device identifiers, IP address, Geolocation.
5. Content metadata: Photos, Videos, Captions, Comments.
6. Interaction with ads and brands.

4. Opt-Out Options

1. Opt-out of ad targeting is included.
2. There is no opt-out from data collection itself within this Terms document.
3. Everything uploaded to the system is not obtainable by opt-out - uploading content gives Instagram a wide license (worldwide, sub-licensable, royalty-free).
4. Opt-out from automated decision-making/AI is not provided.

5. Notable Observations

1. Monetization: Meta has publicly stated that your data is being used to fund the platform by way of advertisements; however, they play down the possible risks involved.
2. Cross-platform data use: Data from different Meta products increase exposure for users and centralization of data.
3. Content Ownership: You own your content; however, Instagram has a wide-ranging license to use it.
4. Surveillance ability: On certain "security" grounds, the content could be shared with law enforcement in some instances or be indefinitely retained.
5. Platform powers: Instagram has the power to remove any content, change the username from any account, and suspend or terminate any account with or without cause.

Instagram's terms should be made simpler to improve accessibility to younger audiences by using clearer, more concise language. In important concepts such as data sharing, content licensing, and user rights, they simply bury users in dense paragraphs. In an effort to comply with state privacy laws, Instagram should have an easy-to-use privacy dashboard with opt-out controls, especially for targeted advertisements and data sharing. This will additionally enhance user trust and transparency under the law by stating explicitly that Instagram is in compliance with state laws such as the CCPA, VCDPA, and CPA.   
 

2. X: Twitter:

1. Complexity of the Agreement:

Reading Level: Reading levels are at a college setting, somewhat like Instagram but with a legal and much denser structuralism.

Clarity: It's certainly plain in some parts; but in others, it has Complex clauses, technical legal disclaimers, buried with permissions-special in content licensing and liability. Very difficult. For the most part, normal human beings can't understand it without prior knowledge of law or technology.

2. Compliance with U.S. Data Privacy Laws:

|  |  |
| --- | --- |
| **Law** | **Observations** |
| **California Consumer Privacy Act (CCPA)** | Partial Compliant, Data use and deletion are mentioned in the Privacy Policy, but mention is not found by a specific CCPA section or ease-of-availability opt-out. |
| **Virginia Consumer Data Protection Act (VCDPA)** | Minimal Compliant, The assigned right, for example, is not one in particular to opt out of data processing, the right to appeal, or so on. |
| **Colorado Privacy Act (CPA)** | Minimal Compliant, There is no such reference in either relation to universal opt-out or purpose limitation. |
| **Emerging State Regulations** | Not Compliant, Regarding compliance with any other state rules upcoming in the future, none were mentioned. |

**3. Types of User Data Collected:**

While there is detailed mention of data collected here, inferred data includes:

1. **User content**: Text, Photos, Video, etc.
2. **Behavioral data**: how user interact with services
3. **Device data**: Location, Technical details
4. **Biometric & AI data use:**Iis implied under “machine learning” training with your content.
5. They reserve the right to share, adapt, and distribute this data globally.

**4. Opt-Out Options:**

1. There is no complete opt-out of data collecting.
2. There is no clear way one can be excluded for the data being used in machine learning/AI training.
3. A person may be able to access certain personalization through ad settings, but that option is not mentioned here.
4. Anytime, one can deactivate his or her account.
5. Poor visibility of opt-out mechanisms for core tracking and data use compared to upcoming laws.

**5. Notable Observations:**

1. This is AI Use: This content can be used to train AI systems (including generative AI) and have neither opt-out nor compensation available.
2. License Your Content: All users grant a global and royalty-free sublicensable license to all content, including reposting, translating, and all other uses in all media.
3. Content Liability Transfer: You remain fully responsible for your posts even if someone misuses them.
4. Limited Legal Rights: Users waive most damage rights; liability will be capped at $100 for the event or at what you paid for 6 months.
5. Liquidated Damages-from access to 1M+ posts/day.

