Reading Privacy and Data Policies

Jessica "jynnie" Tang

INTRODUCTION.

Users often have a disconnect between how they think platforms collect and use their data and how they actually do. In an effort to bridge this gap, in 2018 the EU began enforcing General Data Protection Regulation (GDPR). GDPR enforced many standards about data collection and usage, including enforcing that all users should have the "right to be forgotten". In addition, they added a clause about consent mandating companies "are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form" (EU GDPR 2016). Consent also includes being able to withdraw it as easily as it could be given. This clause is the main concern I will be addressing in this paper. Have companies indeed made their data policies more accessible, readable, and transparent? Is that enough to change "the reality […] that very often customers sign contracts they do not read and give their consent to data processing without being fully informed" (Hoback 2013)? How do various platforms enact "consent"? And most of all, was that rendered "consent" enough?

While some users may not care how platforms process their data, many studies have shown that the collection of this information can be harmful to minorities and may facilitate biased analytics and "dataveillance" (Esposti 2014) (Crawford and boyd 2012).

I'll be doing a close analysis of Facebook, Twitter, Mastodon, Vero, and World of Warcraft's Data Policies, evaluating their rendition of "consent". Aspects of consent we'll examine include how readable the document users consent to is, how transparent are platform practices outlined, and how

consent and data ownership is modeled. Finally, I'll be drawing conclusions about the effectivity of requesting readable, transparent privacy policies.

To be noted, I am not evaluating the actual systems and algorithms behind each platforms usage of data, but rather the systems communicated by their data or privacy policy.

WHY THESE PLATFORMS.

I chose those platforms specifically as I want to look at how social network platforms and I wanted to look at platforms with varying approaches. Facebook is a mainstream social platform often used by users to interface with friends and family, while Twitter is a mainstream platform often used to speak to a larger audience. Mastodon is a decentralized version of Twitter that places a heavier emphasis on user security. Vero claims to be "true social" and tries brings user control of sharing to the forefront of their experience. Finally, World of Warcraft is a massive multiplayer online roleplay game where users interface with others and often create networks like friends, parties, and guilds. Each platform has a slightly different flavor of sociality and networking and gives us a broader view of ways data is used and collected.

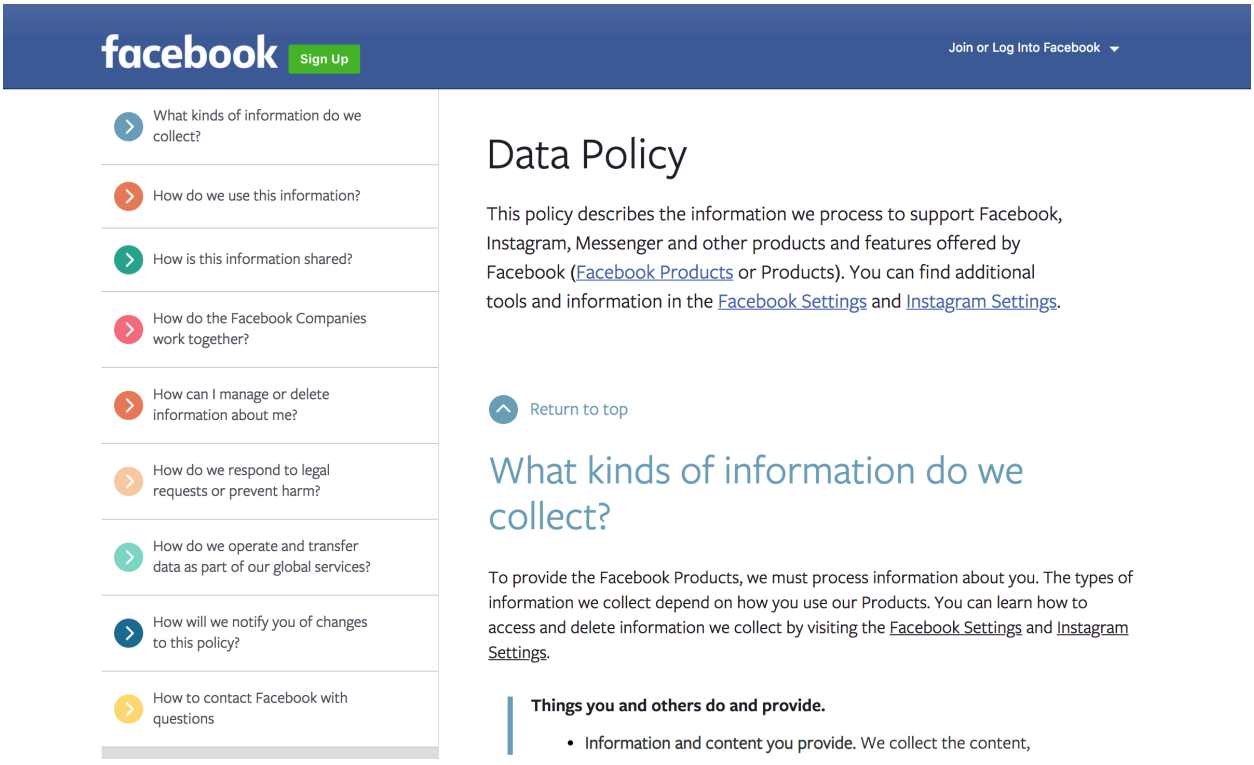
ARE POLICIES CLEAR, UNDERSTANDABLE, AND NAVIGABLE?

