Harper Kates
4/11/25
DATA 6550
Dr. John Wallin

Analysis of 3 End-User License Agreements

● Anaconda Navigator:

Anaconda Navigator is a useful tool for computer programming, containing tools like Jupyter Notebook, allowing users to write Python code into a notebook. This is no doubt useful, but since it is a data-driven software, its end-user license agreement inevitably covers topics like data collection, data privacy, and update procedures. Furthermore, the EULA itself is 25 pages long, which means that the vast majority of people who agree to use this software did not bother to read the full agreement. This can be problematic, as many times, long agreements like this can contain controversial policies on data usage and privacy. Here is an overview of the EULA, spanning 5 different topics.

- Data Collection:

In Anaconda Navigator's privacy policy, they list many types of data that can be collected. These include [2]:

- Personal Identifiers: name, email address
    - If applying for job: date of birth, gender, government ID, passport/visa, legal work eligibility status
- User Credentials: username, password, profile picture
- Payment Information: billing address, records of past payments, company size
- Business Information: user's role in organization

- Employment Information: job title, department, compensation, benefits information, educational history, employment/military history, former disciplinary actions, training records
- Usage and Metadata: activity logs that track usage of specific services
- Device Information: web browser used, OS, IP address, geo-location
- User-Generated Data: texting, social media activity, file metadata
- Third-Party Information: includes social media activity, phone directories, government records, etc.

While most of these categories do not apply to the average user, categories such as usage data, system information, and application logs apply to almost everyone with the software. This means that most people who use Anaconda Navigator are having their data collected in some way. There are many reasons why this software collects user data, including [2]:

- Providing Services: includes product support services, product updates; can possibly access billing data for new software agreements
- Personalization: user preferences/settings
- Improving Software's Services: identify areas for improvement
- Send Communications: includes software updates, promotional offers, etc.
- Research and Development: collects data on how user uses software via surveys, questionnaires, interviews
- Security: protect from cyber-attacks or unauthorized access
- Compliance With Legal Requirements: responding to government requests

While some of the types of data being collected by the software may seem relatively invasive, most of the data collected from the average user is relatively harmless, as most data involves the user's interaction with the software instead of personal information. Furthermore, it helps that the EULA clearly delineates a variety of reasons why user data may be collected; if these reasons are left from the public, this may be a sign that the company may be using the data in an unethical manner.

- Data Sharing:

The privacy policy states that users' data may be shared with third-party service providers. In section 3.1, the agreement states that many of these third-party service providers are known as "sub-processors." These are third-party companies that process data on behalf of another company; in this case, they process data on behalf of Anaconda. Types of data analysis these "sub-processors" can perform include, but are not limited to: "software support services, contract management services, sales support services, software training services, benefits administration, human resource compliance, and management platform, employee stock options management platform, and in-office communications system," [2]. Additionally, according to GDPR, these "sub-processors" must be disclosed in a public list, and they must ensure that each sub-processor upholds data protection standards similar to Anaconda. These specific obligations include processing data only as instructed by Anaconda, securing data via encryption access controls, and audit logs, and ensuring confidentiality of personal data. Compliance with data privacy laws such as GDPR is a key component of data-driven software that can be trusted.

- User Rights/Opt-Out:

Anaconda's user rights depend on the country or state of origin of the user. For example, the GDPR gives users the right to restrict data processing, while California's CCPA agreement does not. Here is a full table showing the status of each user right in Europe, California, Canada, and Brazil:

User Right	Europe (GDPR)	California	Canada	Brazil	Supported in Policy
Right to Access	Yes	Yes	Yes	Yes	Yes
Right to Rectify	Yes	Yes	Yes	Yes	Yes
Right to Erasure	Yes	Yes	Limited	Yes	Yes

Right to Restrict Processing	Yes	No	No	Yes	Limited
Right to Object Processing	Yes	No	No	Yes	Limited
Right to Data Portability	Yes	No	No	Yes	Varies by System
Right to Opt Out of Sharing	N/A	Yes	No	Yes	If Applicable
Right to Limit Sensitive Data Use	Yes	Yes	No	Sometimes	Limited
Right to Withdraw Consent	Yes	Yes	Yes	Yes	Yes
Right to Avoid Automated Decisions	Yes	No	No	Limited	Limited
Right to File Complaint	Yes	Yes	Yes	Yes	Yes
Right Against Retaliation	Yes	Yes	No	Yes	Yes

- Update Policy:

Lastly, Anaconda may update the privacy policy after making changes; this seems likely with the development of AI. Anaconda is under obligation to notify users about the update, and include a “last updated” or “effective date” line before the policy begins. As of April 11, 2025, the policy was last updated on May 3, 2024.

