# Utilizing Actor-Network Theory (ANT) in the Analysis of the TikTok Ban Within the Privacy Landscape

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

**Anika Sharma**

Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Joshua Earle, Department of Engineering and Society

# STS Research Paper

## Introduction:

In this increasingly interconnected world, new technologies have the potential to bring individuals closer, even across the far reaches of the globe. However, this increase in data sharing poses a potential threat for breaches in privacy and personal data security. One of the most prominent industries undergoing this intense scrutiny is the social media landscape. Individuals on these applications regularly share content and information pertaining to their personal lives, or private data.

One of the largest distinctions between the way information spreads is the categorization of it belonging to the public or private domain. Public data has several key characteristics such as it being both highly stable and reliable. Since it is gathered and anonymized by the National Statistics Offices within the United States, it is especially useful for understanding the long-term needs of customers (Digiseg, 2023). Meanwhile, private data is defined as information concerning a person that can be reasonably expected to be secured by public view (Spacey, 2017). This includes information such as individuals' names, contacts, medical information, and behavior data. However, many firms have huge incentive to gain insights on users' behavioral data such as interests and buying habits. The lines are often blurred with the use of what is referred to as third-party data, which essentially follows a users' digital footprint around the internet using 'cookies' that retrieve website visit history. Currently, third-party data is becoming increasingly difficult to access for companies with legislation such as The General Data Protection Regulation (GDPR) of 2018 in the US, but some firms in particular still pose a threat.

TikTok, a popular social networking application owned by parent company ByteDance, is one such firm undergoing scrutiny in the eyes of the United States Government. TikTok itself is an application that came to be as the international version of popular Chinese application

Douyin, after ByteDance acquired the video-sharing platform Musical.ly (Dean, 2024). In March of 2024, the US government passed a bill with a good amount of bipartisan support to ban it in the country (Maheshwari et al., 2024). ByteDance is a Chinese owned company, causing concerns about third-party data being sold in other countries to pose a threat to national security. This highly controversial move goes to show the extent of debate over privacy control standards that continue with the rise in algorithmic social platforms, and their impact on free speech on a national, firm, and individual scale.

The research question this paper hopes to address is: what is the role of privacy within this controversial ban as analyzed under the lens of actor-network theory? This paper will classify the different layers of user groups before diving deep into the actors and networks present within the conflict while uncovering the dynamics and translations of all human and non-human actors. This thorough analysis will provide a placement for privacy as the ultimate conclusion while looking forward to its application in other similar situations.

**Methodology:**

In order to better make sense of the types of data privacy risks, this paper will segment users into three categories prior to elaborating on actor-network theory. These segments include the individual, the firm, and the nation.

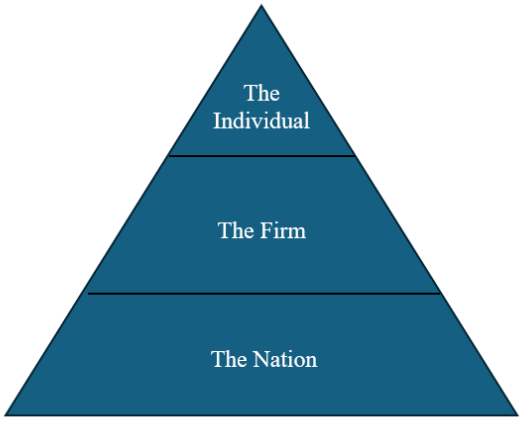

Figure 1: Pyramid of User Segmentation

**The Individual**

The individual makes up the lowest rung in the pyramid but is likely one of the most important. Currently, there is much legislation in place to protect the privacy rights of individuals, one of the most prevalent in the United States being the Privacy Act of 1974 which sets the grounds for "fair information practices". This act focuses on protecting personal information and private data by requiring consent on the disclosure of records.