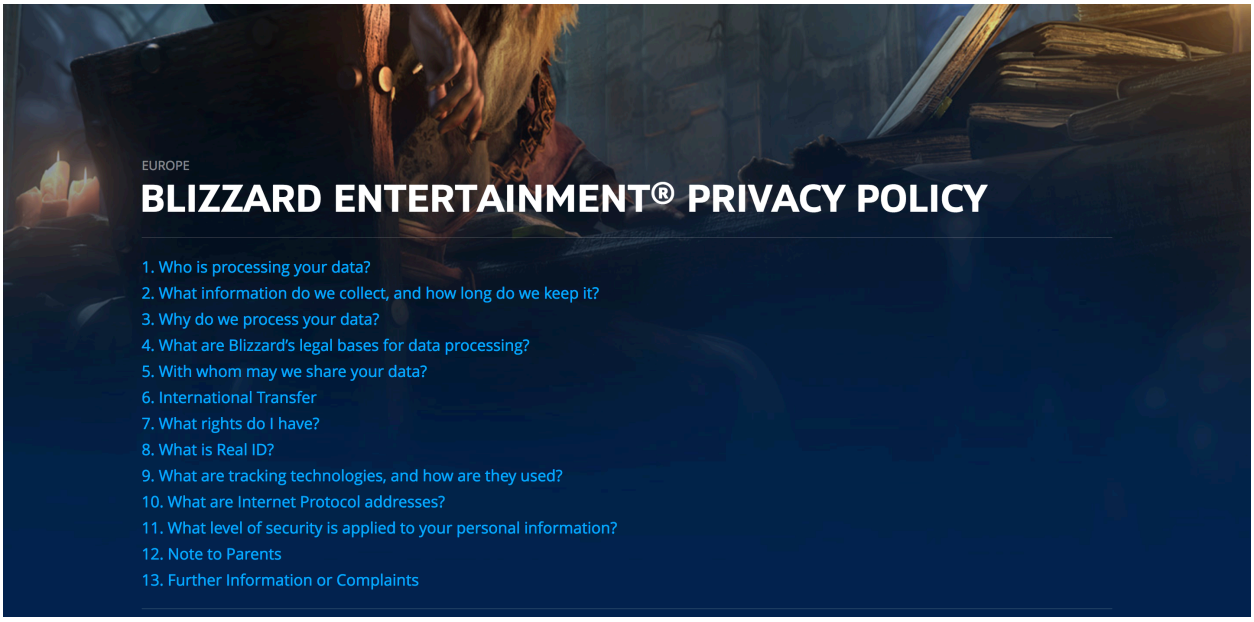
To evaluate readability, I'll be analyzing the overall approach to presenting each policy and pulling out specific examples. I will also use the Dale-Chall Readability scale and Fry Readability Grade Level (these will be further explained later).

Let's begin with each policy's general strategies. Facebook, Mastodon, and Blizzard Entertainment International (the company that produces and maintains World of Warcraft and henceforth referred

to simply as Blizzard) all similarly structure around sections whose headers are either questions users may have or centered around GDPR mandates. For example, all three have a header question about "what information do we collect". All three additionally have a brief paragraph or sentence that generally answers the question and following subsections or bullet points with more detail. For example, all three answer the question of "what information do we collect" in brief and follow up with subsections/bullet points about kinds of information collected. All utilize examples to ground their section. Out of the three, Facebook utilizes the most examples throughout their policy.

Facebook and Blizzard additionally give a table of contents-like area for users to easily navigate to sections they are interested in. (Mastodon's data policy being significantly shorter, perhaps chose to eschew of a table of contents as such).

