

The Paradox of Privacy and Anonymity: When too Much of a Good Thing Becomes Bad

Jared Andraszek

Department of Computer Science, Charleston Southern University

CSCI 415: Algorithms

Dr. Songhui Yue

December 4, 2023

The Paradox of Privacy and Anonymity: When too Much of a Good Thing Becomes Bad

Imagine a world where every action, word spoken, or preference made is recorded and monitored and everyone is held accountable for them. This dystopian scenario is not as far-fetched as it once seemed. For instance, social media giants such as Meta collect up to 86 percent of personal information such as financial information, location, and personal identifiers (Radauskas, 2023), and it is coming to a point where people can lose jobs or potential offers based on what someone has posted online. Where 18 percent of employees have been fired because of their social media accounts and posting information that garnered a large response, or broke a company policy (Dolan, 2022). But does this mean that there should be no data collection and no accountability based on what is stated over the internet? While there are areas to improve what companies collect on their users, too much privacy and anonymity of users can allow for anyone to say anything with no repercussions. With all of these recent developments, this paper delves into the interconnectivity that digital privacy, anonymity, and accountability, while also looking at an example.

As we consider the interconnectivity of digital privacy, anonymity, and accountability, we must first define what these terms mean to provide the groundwork for understanding the scenarios. The definition of digital privacy is diverse and changes based on the company or business; however, according to the Merriam-Webster dictionary, privacy is “a: the quality or state of being apart from company or observation, b: freedom from unauthorized intrusion.” However, this definition does not fully encompass digital privacy because companies track and store the data online for every action we take. This data includes what we used to create accounts and personal information for targeted advertising and business purposes (IDX, What are the

threats to digital privacy?). Primarily, in social media, users expect to share what they want with those they want to see it. This expectation forms an idea of privacy in public, where even though the data is public, we only want to select people to see it. If we use Facebook as an example, users can change who can see their posts based on who they are friends with, friends of friends, or the public. Therefore, digital privacy can be described as the protection of private information stored on the internet and ensuring no unauthorized personnel can view or alter it.

Anonymity and accountability can coexist; however, they also present colliding issues. In the digital context, anonymity is where an individual's identity is unknown or untraceable. It goes beyond fictitious emails, usernames, and contact information to create a social media account but to deliberately hide their identity in interactions. They can say what they want without other users knowing who they are there. Digital accountability is when someone says or does something. The individuals are responsible and may face consequences for them. So, if they make an offensive post or break the law online, they will get fined, fired, banned, or arrested for their actions. However, accountability can also be positive, as when someone accomplishes something or does something positive online, they would be upvoted, liked, or rewarded. However, based on these definitions, they seem not to coexist since if someone is anonymous, how can we keep someone accountable? If everyone was anonymous and there was no accountability, nothing would stop someone from posting or doing whatever they want. However, with decreased anonymity, users are more likely to consider what they post online. While anonymity protects users and allows for personal expression, it raises accountability concerns. Therefore, balancing the two is critical to creating an ethical baseline.

Now that we have defined privacy and anonymity, we can look at their paradoxical nature and their pros and cons. One of the significant benefits of anonymity is that users can speak their minds, such as personal beliefs or politics, without fear of retribution. This lack of retribution means that there would be more unique ideas and experiences available. However, with that freedom, people can exploit it by criticizing, cyberbullying, or saying something outlandish without any repercussions. This con is called the Online Disinhibition Effect, where when in the right online environment, people will do certain activities online that they would not do in person (Suler, 2004).

On the other hand, privacy ensures that a user's files or information is not available to unauthorized personnel, so a company stores that information on a private database for easy access, and only those the user authorizes can see it. A significant pro for privacy is protecting top secret or confidential information such as medical records, social security numbers, and the Coke-a-Cola formula. If anyone released those to the public, someone's medical history, prescriptions, and personal information would be compromised, or Coke-a-Cola would have many competitors. However, too much privacy can lead to issues anonymity presents, where if not enough is shared, such as their name or some way to identify them, they can also avoid repercussions or people not believing their claims. Too much privacy can also lead to mistrust of data since the users do not know what the company will use their data for. So, while privacy and anonymity are essential to having open conversations, they bring many challenges that businesses must address.