On the European front, a key piece of legislation is the establishment of the General Data Protection Regulation (GDPR), which explicitly gives individuals the ownership of their own personal information as well as the legal right to determine the use of it (*General Data Protection Regulation (GDPR) – Legal Text*, 2024). Many individual states in the United States have followed suit to this approach, instituting their own individual statutes that have similar terms to that of the GDPR. There has always been a precarious balance between innovation for individual users and a nation's duty to provide security for its citizens. In recent times, individual data has surely been moving towards a new era of a rights based approach following the EU's view on data management as opposed to the traditional view of policy in place as a mechanism to prevent harm that would seek to mitigate maldoings in specific industries or sectors. Surely enough, this is to have an effect on the firms and businesses that access individual data, or the firm.

**The Firm**

In this paper, firms will take on two meanings. They will, first and foremost, refer to the collection and organization of individuals into groups on a larger scale. Firms will also take on the dual meaning as those organizations that make use of individual and private data. For the

most part, firms are driven by profit that aligns in their interest of knowing as much as possible about their target market of consumers. While individual data is essential to regulatory bodies to best serve their constituents, it also has massive value to firms seeking to draw out patterns and relational characteristics. But along with this comes the danger of biases based on how the personal data is grouped or collected, as well as the seemingly unintended ones from the creators of the technologies themselves.

The Algorithms of Oppression explores how these biases can seep into data that is used to eventually draw conclusions on part of firms (Noble, 2018). This text tackles data discrimination when it comes to large search engines that are often overturned by private interests for promoting certain sites. Most of these private interests are often rooted in many social issues such as sexism and racism, explaining why certain terms come up for some of these specific groups that may be suggestive of the underlying tainted message. It seems that many of these private interests are deeply rooted and then translated to other developing technologies through the data used to train algorithms, truly illustrating the pitfalls that could come with data falling into the wrong hands.

An additional and rather notorious bias that firms should be aware of is confirmation bias, as mentioned in Trust in numbers: The Pursuit of Objectivity in Science and Public Life. This text introduces the term “technoscience” to symbolize the merger between technology and science, while diving deep into the relationship between the two (Porter, 2020). With the increased amount of emphasis on numbers and statistics to serve as the guiding light for empirical research and conclusions, itt seems that no matter how we seek to standardize the data, there will still be gaps that are filled by an individual's own perspective and cultural identity. In this manner, it seems that statistics cannot ever be fully objective. There is always the matter as

to how a person deciphers it as well as the fact that each user may have their own agenda they're seeking to fill - a common type of bias known as confirmation bias. Perhaps this is the most prevalent type of bias of all. Thus there seems to be an ever-preserved bias in the data itself that firms have the power to perceive and regulate.

**The Nation**

On the bottom of the pyramid are the nations that are tasked with protecting the rights and privacy of their individual citizens, while also regulating the way firms interact with the two. Differences exist between nations on a viewpoint standpoint as well when it comes to the approach to how to approach their constituents' privacy. With so much of the TikTok ban controversy having to do with national security, there becomes a clear divide between the approaches of the East vs West when it comes to this issue. Moreover, it is critical to note that ByteDance is a Chinese-based company, which is the main issue for the US government.

The United States has maintained its drive towards research and development of new technologies while coming from a strong view of protecting individual privacy to great lengths. Meanwhile, China takes a different approach with privacy overall. While privacy laws are mostly associated with democracies, autocracies such as China still have their version of them (*What's Behind China's Laws to Protect Privacy?*, 2023). China's first comprehensive privacy law enacted in 2021, the Personal Information Protection Law (PIPL), instantiates greater compliance obligations from large internet platforms with a requirement to create an independent body to look over their privacy protection work. As stated by Mark Jia on China's new laws to protect privacy, he hypothesized that these laws are formed in large part to "highlight its responsive governance in the face of new vulnerabilities and dependencies that have arisen out of China's data-driven society" (Ding 2018). Moreover, it is important to take note of China's long

standing view of foreign technology companies and its general preference to domestic development when examining the overall landscape of emerging technologies. As Ding analyzes in, *Deciphering China's AI Dream*, the East has always taken a different approach when it comes to technology development and implementation. This could be due to a variety of different reasons such as the difference in government structures or types of programs that benefit from new R&D in technology. Understanding of both these key viewpoints is critical to developing an all-encompassing lens at the types of privacy outlooks different nations can take to meet their own domestic goals.