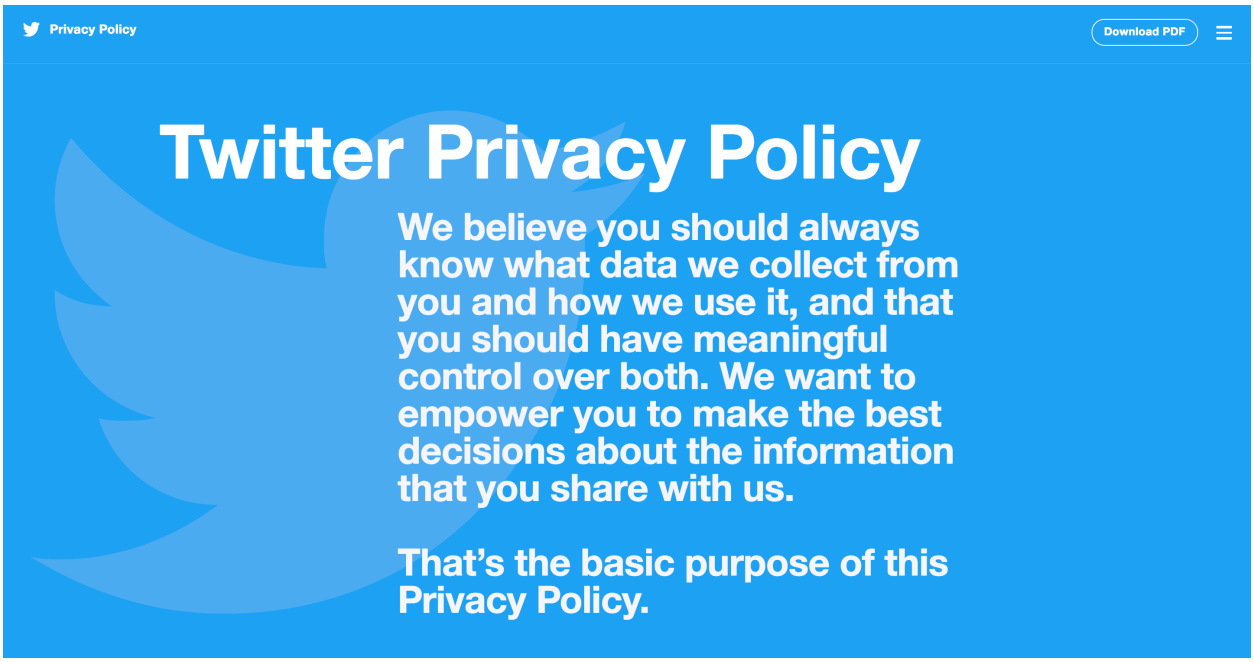




Facebook, Mastodon, and Blizzard differ slightly in strategy to better answer their platform specific questions. Both Facebook and Blizzard provide either supplementary links or definitions for platform specific terms like "profile fields" on Facebook and "player account data" for Blizzard.

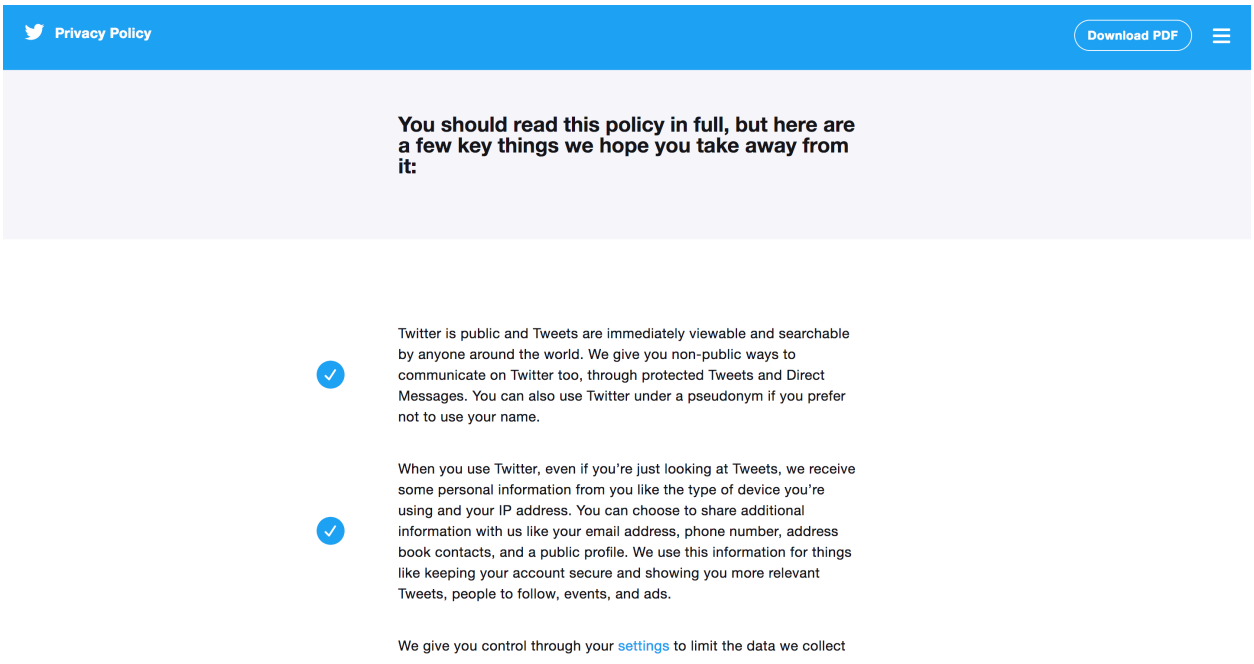
This general structure of sections centered around common questions easily points users to relevant sections. Examples further ground users as to what is exactly impacted. Explicitly detailing what things like "location-related information" actually means (Facebook says "such as your current location, where you live, the places you like to go, and the businesses and people you're near") makes it much less likely that users will misunderstand how their data is being used (Facebook 2018).

