

https://dspace.org/

Privacy in the Digital Age: Examining the Implications of Screenshotting Conversations

Ramkhelawan , Nishka

2025
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/50138
Ramkhelawan , Nishka. (2025). Privacy in the Digital Age: Examining the Implications of Screenshotting Conversations [Master's dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/50138

Downloaded from a DSpace repository. https://dspace.org/

PRIVACY IN THE DIGITAL AGE: EXAMINING THE IMPLICATIONS OF SCREENSHOTTING CONVERSATIONS

By

Nishka Ramkhelawan (Student Number: 1775294)

Supervisor: Professor Victoria Bronstein

Submitted in partial fulfilment of the requirements for the degree of

Master of Laws by Coursework and Research Report

at the University of the Witwatersrand, Johannesburg

Date: 28 February 2025

DECLARATION

I, 1775294, declare that this Research Report is my own, unaided work. It is submitted in partial fulfilment of the requirements for the degree of Master of Laws (by Coursework and Research Report) at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination in this or any other university.

I have submitted my final Research Report through TurnItIn and have attached the report to my submission.

Word Count: 10 492

ABSTRACT

In an era where digital communication reigns supreme, the unregulated practice of screenshotting and sharing private conversations on social media has emerged as a formidable threat to privacy. This research delves into the unconsidered implications of the screenshotting phenomenon, revealing how this feature disrupts traditional privacy expectations and compromises the integrity of online interactions.

Legal scholars have extensively discussed the right to privacy, emphasising its importance in the digital age. However, these discussions often overlook the specific challenges posed by the ease of capturing and sharing digital content using the screenshot feature. This research report argues that social media platforms are currently ill-equipped to handle the emerging screenshotting trend and proposes a proactive approach to privacy protection, advocating for technological measures that prompt users to request permission before taking screenshots. By applying a consent-based framework, this study offers a novel solution to enhance user control over private interactions.

The intellectual contribution of this paper lies in its forward-thinking strategies to address the inadequacies of current privacy measures, aiming to better protect individuals' privacy in an increasingly interconnected world. In addition, this report not only contributes to the academic discourse on digital privacy but also provides practical recommendations for policymakers and social media platforms to uphold and respect user privacy. By examining the policies of leading social media platforms such as Meta, Snapchat, and TikTok, the study highlights the varying degrees of protection against unauthorised screenshotting and underscores the need for more robust measures. The findings of this report emphasise the importance of a consent-based approach to online privacy, which can significantly enhance user trust and security in digital communications.

On the whole, this research report aspires to cultivate a safer and more respectful digital landscape on social media platforms, where privacy is not an afterthought, but an indispensable right that is actively protected and respected.

TABLE OF CONTENTS

Declaration 2

Abstract..... 3

1. Introduction..... 5

2. The internet's influence – An analysis on the evolution of the right to privacy 8

3. An examination of the concept and functionality of screenshots..... 13

4. Meta: Navigating privacy challenges in the age of end-to-end encryption and social media dominance 16

5. The ephemeral revolution: Snapchat's impact on digital privacy 22

6. TikTok: A global phenomenon and its privacy paradox..... 26

7. Beyond the screenshot: A forthcoming perspective for strengthening user privacy on social media..... 29

8. The legal stance on screenshotting private messages in South Africa.... 33

9. Conclusion 37

Bibliography 40

1. INTRODUCTION

Imagine this scenario: You are comfortably seated at home, unwinding after a long day and casually scrolling through Instagram. As you navigate through the endless stream of posts, a direct message notification catches your eye. Intrigued, you open your private messages to discover a random compliment from an unfamiliar Instagram user.[1] Amused by this unexpected interaction, you decide to engage in a conversation. Almost reflexively, you take a screenshot of this conversation and share it with your friends on WhatsApp Messenger, eager to share the amusement and get their views on the conversation, without considering the privacy rights of the Instagram user who sent the message or the potential legal implications of your actions.

A screenshot, essentially a digital capture of the content displayed on a screen, has become a ubiquitous tool in our daily interactions. However, the act of screenshotting and sharing private messages raises critical questions about consent and the boundaries of personal privacy on the internet.