**Actor-Network Theory**

Due to the nature of there being many user groups involved in this analysis, a useful framework to apply would be actor-network theory (ANT). ANT theory is used to conduct relational analysis of both the non-human and human "actors", or individual constituents that make up the actor-network (Lolha, 2022). The actor-network then consisted of the grouping of aligned interests in both organization and standards. The theory introduces the idea of there being non-human actants that also hold an equal role in generating network assembly. In the context of applying this theory to privacy, the individual actors at play will be listed out, grouping by human and non-human. Then, a closer inspection will be done on the alliances within the actor-network, or how these actors group based on aligned interests to be accommodated for. Since actors within networks must translate interests in order to work in agreement with the network, we can also take a look into the volatility of the actors. That is, taking a look into how stable the alliances between the network may be in relation to the network as a whole. This will help to create an overarching diagram of the relationships of the entirety of the actor-network.

**Analysis:**

This section will dive into actor network theory by starting out with the separation of human and non-human actors that will eventually converge and interact in future steps.

Human actors:

The human actors within this specific case of actor-network theory can fit well into the aforementioned pyramid (fig 1.). Starting at the top of the pyramid at the individual scale, the key human actors in this case are individuals, users or subjects. This includes all users of ByteDance applications, specifically the ones that view and create content on TikTok. Directly related to individuals are users that play a large role in generating the content on the application, or content creators. It is important to also note that Americans 18 and over are estimated to spend 55.8 minutes per day on TikTok, a bulk of these users being casual viewers (Dean, 2024). Thus this distribution between content creators and content viewers should also be taken into account as separate actors. On the privacy side of things, other human actors include those involved deeply in the advocacy side - privacy advocates and activists. This association also fits into the second run of the ladder: firms. The actor that translates to this are institutions. Another actor in this rung is ad-tech companies. Within the bottom of the pyramid, the relevant actors include the regulators and policymakers, the national government, and international regulatory bodies. Related human actors include data scientists and media professionals, all of which play a role in the overall controversy and situation.

Non-human actors:

The bulk of the actors within this case of actor-network theory comprise of non-human actors. The application TikTok, or ByteDance, will be at the center itself. Other related non-human actors include data and content, which are further broken down into datasets, third-party

data, and biases. Network infrastructure and information systems are other actors on the operational front of the conflict and application itself. From the privacy standpoint, non-human actors include privacy regulations, advertisements, surveillance, content controls, surveillance, and social media platforms. The initial actors are mapped down below:

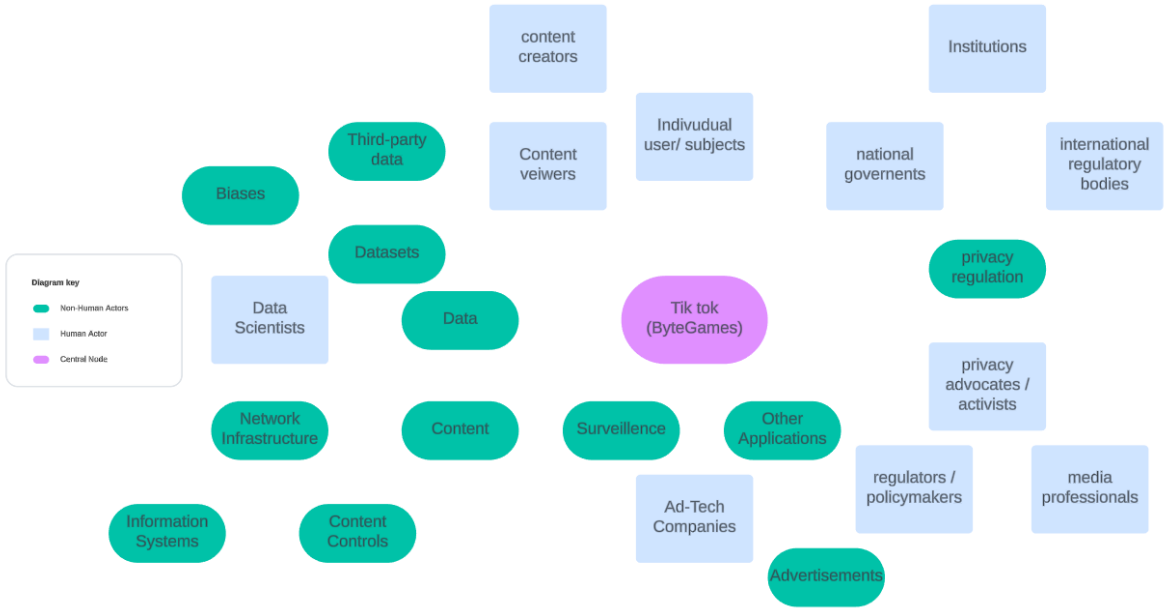


Figure 2: Initial Actors

Interactions and Alliances:

A key portion of actor-network theory is acknowledging that "actants are measured and valued only by how they interact in the system" (Sismondo, 2011). Thus by placing human and non-human actors on the same level, we can start to draw interactions that eventually form alliances between the different actors. One of the first key interactions will transpire between *users* and *privacy advocates*. As users start to express concerns surrounding TikTok's data collection methods and share their experiences about the potential risks of the application, privacy advocates can be heightened in their approach and consideration of these newly brought upon perspectives. The distinction between *content creators* and *content viewers* can also garner

different responses when it comes to outlooks on privacy. In this sense, the non-human actor *data* also plays a key role in this interaction. The application openly expresses that it collects the following information in its privacy policy: IP address, Geolocation data, Device identifiers, Browsing and search history, Cookies, Email address, Phone number, Age, Information about photos and videos, and Clipboard contents (Fung, 2023). However, data takes another turn with the introduction of the element of *third-party data*, as well as the notion of where this data is stored and eventually goes. There have been numerous studies reporting that TikTok uses this third-party data in the form of cookies to follow around users around the web even when they are not using the app (Germain, 2022). It is important to also note here that a lot of *ad-tech companies*, another actor coming into this interaction, also utilize the same types of tracking technology and rely heavily on third-party data in targeting *advertisements*, albeit on an even larger-scale (Malwarebytes, 2022).

Tiktok has also faced claims around the practice of keylogging. Keylogging involves the tracking of users's keyboard entries using in-app searching mechanisms. While this isn't inherently a negative action, according to analyst Felix Kruase, it does have the potential to cause security concerns when it comes to the collection of sensitive data such as passwords and credit card information. While there is no conclusive and current evidence as to the extent to which this action has been used as a malpractice as well as the notion of keylogging being a common practice among many *other applications* in the technology industry, it brings up the idea of casting doubts on particular firms. Thus, the interaction between other applications that follow a similar social media based *content* sharing mechanism can be devised.

The difference between the interaction of these *other applications* and *privacy advocates* vs. the interaction between *TikTok* and *privacy advocates* can also be scrutinized. TikTok has

long been investigated due to its parent company being Chinese-based, even though it has made its stance clear on the application being intended for non-Chinese markets and being unavailable in the Chinese mainland. Moreover, the doubts surrounding TikTok's data sharing practices have been investigated to be just as common and as invasive as other US based applications. The main concern remains that the Chinese government may be collecting the data secretly from the ByteDance for intelligence-gathering purposes or the possibility of using TikTok's content recommendations algorithms for the purpose of spreading misinformation (Maheshwari & Holpuch, 2024).Thus, this interaction may be a little more similar than originally thought to be, although there have been many doubts due to the base of the ByteDance itself.