Twitter — like Facebook and Blizzard — breaks into sections centered around user concerns (not phrased as questions) and provides a details table of contents, but opens up differently. Twitter starts with their Privacy Policy's philosophy.



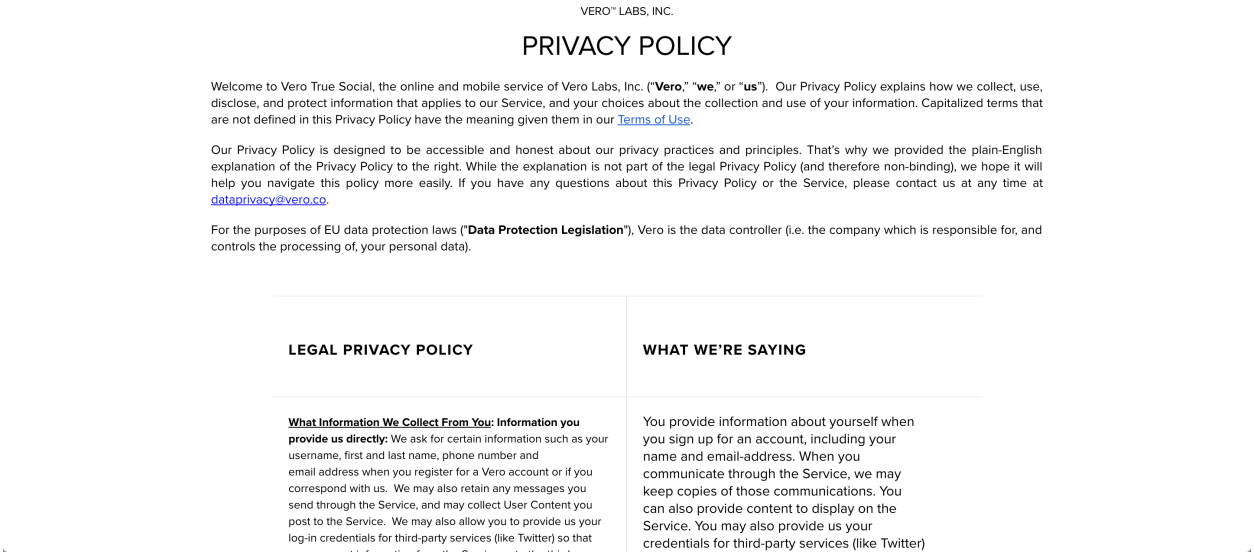
This philosophy not only places user control at the forefront of their concern, but also transparency.

Twitter follows this up with five key points users can take away and which support their philosophy.



This gives a quick summary for users who don't have time. The chosen key points also generally cover what kind of data is public, what data is processed, and how users can control their data. And similar to Blizzard and Facebook, Twitter provides supplementary links to definitions, support, and settings pages.

Unlike Facebook, Mastodon, Blizzard, and Twitter which generally lose legalese entirely, Vero keeps it. Vero splits their policy page in half, with one side detailing the legal policy, the other being a layman's explanation.



VERO™ LABS, INC.

PRIVACY POLICY

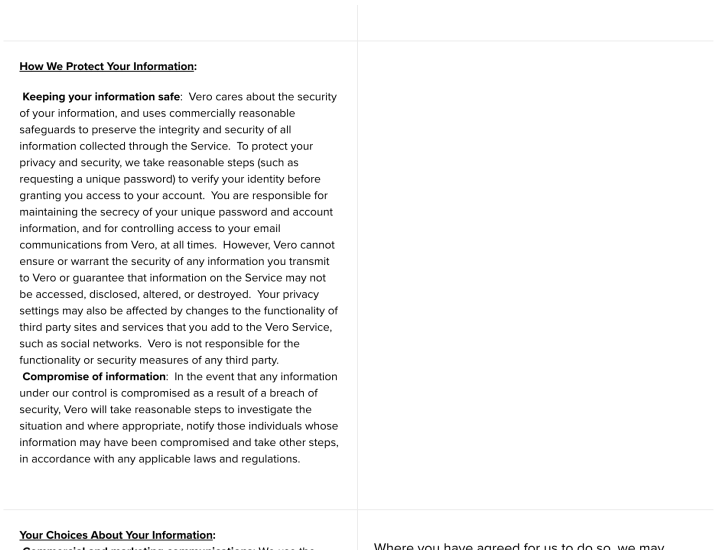
Welcome to Vero True Social, the online and mobile service of Vero Labs, Inc. ("**Vero**," "**we**," or "**us**"). Our Privacy Policy explains how we collect, use, disclose, and protect information that applies to our Service, and your choices about the collection and use of your information. Capitalized terms that are not defined in this Privacy Policy have the meaning given them in our Terms of Use.