Screenshotting has become so ingrained in our digital behaviour that it feels almost instinctual. It is a practice that many of us have engaged in, often without a second thought. The normalisation of this behaviour has led to a collective desensitisation, where potential privacy implications are overlooked. The ease with which social media users capture and share digital content has fundamentally altered our perception of privacy, making it imperative to re-evaluate the legal frameworks that govern our online interactions.

The right to privacy, enshrined in section 14 of the Constitution of the Republic of South Africa, 1996,[2] is a fundamental human right that protects individuals from unwarranted intrusions into their personal lives. However, the advent of digital technology and social media has posed significant challenges to the enforcement of this right.[3] This research report seeks to illuminate the ways in which the act of screenshotting and sharing private communications online infringes upon the right to privacy in South Africa's contemporary digital landscape.

[1] A 'user' refers to an individual who interacts with social media platforms.
[2] Hereinafter referred to as 'the Constitution'.
[3] Social media is considered to be an online medium for interactions between people.

Further, this report will provide a comprehensive analysis of the evolution of the right to privacy in South Africa, tracing its historical developments and its current interpretations. Thereafter, it will delve into the concept of a screenshot, exploring its technical aspects and its role in modern communication.

The study will then critically examine the policies and frameworks of three prominent social media platforms—Meta, Snapchat, and TikTok—regarding the practice of screenshotting and sharing of private conversations. The aforementioned platforms have become integral to our social interactions, each offering unique features that facilitate communication and content sharing. While these applications recognise that users frequently screenshot content and caution them against this, they have yet to implement robust measures to safeguard user privacy effectively.

Meta, for instance, provides users with the ability to report privacy violations but lacks proactive measures to prevent unauthorised screenshotting. Snapchat, known for its ephemeral messaging and screenshot notification feature, does not prevent the act of screenshotting itself. TikTok, a platform centred around video content, faces challenges in controlling the dissemination of screenshots and screen recordings to large audiences.

This research argues that there is an urgent need for more stringent and user-friendly protections concerning the screenshotting and sharing of private content and proposes a consent-based technological measure in an attempt to aid the harm caused by this trend.

Finally, a comprehensive analysis will be conducted on the legal stance adopted by South African law and the judiciary concerning the practice of capturing and distributing private conversations online.

Ultimately, this research report aims to contribute to the ongoing discourse on digital privacy by highlighting the inadequacies of current measures and proposing a forward-thinking approach to better protect individuals' privacy in today’s technologically driven world. By addressing the pervasive practice of screenshotting, this research underscores the necessity for comprehensive strategies that balance user engagement with the fundamental right to privacy.

The findings of this report aim to not only inform policymakers and social media platforms but also to empower users to make informed decisions about their online interactions.

2. THE INTERNET'S INFLUENCE – AN ANALYSIS ON THE EVOLUTION OF THE RIGHT TO PRIVACY

'People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.' – Mark Zuckerburg.[4]

Social networking has undoubtedly eroded traditional expectations of privacy. With the recent boom in technological advancements such as artificial intelligence, social media and quantum computing, there is an expectation that the law will progress in tandem with technology and will swiftly reshape itself to accommodate for these new developments.[5] However, the unfortunate reality is that technology is developing at a rapid pace and the law cannot reasonably respond fast enough to protect individuals and their constitutionally protected right to privacy.[6] This sentiment was echoed in the judgment of *H v W* 2013 (5) BCLR 554 (GSJ) where the court acknowledged that addressing the challenges arising from rapid technological advancements requires a high level of skill from the judiciary.[7]

The growing disconnect between technological advancements and legal protections underscores the critical importance of the right to privacy. Privacy is a fundamental human right that plays an essential role in preserving human dignity.[8] As O'Regan J remarked in *Khumalo and Others v Holomisa* 2002 (5) SA 401 (CC), the right to privacy 'recognises that human beings have a right to a sphere of intimacy and autonomy that should be protected from invasion. This right serves to foster human dignity.'[9]