- Nintendo Switch:

The latest Nintendo video gaming console, the Nintendo Switch, has been one of the best-selling consoles in history, selling over 150 million units in total and peaking at 28.83 million units in 2021 [5]. However, Nintendo has always been notorious for doing whatever it takes to protect its intellectual property, especially when dealing with video game emulators, mods, and fan-made games [6]. Here is an overview of the Switch's EULA:

- Data Collection:

Nintendo has the right to collect personal information, including name, email address, and payment details [7]. It also collects console usage data, such as which games are being played and how long each game is played for, as well as console performance and functionality metrics. While Nintendo is not as data-driven of a company as Anaconda Navigator, there are still many ways in which this data collection can be useful for the company. Examples include improving upon Nintendo's services, enhancing user experience, ensuring security, and complying with legal obligations. These reasons for data collection are almost the exact same as in Anaconda Navigator; one can make the assumption that these are the default reasons for user data collection that many companies choose when forming an EULA.

- Data Sharing:

Nintendo mainly shares user data with Nintendo affiliates; mainly Nintendo subsidiaries for various countries or regions. Data that may be shared with these affiliates include: account information, usage data, device and performance data, and support inquiries. The main reasons for sharing this data mainly fall into one of three categories: customer support, global services, and regulatory compliance. Compared to Anaconda, Nintendo does not share as much personal data, and since it only shares with Nintendo affiliates, it does relatively well with protecting user data. However, as explained earlier, users of Nintendo products do not have as many rights as in other privacy agreements.

- User rights:

The main point of Nintendo's sale of their products is that the software is "licensed, not transferred to you," [4], which means that users may not necessarily "own" the product like any other typical consumer product. This severely limits the rights that users have when using the software, including, but not limited to [4]:

- Users cannot use the software for commercial use.
- Users cannot modify or reverse-engineer the software.
- Users cannot use any software not authorized by Nintendo.
- In some cases, system updates must be accepted to use the software.
- Nintendo has the right to make the system unusable if any rules in the EULA are violated.
- Users cannot use the system to threaten Nintendo's intellectual property (Nintendo uses "threaten" very loosely)

An example of Nintendo being extremely protective of their intellectual property can be seen in the case of fan-made games, including AM2R (an unofficial remake of Metroid II) and Pokemon Uranium (a highly acclaimed fan-made game). Despite these games being generally well-received by the public, in August 2016, both of these games were discontinued under legal pressure from Nintendo [6]. This is different from what other video game companies do, as most video game companies (example: Riot, Bethesda, Valve, Sega) have specific guidelines on fan-made games, while Nintendo outright bans all fan-made games entirely [6]. Again, this goes back to the main point of buying a Nintendo console; the agreement states that the console is still technically owned by the company, not the consumer, so the "consumer" has to be extremely careful not to violate any rules in the EULA.

- Opt-Out Policy:

As for the opt-out component of owning a Nintendo Switch, Nintendo keeps it very simple: for most parts of the EULA, it is impossible to opt out. The only exception is the arbitration/class waiver portion, which is for consumers who intend to sue the company via class-action lawsuit instead of private arbitration. The consumer must send a physical letter

proclaiming their intention to opt out of the arbitration clause, and it must be sent to the nearest Nintendo headquarters within 30 days. Other than this specific instance, it is impossible to opt out of the EULA without violating articles; in this case, the agreement would be terminated and the company would be able to permanently disable the product.

- TikTok:

Out of all social media apps, TikTok has one of the most proficient algorithms in terms of keeping users on the app. This TikTok algorithm is not only addictive, but it also accesses an incredibly high volume of personal data. The main reason TikTok collects this much data is to improve the algorithm, thus keeping people on the app. Here is an overview of TikTok's EULA:

- Data Collection:

This is the most notorious part of TikTok's EULA, as some of the data collection policies that TikTok employs are downright invasive. Here are the various types of data the app collects [8]:

    - User-provided information:
        - Name, email, phone number, username, password, profile image, date of birth
        - User's videos, photos, comments, streams, video metadata
        - Messages, message metadata
    - Automatic:
        - Device information, including OS, IP address, mobile carrier, time zone
        - Interactions with app, videos watched, time spent, engagement patterns
        - Location data based on IP address

As explained earlier, the majority of the reasons TikTok collects user data relate to improving the algorithm. This algorithm is used to keep people on the app longer, leading to

more data collection to fuel the algorithm. This vicious cycle is already invasive enough, but it is made far worse when looking at who the app shares data with.