Our Privacy Policy is designed to be accessible and honest about our privacy practices and principles. That's why we provided the plain-English explanation of the Privacy Policy to the right. While the explanation is not part of the legal Privacy Policy (and therefore non-binding), we hope it will help you navigate this policy more easily. If you have any questions about this Privacy Policy or the Service, please contact us at any time at dataprivacy@vero.co.

For the purposes of EU data protection laws ("**Data Protection Legislation**"), Vero is the data controller (i.e. the company which is responsible for, and controls the processing of, your personal data).

LEGAL PRIVACY POLICY	WHAT WE'RE SAYING
What Information We Collect From You: Information you provide us directly: We ask for certain information such as your username, first and last name, phone number and email address when you register for a Vero account or if you correspond with us. We may also retain any messages you send through the Service, and may collect User Content you post to the Service. We may also allow you to provide us your log-in credentials for third-party services (like Twitter) so that	You provide information about yourself when you sign up for an account, including your name and email-address. When you communicate through the Service, we may keep copies of those communications. You can also provide content to display on the Service. You may also provide us your credentials for third-party services (like Twitter)

This strategy makes it much harder for users to find specific answers to questions. Sections still use headers similar to that of Twitter, but general explanations are given in layman's terms while details remain in legalese. Not to mention, entire sections of the legal privacy policy lack a corresponding "what we're saying" section.



How We Protect Your Information:

Keeping your information safe: Vero cares about the security of your information, and uses commercially reasonable safeguards to preserve the integrity and security of all information collected through the Service. To protect your privacy and security, we take reasonable steps (such as requesting a unique password) to verify your identity before granting you access to your account. You are responsible for maintaining the secrecy of your unique password and account information, and for controlling access to your email communications from Vero, at all times. However, Vero cannot ensure or warrant the security of any information you transmit to Vero or guarantee that information on the Service may not be accessed, disclosed, altered, or destroyed. Your privacy settings may also be affected by changes to the functionality of third party sites and services that you add to the Vero Service, such as social networks. Vero is not responsible for the functionality or security measures of any third party.
Compromise of information: In the event that any information under our control is compromised as a result of a breach of security, Vero will take reasonable steps to investigate the situation and where appropriate, notify those individuals whose information may have been compromised and take other steps, in accordance with any applicable laws and regulations.

Your Choices About Your Information:

Where you have agreed for us to do so, we may

In comparison to our other platforms, Vero's structure is much less readable and navigable to users.

Despite much of these companies attempts to make more readable policies, these policies score from 8.57 to 10.18 on the Dale-Chall readability scale and indicate grade levels of 8 to 15 on the Fry Readability scale. I utilized *datayze*'s readability application to analyze these scores (Datayze n.d.). The Dale-Chall metric looks for difficult words based on a list of conglomerated easy words. Scores between 9.0 - 9.9 indicate a college-level readability. The Fry Readability scale indicates the grade level the text corresponds to. Twitter scores the best overall with a Dale-Chall score of 8.6 and a Fry Readability Grade Level of 8. Blizzard does the worst with a Dale-Chall score of 10.18 and a Fry Readability Grade Level of 15.

These scores indicate a difficulty in words and terms used in each policy. I mentioned above that Facebook, Blizzard, and Twitter do provide links and some definitions, but Facebook and Blizzard lack definitions for some more technical terms. For example, Facebook uses the term "metadata" as

an example of "content you provide", but does not explain what metadata is. Metadata is a more technical term that all users cannot be expected to know. Additionally, the abbreviated form of internet service provider (ISP) is thrown around without explanation. Blizzard also answers questions of "who has access to this type of data" with general terms such as "Operations and Esports" (Blizzard Entertainment International 2018), which may be a specific department in Blizzard, but is not clearly stated. Twitter does a better job of baking in definitions into the privacy policy, for example, defining what a cookie is in the privacy policy itself. Facebook, on the other hand, uses the term cookie throughout their data policy, but defines it in a cookie specific policy which is located on another page entirely. Mastodon fully relies on user technicity (familiarity or literacy with technical and computer specific language) and background of how Mastodon operates to understand terms like "server".

ARE POLICIES TRANSPARENT? WHAT ARE WE MISSING?

We have generally looked at the structures of each data policy, but is the content of each sufficient? For this section, I will be examining how much detail is provided in each platform's respective data or privacy policy and what barriers there are to users accessing more information.

Drawing off the last point in the above section, Blizzard's privacy policy answers who has access to what data, but fails to answer why. For example, social data is accessed by "Operations" and "Publishing". It's quite unclear what "Operations" is and does. Additionally, "Publishing" sounds like a department that publicizes for Blizzard. Why do they have access to players' social data? How much of players' social data does each branch/department have access to?