Despite the absence of a formal definition for the term 'privacy', it is broadly

---

[4] The Guardian 'Privacy no longer a social norm, says Facebook founder' available at *https://www.theguardian.com/technology/2010/jan/11/facebook-privacy#:~:text=The%20rise%20of%20social%20networking,to%20Facebook%20founder%20Mark%20Zuckerber,* accessed on 29 August 2024.
[5] World Jurisprudence 'The Impact of Technology on Law: Transforming Legal Frameworks' available at *https://worldjurisprudence.com/impact-of-technology-on-law/,* accessed on 22 August 2024.
[6] World Economic Forum 'The law can't keep up with new tech. Here's how to close the gap' available at https://www.weforum.org/stories/2018/06/law-too-slow-for-new-tech-how-keep-up/, accessed on 22 August 2024.
[7] *H v W* para 8.
[8] Sylvia Papadopoulos & Sizwe Snail ka Mtuze (eds) *Cyberlaw@SA the law of the internet in South Africa* 4 ed (2022) 307.
[9] *Khumalo v Holomisa* para 27.

understood as

‘an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined should be excluded from the knowledge of outsiders and in respect of which there is a will that they be kept private.’[10]

South Africa has consistently demonstrated a deep-seated commitment to protecting the right to privacy. Despite our courts historically equating privacy and dignity[11], the landmark case of *O’Keeffe v Argus Printing and Publishing Co Ltd and Another* 1954 (3) SA 244 (C) recognised the right to privacy as a standalone, legally protected personality interest in 1954.

Privacy enjoys protection under the common law and the Constitution. In terms of the common law, actions such as search and seizure, intrusion, and the disclosure of private facts are considered violations of the right to privacy.[12] Moreover, it is imperative that individuals possess the autonomy to determine whether their personal information may be collected, intercepted, or utilised.[13] The judicial interpretation of the common law right to privacy has played a pivotal role in shaping the conceptualisation and application of this right within the constitutional framework.

The constitutional right to privacy is wider than that offered under the common law.[14] The right was formerly enshrined in section 13 of the Constitution of the Republic of South Africa, Act 200 of 1993, and has since been safeguarded under section 14 of the Constitution which reads:

‘[e]veryone has the right to privacy, which includes the right not to have—

(a) their person or home searched;

(b) their property searched;

[10] Johann Neethling *Die Reg op Privaatheid* (LLD thesis, University of South Africa, 1976) 287.
[11] J Neethling, JM Potgieter & A Roos *Neethling on Personality Rights* (2019) 308.
[12] Max Loubser (ed) et al *The Law of Delict in South Africa* 3 ed (2018) 89.
[13] Papadopoulos & Snail ka Mtuze op cit note 8 at 307.
[14] N Mashinini, ‘Unauthorised use of images in memes: Revisiting the privacy and identity debate’ (2022) 33 *Stellenbosch Law Review* at 660.

(c) their possessions seized; or

(d) the privacy of their communications infringed.'

It can be appreciated that within South African law, there is no exhaustive list of factual circumstances under which privacy may be violated and the notion of transformative constitutionalism[15] has been recognised by the judiciary when handing down its judgments.[16]

The coming of South Africa's newfound democratic era afforded our courts the opportunity to interpret the right to privacy within the context of the constitutional democracy. This was particularly seen in the case of *Bernstein and Others v Bester NO and Others* 1996 (4) BCLR 449 (CC) where the court characterised the right to privacy as a continuum by stating that '[p]rivacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly.'[17] Hence, the continuum begins in the wholly inviolable inner self, then moves to the impervious sanctum of the home and personal life and ends in the public realm where the right to privacy would only be remotely implicated.[18]

Similarly, the court in *The Investigating Directorate: Serious Economic Offences and others v Hyundai Motor Distributors (Pty) Ltd and others:* In re: *Hyundai Motors Distributors (Pty) Ltd and Others v Smit NO and Others* (2000) JOL 7338 (CC)[19] concurred that the right to privacy flows however, when people are in their offices, cars or on mobile telephones, they retain the right to be left alone.[20]

Accordingly, it is clear that our courts adopted the view that the privacy is not limited to a person's home.[21] Although, this right decreases the more an individual interacts with the public.[22]

---

[15] Transformative constitutionalism is the idea that the Constitution is not just a legal document but a tool for social transformation.
[16] Papadopoulos & Snail ka Mtuze op cit note 8 at 310.
[17] *Bernstein v Bester* para 67.
[18] *Mistry v Interim National Medical and Dental Council of South Africa and Others* 1997 (7) BCLR 933 (D) para 27.
[19] Hereinafter referred to the 'Hyundai Motors Distributors' case.
[20] *Hyundai Motor Distributors* para 16.
[21] Sylvia Papadopoulos & Sizwe Snail (eds)*Cyberlaw@SA III: The Law of the Internet in South Africa* 3 ed (2012) 277.
[22] *Hyundai Motor Distributors* supra note 19.