Two other actors also come into play here in analyzing this interaction: *national governments* and *institutions*. In many ways, the TikTok privacy concerns have reached the point of bypassing the individual scale and being seen as a threat to national security. On an international scale, 71% of all countries have some sort of legislation surrounding data protection and privacy, those of which the actor *international regulatory bodies* comes into play (*Data Protection and Privacy Legislation Worldwide*, n.d.). *Regulators and policymakers* in the United States have played a key role in shaping the *privacy regulation* surrounding the decision to ban TikTok, with the senate even passing a vote to give the company up to a year to find a buyer in the US market. The national government also plays a key role in determining the amount of information that is protected and how much access companies receive in the first place. Interestingly enough, the United States does not have any federal privacy laws regulating companies, although individual states do have their own. So, it is possible for companies to not notify you if a data breach occurs or if your data is sold to third parties (Klosowski, 2021). Thus, the ecosystem of current *privacy regulation* as set by the *national governments* themselves has a

key role in determining the manner in which its constituents interact with applications. In the furthest of cases, user data can be used as a technique to issue *surveillance*, either on part of the company or with the characteristics of the national government itself.

The interaction between *data scientists* and *content* also has a unique role in the conflict. TikTok is prided on its content-recommendation algorithm, which is able to learn quickly about the user tastes and interests in content utilizing user signals rooted in machine learning and built upon *data sets (TikTok Algorithm Guide 2024: How to Get Your Videos on FYPs, n.d.)*. *Biases* also place themselves within this interaction, as user patterns and trends can be misinterpreted and be utilized to spread misinformation. In a way, *media professionals* also have a large role to play in preventing this transfer of misinformation, as they have the influence of creating narratives for certain issues. TikTok's own policies directly state that the application contains "robust policies around specific types of misinformation like medical, climate change, and election misinformation, as well as misleading AI-generated content, conspiracy theories, and public safety issues like natural disasters." (Cheong, 2024) With this, an additional interaction can be formed in between the *network infrastructure*, *information systems*, and *content controls*. All these components play a role in devising the type of content shown to specific users utilizing the algorithms and user signals. In this way, all the actors in this network form interactions with each other, pushing and pulling on each other in various ways. These translation processes can be explored more in the next section.