Imagine an anonymous social media platform where nobody can be tracked back to their identity. Now, someone makes a post about their daughter's suicide and asks for assistance for

funds to pay for the funeral. There will be those who post helpful and supportive posts and donate funds, but then someone posts a picture of a noose or other references to their daughter's suicide. Should that person be reprimanded for their actions? To them, they thought the post was funny or warranted that response. However, to the family, seeing that message can cause multiple psychological problems. This scenario was an actual situation that occurred to Alexis Pilkington in 2010. However, because the posts were anonymous, the police could not identify who they were and determine if they were related to the suicide (Martinez). Imagine that the company has all the user data but allows someone to post anonymously. If something they say breaks the law, the police can get that information from the company. This scenario illustrates the complexities of privacy and anonymity as should the anonymity or privacy of the users be removed if their actions could harm someone mentally, physically, or emotionally? As much as anonymity and privacy give to users, I believe it has a larger potential to inflict damage to users. So, while users might claim that they want privacy and anonymity, they actually do not want the repercussions of their actions. On social media platforms, users can post whatever they want within the terms of service, however that does not mean they can avoid the reactions and issues of what they say (Sheppard, 2022).

All in all, privacy and anonymity are important to online users as users have an added sense of security and freedom to say and do what they want. However, there is a fine balance between the two and accountability, so the user can say what they want and feel validated, but also held accountable for their actions, positively or negatively. As we traverse a world with more data collection than ever before, we must find a balance that honors the user's freedom and security of data and who they share that with, while also ensuring that those who intend to inflict

harm are held accountable for their actions. Remember the freedom of speech does not equal the freedom of consequences.

Sources

- Choi, S. (2018, January 25). *Can anonymity and accountability coexist?*. Opensource.com.
<https://opensource.com/open-organization/18/1/balancing-accountability-and-anonymity>
- Digital Anonymity: Pros & cons*. Whispli. (n.d.). <https://resources.whispli.com/blog/pros-cons-digital-anonymity>
- Leetaru, K. (2019, July 28). *Is social media changing society through greater accountability?*. Forbes. <https://www.forbes.com/sites/kalevleetaru/2019/07/28/is-social-media-changing-society-through-greater-accountability/?sh=fe3761a6aca7>
- Martinez, E. (2010, March 26). *Alexis Pilkington brutally cyber bullied, even after her suicide*. CBS News. <https://www.cbsnews.com/news/alexis-pilkington-brutally-cyber-bullied-even-after-her-suicide/>
- Pros and cons of being anonymous online*. DeleteMe. (2023, November 15).
<https://joindeleteme.com/blog/pros-and-cons-of-being-anonymous-online/#con-anonymity-makes-us-meaner>
- Radauskas, G. (2023, November 15). *All social media apps collect user data but threads is king*. All social media apps collect user data but Threads is king.
<https://cybernews.com/news/threads-user-personal-data/>
- Sheppard, A. (2022, September 11). *Posting on social media may be impacting your job*. WINK News. <https://winknews.com/2022/09/09/posting-on-social-media-may-be-impacting-your-job/>
- Suler J. (2004). *The online disinhibition effect. Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society*, 7(3), 321–326.
<https://doi.org/10.1089/1094931041291295>
- What Is Digital Privacy—and How Can It Be Protected?*. Idx.us. (n.d.).
<https://www.idx.us/knowledge-center/what-is-digital-privacy-and-how-can-it-be-protected>
- Zhuo, J. (2010, November 30). *Where anonymity breeds contempt*. The New York Times.
<https://www.nytimes.com/2010/11/30/opinion/30zhuo.html>