Privacy can be violated only when personal information is accessed by outsiders against the wishes and consent of the individual whose right to privacy is being infringed.[23] In evaluating whether there has been a breach of the right to privacy, both subjective and objective tests are employed.[24] The subjective test considers whether the individual in question genuinely expected privacy, based on their actions and attitudes towards the matter.[25] The objective test then determines whether this legitimate expectation of privacy is one that society would recognise as reasonable.[26] If the expectation is found to be reasonable, the court will apply the limitations clause to assess whether the privacy intrusion is justifiable within an open and democratic society that upholds human dignity, equality, and freedom.[27]

The longstanding legitimate expectation test has reliably guided privacy assessments for many years. However, the advent and pervasive use of social media present new challenges that undermine the quality and value of individuals' privacy.[28] Roos argues that that subscribing to a social networking service and completing a profile is similar to appearing in a public place.[29] Conversely, the Constitutional Court in *Botha v Smuts and another* (Campaign for Free Expression NPC as *amicus curiae*) 2024 (12) BCLR 1477 (CC) found that when a person puts something into the eyes of the public, that person has the right to determine the conditions and purpose for which it is in the public domain.[30] This juxtaposition of perspectives highlights the confusion surrounding the current position on privacy in the digital age.

While precedent has established that privacy exists on a sliding scale, the outdated notions of privacy have not aged well resulting in approaches which fail to address digital privacy reservations.[31] Additionally, the widespread engagement with social media has drastically altered the landscape and blurred the lines of traditional privacy expectations.[32] The expected privacy standards within digital communication networks

[23] Mashinini op cit note 14 at 661.
[24] Pierre De Vos (ed) et al *South African Constitutional Law in Context* 2 ed (2022) 462.
[25] Ibid.
[26] Ibid.
[27] Ibid note 23.
[28] Mashinini op cit note 14 at 669.
[29] Anneliese Roos 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *SALJ* at 398.
[30] *Botha v Smuts* para 133.
[31] Will Thomas DeVries 'Protecting Privacy in the Digital Age' (2003) 18 *Berkeley Technology Law Journal* at 283.
[32] Ibid note 28.

are not entirely predictable and the development of tools such as the screenshot feature amplifies this uncertainty.[33]

The court in *Heroldt v Wills* (2014) JOL 31479 (GSJ) pointed out that the dominance of social media has created a tension between rights which could not have been foreseen by the Roman Emperor Justinian's legal team, the learned Dutch legal writers of the seventeenth century or the founders of the Constitution.[34] The court went on to state that the common law needs to develop especially concerning privacy violations which take place on social media.[35]

Given that we live in a world where personal lives are becoming increasingly public, our courts are gradually having to deal with the challenges posed by social media and the practice of screenshotting and sharing private conversations further epitomises this issue as it directly challenges the traditional understanding of the right to privacy.

[33] Alexis Shore Ingber 'Protecting Privacy Communications through Law and Policy: The Case of the Screenshot Feature' (2024) 29 *Communications Law and Policy* at 1.
[34] *Heroldt v Wills* para 7.
[35] *Heroldt v Wills* supra para 31.