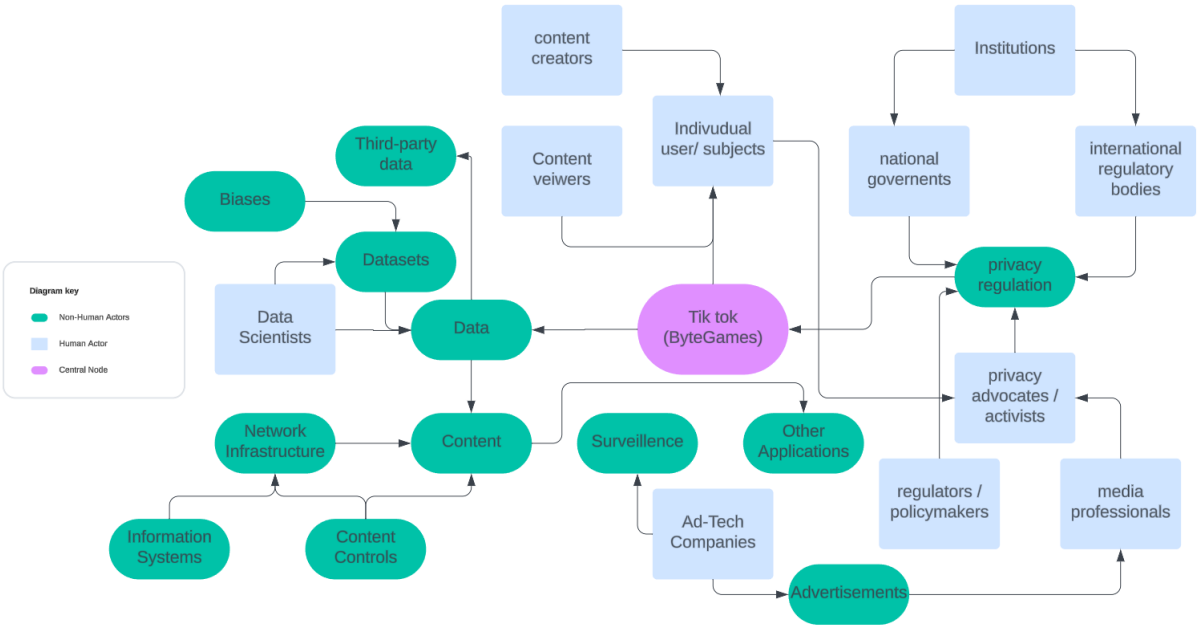


Figure 3. Network Interactions

Translation and Networks

Within ANT, the translation process refers to how actors align their interests to form networks of associations or resistance. The first translation process involves articulation, where issues are framed and defined within the network (Sismondo, 2011). Within the TikTok ban, many actors articulate their privacy concerns by bringing up definite instances in which individual and national privacy has been upended. For example, in an earlier interaction described, privacy advocates may gain experiential information from users subject to where privacy issues have arisen.

The next stage is enrolment, where actors are enlisted to support or align with a particular interest. Here, actors will strive to enlist other actors to adopt their views on the privacy concerns and ban. The United States government and other institutions are working to enlist other actors such as users and other applications to adopt its view on why TikTok possesses threats to national security. Meanwhile, content creators and ad-tech companies that seek to profit from

TikTok may be attempting to enlist actors such as privacy regulation by providing specific use cases and evidence as to why the application does not pose a threat to national security or individual data. In the intermediary transition phase, interests are mediated between actors within the network. Within this network, intermediary actors such as data, media professionals, and third-party data may have a large role in shaping public discourse on privacy laws as well as the overall perception of privacy regulation. These intermediaries possess the opportunity to connect and translate the different beliefs of different alliances and parts of the network, thereby creating potential opportunities for new enlistments.

In the interessant phase, interests will be mobilized in support of particular agendas or goals. For example, the United States government may work to completely ban the application or sell it to a US based company, using evidence gained amongst alliances with other actors as the backbone in fueling processes. Actors may also interesse other stakeholders such as the data scientists utilizing the existence of biases and misinformation to interasse the United States government into banning the application. In this manner, actors are able to push their agendas agreed upon in their preexisting alliances. Finally, problematisation involves framing issues as problems that need to be addressed within the network. Actors may use this translation process to create urgency within the network for immediate mobilization. In the network regarding the TikTok ban, actors may frame the privacy concerns as those threatening individual security and safety or even a threat to national security. These may arouse reactions from other actors in the network and quicken the process of alliance formation as well.

**Discussion:**

In a way, it seems that the emergence of this new legislation almost puts the existing network to the test. It is important to consider what repercussions its passing has on all actors and

the landscape of privacy as a whole. In this analysis, privacy itself is almost used as a mechanism for translation between the different actors as well as a framework in alliance formation. While the fate of TikTok still remains unclear, the landscape of privacy on the individual, firm, and nation level has been altered. The result of these interactions will set the stage for relations between the East and West on the institution level, the amount of control and access firms have to data and ability to decide what to do with it, and the depth to which individuals' value their privacy. It is clear that applications such as TikTok also have a resounding impact on individuals' mental health as well as just privacy. According to the World Health Organization, TikTok's key target demographic is already prone to struggling with mental health challenges (World Health Organization: WHO, 2021). Adding such a robust content-sharing application may only aid this isolation epidemic that many youth face with increased rates of social anxiety and depression (*TikTok and Youth Mental Health: Weighing the Pros and Cons - Depression and Bipolar Support Alliance*, 2022). These added concerns may be used to build a stronger case in banning TikTok. However, this creates a question of precedent and whether or not similar existing applications should also face the same treatment. Still, it is clear that the decision will cause ripples throughout not only the network described in this paper, but also the future of the definition of privacy in the social media app development and the intersection of foreign climates.