The X platform should define in clear terms how user-generated content is utilized in AI training and give such users an option to opt out. The company's terms and conditions are complex legal jargon that grants huge licenses over user content with little if any, compensation to the user and no clear restraints. Greater transparency can be achieved by including a clear statement of compliance with relevant U.S. privacy laws, along with simpler controls for user data. Including reasons for moderation decisions and increasing mechanisms for dispute resolution would benefit platform fairness and accountability.   
 

3. Tiktok:

1. Readability & Complexity:

1. Reading Level: These types of content are written at a level that requires some readings at the University level (Grade 14 and beyond)- critical complexity with technical terms and very-long sentences.
2. Legal Jargon: High. Many uses of words like royalty-free, non-exclusive license, waiver of rights, and so on.
3. Liberation in its accessibility: Not really friendly at all to younger audiences, even if TikTok-mania among teens is thriving.
4. Complex and dense, definitely not easy for average users (especially under 18) to understand.

2. Compliance with U.S. Data Privacy Laws:

|  |  |
| --- | --- |
| **Law** | **Observations** |
| **California Consumer Privacy Act (CCPA)** | Partial Compliant, In the Privacy Policy, mentions of Data use and deletion are there for Partial Compliance, but there is no reference regarding disclosing CCPA specifically or simply ease-of-availability opt-out. |
| **Virginia Consumer Data Protection Act (VCDPA)** | Minimal Compliant, The assigned right, for example, to the right no longer to be a person with an objection to the processing of data, to give appeal rights, and so forth. |
| **Colorado Privacy Act (CPA)** | Minimal Compliant, No direct mention of universal opt-out or purpose limitation is made for any of the working documents. |
| **Emerging State Regulations** | Not Compliant, It was pointed out that no other state legal requirements were actually discussed and required. |

While TikTok does fulfill minimum privacy requirements, particularly for being in California, it is not fully transparent about how it complies with other newer state-level laws.

**3. Types of User Data Collected**

While there is detailed mention of data collected here, inferred data includes:

1. **Personal identifiers**: Name, Contact info
2. **User content**: Videos, Sounds, Images
3. **Behavioral data:** Likes, Shares, Interactions.
4. **Device & location info**
5. **Biometric/audio/voice data**    
      
   TikTok may use the content of its users in AI systems or monetize it without any compensation rendered to the users.

**4. Opt-Out Options**

1. The Terms contain no general opt-out from data processing or personalization.
2. California minors may ask for the removal of their content.
3. Data deletion and account deactivation may be requested.
4. Ad control and tracking details are described, but these are deeply buried in external policies.
5. Control over how TikTok uses or monetizes its data is not clear or straightforward for users.

**5. Notable Observations:**

1. License User Content: You grant TikTok an identity license for the entire world and forever create royalty-free use, alteration, distribution and commercializing for your content.
2. No sharing of revenue: Even if TikTok earns using your content-e.g., advertisements, AI-you get nothing in return.
3. AI Use Not Disclosed: This grants a license to content to serve for training purposes or model uses.
4. Not opting from significant data processing: A modern red flag under privacy standards.
5. Disputes: Must be resolved in California courts, and claims must be filed within 1 year.
6. General limits on content: Long list of forbidden behaviours and topics, from identity impersonation to offensive material.

      TikTok's agreement should ensure user rights protection and transparency in respectdata collection, especially among minors and biometric data. The content license that is surprisingly broad is offered solely to TikTok for reuse of all works; therefore, users should be granted rights to reuse their content, including reuse for AI training. TikTok must explicitly refer to U.S. state privacy laws, offer a much clearer mechanism for easy access to opt-outs from targeted advertising, and data-sharing arrangements to improve compliance. Simplifying the heavy legal jargon will further make it easier on the end user.

Privacy Analysis

*Will Holt, Sebastian Segura, Vaishnavi Paniki*

*Introduction*

*Our analysis focuses on how these companies collect, share, and protect user data and how these privacy practices align with major regulations such as CCPA, GDPR, and VCPDA.  These platforms represent diverse cross-section of service types and company sizes which range from the big tech companies to the more traditional companies that offer retail-based digital offerings. The project aims to highlight the industry standards to identify gaps in user protection.*