- Data Sharing:

TikTok shares user data with a variety of business entities, including its parent company, ByteDance. This is a Chinese-based company that frequently shares data with the Chinese government [10], which is notorious for its censorship practices. Due to this, TikTok has been documented to remove or suppress politically sensitive content, often complying with Chinese censorship regulations. This is not only a breach of user privacy, but it can also be a human rights issue, as any political statements made against the Chinese government's unethical practices are likely to be censored. Furthermore, the Chinese government can use the data from American individuals to determine people's opinions on sensitive political and social issues, such as gun control, abortion, and LGBTQ+ rights. This proves that on TikTok, nothing is private; even the most minute detail about the user as a person can be determined by a regime that does not even govern the user. In conclusion, the type of data being shared, as well as who the data is being shared with, raises extreme concerns about the ethics of the app's practices.

- User Rights/Opt-Out:

The main right that users of TikTok have is the right to ownership of their content. However, TikTok does have a license to use this user-generated content. This can involve reproducing, distributing, and sometimes blocking or removing the content. As for user privacy, users can control their content's visibility by adjusting privacy settings in the app, but this does not make the content private to the company, as TikTok can still use your data, even if it is private to other users.

The most important user right is the right to handle disagreements between users and the platform. Disagreements can be handled in either arbitration or a class action waiver, and users have a right to opt out of arbitration if they want to retain their right to sue the company [9]. Similar to Nintendo, this opt out clause only applies to the arbitration clause, and it must be sent

to the TikTok headquarters via mail within 30 days. In a class action waiver, the user agrees not to file a class action lawsuit against TikTok, and everything is resolved on an individual basis. The reason lawsuits are resolved individually instead of as a group is because of cost considerations for the company. If a large group decides to file a class action waiver against the company, this would likely be more costly than simply resolving disputes with each person individually. In conclusion, users have some important rights, but not enough to make up for the highly unethical data collection and sharing practices of TikTok.

- Updates:

TikTok takes great pride in its addictive algorithm that is improving every second, so installing updates that may improve this algorithm's performance would definitely be in the company's best interest. While updates are not outright forced like in the case of Nintendo, they are strongly encouraged by the platform, so users still have the right to choose whether or not to update the app. Updates may also occur in the company's privacy policy and community guidelines, and it is in every user's best interest to keep an eye on any changes that might occur in these policies.

● Comparison Matrix:

Topic	Anaconda-Navigator	Nintendo Switch	TikTok
Data collection	Collects action logs, usage data, system information	Basic personal information, console usage data	They collect EVERYTHING.
Data Sharing	Shared with sub-processors	Shared with Nintendo affiliates	Shared with parent company, shared with Chinese government
User Rights	Many rights, depends on region jurisdiction	Very limited, users do not technically "own" the console	Ownership of content

Opt-Out	US has right to opt out of data sharing	Users can opt out of arbitration, with intent to sue company	Users can opt out of arbitration, with intent to sue company
Updates	Users are notified of policy updates	Updates are forced	Updates are encouraged

Sources:

[1] https://legal.anaconda.com/policies/en/?name=end-user-license-agreement

[2] https://legal.anaconda.com/policies/en?name=privacy-policy

[3] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/

[4] https://www.nintendo.com/sg/support/switch/eula/usage_policy.html?srsltid=AfmBOopYvUC69wELKNo7gQINDkXziGes4g7Hm6NtP2I5TW64YDgupWv_

[5] https://vgsales.fandom.com/wiki/Nintendo_Switch

[6] https://en.wikipedia.org/wiki/Intellectual_property_protection_by_Nintendo

[7] https://en-americas-support.nintendo.com/app/answers/detail/a_id/48058/~/nintendo-switch-family%3A-user-agreement

[8] https://www.tiktok.com/legal/page/us/terms-of-service/en

[9] https://www.tiktok.com/legal/page/global/partner-privacy-policy/en

[10] https://en.wikipedia.org/wiki/ByteDance