Facebook attempts to answer these kinds of "why" questions in its policy. It provides reasoning and

explanation with examples for why certain choices are made. For example:

We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed below.

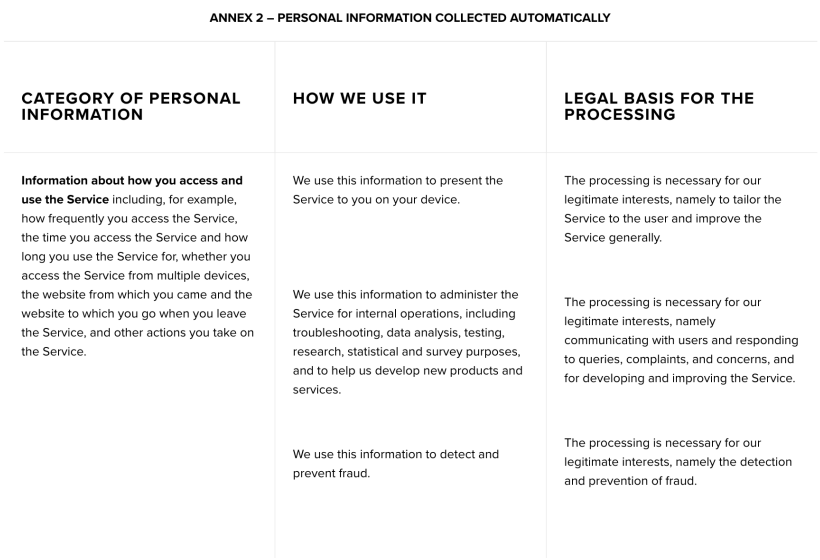
This provides a much clearer picture of both the system and the reasoning behind it. This kind of detail shows more clearly that the platform abides by GDPR Article 23 which calls for data minimisation — only data necessary for a controller's duty should be processed and held (EU GDPR 2016).

Mastodon does something similar and provides explanations of data sharing related to its decentralized structure. Decentralization means Mastodon relies on various independent server instances to operate. However, these servers may have different/specific privacy policies and data practices outside of those outlined in the general Mastodon Privacy Policy. Thus, in the policy, Mastodon outlines that:

We make a good effort to limit the access to [direct and followers-only] posts only to authorized persons, but other servers may fail to do so. Therefore, it's important to review servers your followers belong to. You may toggle an option to approve and reject new followers manually in the settings.

Mastodon recognizes possible faults in other servers, encourages users to look into their servers' policies, and provides an option for users to more scrupulously control how their information is being shared.

Vero is perhaps most explicit and offers multiple charts with what kind of data is processed, how it's used, and why it's necessary.