**Citations:**


Cheong, M., (2024, March 20). *Combating harmful misinformation | TikTok*. TikTok. https://www.tiktok.com/transparency/en-us/combating-misinformation/

*Data protection and privacy legislation worldwide*. (n.d.). UNCTAD. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Dean, B. (2024, February 15). *TikTok Statistics You need to know*. Backlinko. https://backlinko.com/tiktok-users

Digiseg. (2023, February 8). *Public vs. Private Data Guide*. Digiseg. https://digiseg.io/news/private-vs-public/

Ding, J. (2018). *Deciphering China's AI Dream*. Future of Humanity Institute.

Fung, B. (2023, March 24). TikTok collects a lot of data. But that's not the main reason officials say it's a security risk. *CNN*. https://www.cnn.com/2023/03/24/tech/tiktok-ban-national-security-hearing/index.html

*General Data Protection Regulation (GDPR) – legal text*. (2024, April 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Germain, T. (2022, September 29). How TikTok tracks you across the web, even if you don't use the app. *Consumer Reports*. https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/

Klosowski, T. (2021, September 8). The state of consumer data privacy laws in the US (And Why it matters). *Wirecutter: Reviews for the Real World*. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Lolha, E. (2022, May 30). A brief explanation about Actor-Network Theory - Erron Lolha - medium. *Medium*. https://aprilliale.medium.com/a-brief-explanation-about-actor-network-theory-d8e9aad41a18

Maheshwari, S., & Holpuch, A. (2024, April 24). Why Congress voted to force a sale of TikTok in the U.S. *The New York Times*. https://www.nytimes.com/article/tiktok-ban.html

Maheshwari, S., McCabe, D., & Karni, A. (2024, March 13). U.S. House passes bill that could ban TikTok. *The New York Times*. https://www.nytimes.com/2024/03/13/technology/tiktok-ban-house-vote.html

Malwarebytes. (2022, October 3). *TikTok's "secret operation" tracks you even if you don't use it*. https://www.malwarebytes.com/blog/news/2022/10/tiktoks-secret-operation-tracks-you-even-if-you-dont-use-it

NYU Press. (2019, July 2). *Book details - NYU Press.* https://nyupress.org/9781479837243/algorithms-of-oppression/

Porter, T. M. (2020). T*rust in numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton University Press.

Sismondo, S. (2011). *An introduction to science and technology studies*. John Wiley & Sons.

Spacey, J. (2017, August 28). *9 Examples of private data*. Simplicable. https://simplicable.com/society/private-data

*TikTok and Youth Mental Health: Weighing the pros and Cons - Depression and Bipolar Support Alliance*. (2022, July 25). Depression and Bipolar Support Alliance. https://www.dbsalliance.org/education/newsletters/tiktok-and-youth-mental-health/

*TikTok Algorithm Guide 2024: How to get your videos on FYPs*. (n.d.). Buffer: All-you-need Social Media Toolkit for Small Businesses. https://buffer.com/resources/tiktok-algorithm/

*What's behind China's laws to protect privacy?* (2023, October 16). ChinaFile. https://www.chinafile.com/reporting-opinion/notes-chinafile/whats-behind-chinas-laws-protect-privacy

World Health Organization: WHO. (2021, November 17). *Mental health of adolescents*. https://www.who.int/news-room/fact-sheets/detail/adolescent-mental-health