3. AN EXAMINATION OF THE CONCEPT AND FUNCTIONALITY OF SCREENSHOTS

A screenshot is a captured image of what appears on the screen of a computer or mobile device.[36] It is created by the operating system or software running on the device powering the display.[37] The primary functionality of screenshots includes record keeping, documentation and sharing.[38]

The art of screenshotting is not a novel trend. Screenshots, also referred to as screen captures or screen grabs, have a historical lineage tracing back to the early days of computing.[39]

The first known screenshot was taken in 1959 using a Polaroid camera to capture the image on a cathode-ray tube screen.[40] The Apple Macintosh, introduced in 1984, was the pioneering device to incorporate an integrated screenshotting tool, enabling its users to capture screen content via a keyboard shortcut. This, in turn, facilitated the ease of capturing and disseminating screen information.[41] Subsequently, in 2007, the iPhone, was the first mobile device to embed a screenshotting function, a feature which was soon adopted by Android devices in 2011.[42]

Whilst the introduction of screenshot technology represents a significant technological advancement, it also introduces the potential for privacy violations. The ease with which screenshots can be taken and shared on social media platforms creates new challenges for protecting individual privacy.

---

[36] Frances Corry 'Screenshot, save, share, shame: Making sense of new media through screenshots and public shame' (2021) 26 *First Monday* at 1.

[37] Webwise 'How to Take a Screenshot on your PC, phone or Tablet' available at *https://www.webwise.ie/parents/take-screenshot/#:~:text=A%20screenshot%20or%20screen%20capture,using%20particular%20keyboard%2Fbutton%20shortcuts,* accessed on 7 December 2024.

[38] TechSmith 'What is a Screenshot? The Basics' available at *https://www.techsmith.com/blog/screenshot/#:~:text=A%20screenshot%2C%20sometimes%20referred%20to,a%20reference%20point%20later%20on*, accessed on 7 December 2024.

[39] Ibid.

[40] Vice 'How the Screenshot Became One of the Internet's Most Powerful Tools' available at *https://www.vice.com/en/article/history-of-the-screenshot/#:~:text=The%20screenshot%20moved%20toward%20the,to%20send%20in%20their%20pictures,* accessed on 7 December 2024.

[41] Mac-History.Net 'The History of the Apple Macintosh' available at *https://www.mac-history.net/2021/02/10/history-apple-macintosh/*, accessed on 10 December 2024.

[42] Ibid note 40.

Screenshots capture and preserve digital interactions with a single click, making it possible to document conversations, transactions, and interactions. However, this convenience also means that private information can be exposed without consent and authorisation. The proliferation of social media amplifies this risk, as screenshots can be disseminated in an instant, reaching vast audiences and potentially causing significant harm. In addition, the screenshot feature has notoriously been used as a mechanism to leverage private information for public shaming and blackmail.[43]

The integration of screenshot technology has been extended into numerous facets of our everyday lives, including the judiciary and court systems. The American cases of *United States v. Vayner,* 769 F.3d 125 (2d Cir. 2014) and *Moroccanoil, Inc. v. Marc Anthony Cosmetics, Inc*., 57 F. Supp. 3d 1203 (C.D. Cal. 2014), saw screenshots of social media profiles being submitted as evidence, albeit the authenticity of the screenshots did not pass judicial muster.[44] On the opposite side of the globe, in the Australian case of *Voxson Pty Ltd v Telstra Corporation Limited (No 10)* (2018) 134 IPR 99; [2018] FCA 376, the applicant explicitly annexed screenshots from The Wayback Machine[45] to its court papers, demonstrating the growing reliance on screenshots.

South Africa was no exception to this trend and progressively adapted to this digital transformation, particularly through the enactment of several pieces of legislation including the Electronic Communications and Transactions Act 25 of 2002 and Protection of Personal Information Act 4 of 2013. Moreover, in July 2021, following an incident where photographs of former president Jacob Zuma were distributed on social media after his transfer to a Department of Correctional Services facility, the Information Regulator of South Africa issued a warning against publishing personal information, including photographs, without consent.[46]

---

[43] Corry op cit note 36 at 5.

[44] Forbes 'Can screenshots of text messages be used as digital evidence in court?' available at *https://www.forbes.com/sites/larsdaniel/2024/11/13/think-that-screenshot-is-proof-heres-why-it-might-not-hold-up-in-court/,* accessed on 10 December 2024.

[45] The Wayback Machine is a comprehensive digital archive that enables users to retrieve and explore historical versions of website content.

[46] Information Regulator (South Africa) 'Information Regulator warns against the processing of personal information of data subjects without their consent' available at *https://inforegulator.org.za/wp-content/uploads/2020/07/ms-20210713-ProcessingPersonalInfo.pdf,* accessed on 10 December 2024.