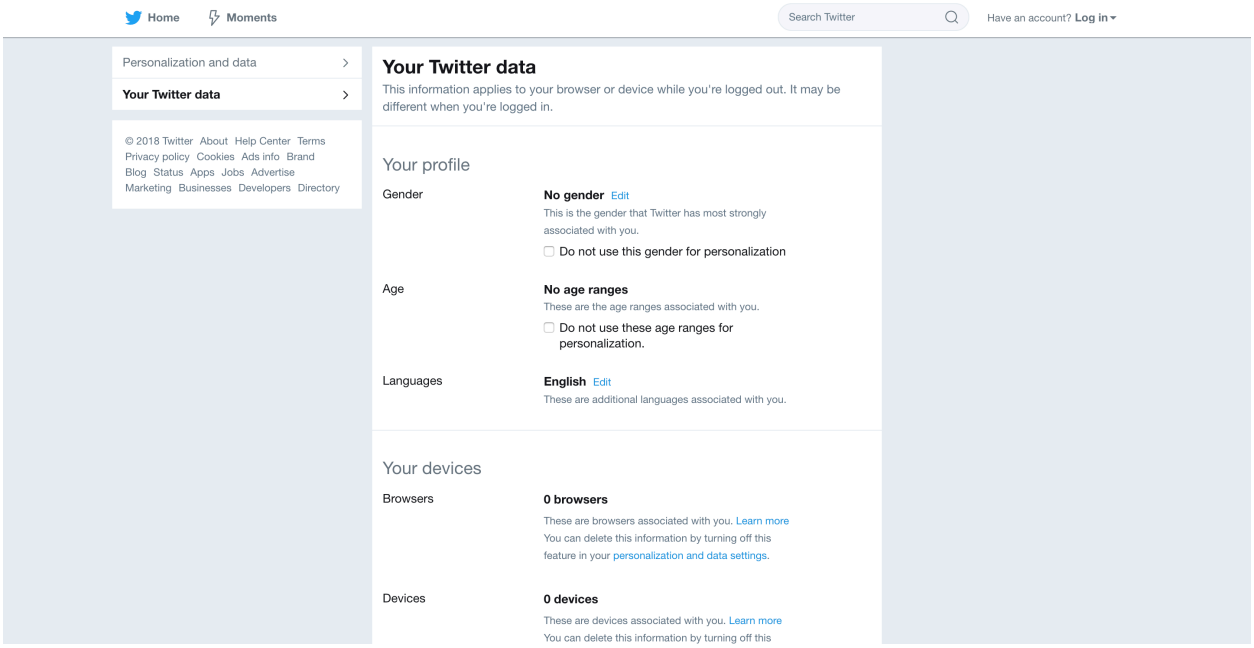


ANNEX 2 – PERSONAL INFORMATION COLLECTED AUTOMATICALLY

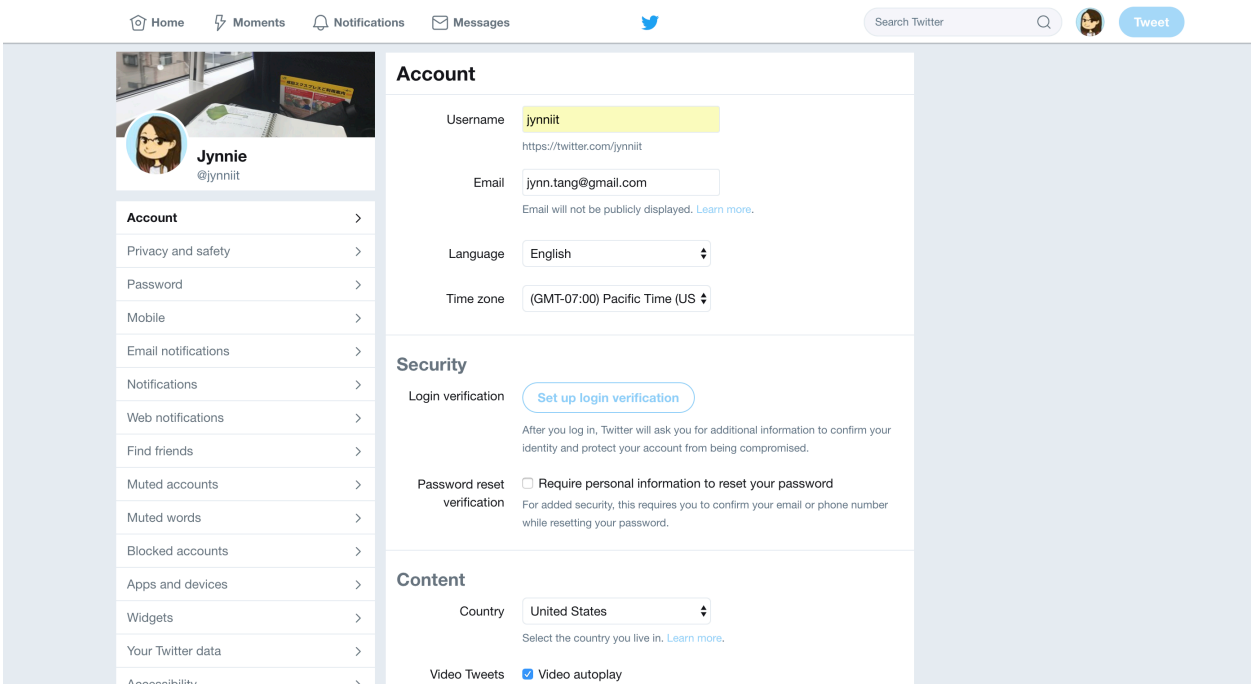
CATEGORY OF PERSONAL INFORMATION	HOW WE USE IT	LEGAL BASIS FOR THE PROCESSING
Information about how you access and use the Service including, for example, how frequently you access the Service, the time you access the Service and how long you use the Service for, whether you access the Service from multiple devices, the website from which you came and the website to which you go when you leave the Service, and other actions you take on the Service.	We use this information to present the Service to you on your device.	The processing is necessary for our legitimate interests, namely to tailor the Service to the user and improve the Service generally.
	We use this information to administer the Service for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes, and to help us develop new products and services.	The processing is necessary for our legitimate interests, namely communicating with users and responding to queries, complaints, and concerns, and for developing and improving the Service.
	We use this information to detect and prevent fraud.	The processing is necessary for our legitimate interests, namely the detection and prevention of fraud.

However, there is obfuscation in its language, such as "we use this information to present the Service to you on your device". This really doesn't say much at all.

Twitter and Facebook additionally link to user settings for supplementary information on how users have control over their data. Facebook links to both its and Instagram's user and privacy settings. However, Facebook and Twitter require you to be logged in (already have an account) to be able to see settings pages. This limits unregistered user's knowledge of what exactly they have control over. Twitter does let you see a "Your Twitter Data" and personalization settings page even if you are not logged in — filling the page with no data. This does provide a better look into what kind of data and options a user has, but still lacks detailed setting options.



Accessible as an unregistered user



Settings accessible when logged in

IS AMPLE CONSENT COMMUNICATED?

GDPR mandates "it must be as easy to withdraw consent as it is to give it" (EU GDPR 2016). And all of the data policies we look at state that users may withdraw their consent and delete their data/account at any time. However, each policy gives a varying amount of detail with this form of withdrawal. Mastodon only states "you may irreversibly delete your account at any time" (Mastodon 2017). There is no reassurance of all your data being erased on the server and whether all decentralized servers will erase your data. In fact, this is concerning since it's previously mentioned in their policy that different servers may have different policies for data sharing. Vero similarly also states that users have the right to withdraw consent. However, "if you wish to exercise one of these rights, please contact us at dataprivacy@vero.co" (Vero Labs Inc. 2018). There are not only no details about what Vero considers withdrawing consent to mean in their privacy policy, but also the process is not ostensibly as easy as signing up with an email and password and consenting. Consent is not as clear cut as it seems.

On the other hand, Facebook explicitly mentions what is deleted when a user deletes their account.

When you delete your account, we delete things you have posted, such as your photos and status updates, and you won't be able to recover that information later. Information that others have shared about you isn't part of your account and won't be deleted.

In revealing what is deleted, Facebook also models what information and data is owned by who. What's deleted is not necessarily all data *about* you, but all data in your account. Others can own data about you and as long as they consent, information about you may still be retained and processed. Twitter similarly outlines clear instructions and information about deleted information, but also adds

that third parties may still retain copies of your data. While consent is more thoroughly detailed and the method to withdraw consent is also given, a platform's idea of what data is yours may not match what users' ideas are.

Blizzard is mixed on how clearly consent is rendered in their policies. Their policy clearly lays out what and how consent is obtained for various services or features, but does not always explicitly point to how to withdraw consent. Also, just stating that consent can be withdrawn at any time.

CONCLUSION.

By examining this wide array of policies, we see what works and what feels insufficient. Readability is not just about not using legalese, but also structure and providing access to definitions of esoteric and technical terms. In addition, we see what we want from transparency is not just what and how data is used, but why. And are non-users afforded the same transparency as users? Each policy also renders consent differently. We lack a clear understanding of how much can you withdraw. Twitter, Facebook, and Mastodon point most clearly towards account deletion as a withdrawal of consent — an all or nothing choice. Twitter and Facebook mention opt-out options of certain services through settings, but are hazy on what that means for your data. Vero provides little to detail what is withdrawn at all. Blizzard mentions slightly more fine-grain control in being able to erase specific information (such as player allergies).

The provisions called for by GDPR don't necessarily relieve the concerns Crawford, boyd, and Espoti have about data collection and user control. Hoback's reality that data policies may continue to go unread before consent also doesn't appear to be addressed. Users are still unlikely to read through a long essay of privacy policies before connecting a third-party application. Instead, these

documents appear geared for users who retroactively want to make changes to how their data is used and kept or just want some vague assurance that their data is secure.

All in all, I see a call for clearer details to be provided to both users and non-users over what control they have. And I would like to suggest that a third-party categorization system may be useful in broadly outlining privacy policies of different platforms. Many of the policies I've examined have come a long way from unreadable legalese. But perhaps what we need is not just readable, transparent policies; but a system for users to easily understand what a policy generally outlines before consenting, without having to read 4,000 or so words each time.

Bibliography

Blizzard Entertainment International. 2018. "BLIZZARD ENTERTAINMENT® PRIVACY POLICY." *Blizzard*. April. Accessed October 20, 2018. https://www.blizzard.com/en-gb/legal/8c41e7e6-0b61-42c4-a674-c91d8e8d68d3/blizzard-entertainment-privacy-policy.

Crawford, Kate, and danah boyd. 2012. "CRITICAL QUESTIONS FOR BIG DATA." *Information, Communication & Society*, May 10: 662-679.

Datayze. n.d. *Readability Analyzer*. Datayze. Accessed October 24, 2018. https://datayze.com/readability-analyzer.php.

Esposti, Sara Degli. 2014. "When big data meets dataveillance: The hidden side of analytics." *Surveillance & Society*, 209-225.

EU GDPR. 2016. "GDPR Key Changes." *EU GDPR*. April. Accessed Oct 20, 2018. https://eugdpr.org/the-regulation/.

Facebook. 2018. "Data Policy." *Facebook*. April 19. Accessed October 20, 2018. https://www.facebook.com/privacy/explanation.

2013. *Terms and Conditions May Apply*. Documentary Film. Directed by Cullen Hoback. Produced by Hyrax Films and Topiary Productions.

Mastodon. 2017. "Privacy Policy ." *Mastodon*. March 7. Accessed October 20, 2018. https://mastodon.social/terms.

Vero Labs Inc. 2018. "Privacy Policy." *Vero*. July 20. Accessed October 20, 2018. https://www.vero.co/privacy-policy/.