The implications of capturing and disseminating screenshots extend beyond legal ramifications into other aspects of individuals' lives including personal aspects, employment and mental health. This was demonstrated in the case of Amanda Todd, a 15-year-old Canadian student, who fell victim to severe cyberbullying and sexual extortion when screenshots of her private interactions were taken without her consent and shared publicly, leading to relentless online harassment.[47] The intense victimisation experienced by Amanda contributed to her mental health struggles, which lead to her suicide in 2012.[48] This incident is unfortunately not isolated and underscores the profound impact and potential harm of screenshots in contemporary society.

The unauthorised screenshotting and sharing of private conversations has become a global concern, particularly given the ease with which content can go 'viral' on the internet and social media.[49] A single screenshot can rapidly be disseminated across various platforms, reaching a vast audience within a matter of minutes. This occurrence not only exacerbates the potential for privacy breaches but also heightens the risk of misinformation and reputational harm. The viral nature of social media implies that once private information is exposed, it becomes exceedingly difficult to contain, leading to significant and often irreversible consequences for the individuals involved.

As the world navigates the complex terrain of the ever-evolving landscape of digital communication, it becomes clear that the solutions of yesterday are insufficient for the demands of today. Screenshots have evolved from a rudimentary method of capturing screen content into an indispensable tool deeply embedded in modern technology. However, despite its undeniable utility, screenshot technology has also emerged as a double-edged sword. On the one hand, it enables greater accessibility, productivity, and communication by allowing users to document and circulate screen content effortlessly. Though, on the other hand, the same simplicity and convenience of screenshots have given rise to significant ethical, moral and legal challenges.

---

[47] The Canandian Encyclopedia 'Amanda Todd Case' available at *https://www.thecanadianencyclopedia.ca/en/article/amanda-todd-case,* accessed on 20 January 2025.
[48] Ibid.
[49] The term 'viral' refers to the online phenomenon that occurs when a social media post exponentially grows in popularity, being viewed, shared, liked, or commented on by a large number of social media users in a very short period of time.

4. META: NAVIGATING PRIVACY CHALLENGES IN THE AGE OF END-TO-END ENCRYPTION AND SOCIAL MEDIA DOMINANCE

On or about 8 July 2023, Sarah Brady, a professional surf instructor and model, posted a series of screenshots on her Instagram profile of text messages between her and her celebrity boyfriend, Jonah Hill, wherein he expressed his 'boundaries' for their relationship.[50] The screenshotted conversations caused an internet uproar with many users accusing Jonah Hill of being 'controlling' and 'abusive'.[51] Regardless of the relationship dynamics at play, this incident raised questions about whether social media platforms endorse the act of screenshotting and sharing of private conversations, with many users expressing that it is neither appropriate nor proper to post private messages online for others to view and comment on.[52] This debate brings into focus the role of social media giants in moderating content and protecting user privacy.

Meta Platforms Incorporated, formerly known as Facebook Incorporated, is an American technology corporation that dominates the social media world with its extensive portfolio of programs and services that aims to connect billions of users globally and shape the way people communicate and share information.[53]

Meta's dominance is underscored by its ownership of several leading social media networks, including Facebook, Instagram and WhatsApp Messenger.[54]

In December 2021, Meta communicated its commitment to user privacy through the publication of its approach to safer private messaging.[55] This initiative aimed to

---

[50] Know Your Meme 'Jonah Hill's "Boundaries" Texts' available at *https://knowyourmeme.com/memes/events/jonah-hills-boundaries-texts*, accessed on 10 December 2024.
[51] Ibid.
[52] Ibid.
[53] Newsweek 'What is Meta, Exactly? What Facebook's rebrand means' available at *https://www.newsweek.com/facebook-meta-rebrand-stock-prices-explained-1643779#:~:text=Not%20only%20does%20the%20company,more%20than%20just%20social%20media*, accessed on 10 December 2024.
[54] Investopedia 'Top 3 Companies Owned by Facebook (Meta)' available at *https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp*, accessed on 10 December 2024.
[55] Meta 'Our Approach to Safer Private Messaging' available at *https://about.fb.com/news/2021/12/metas-approach-to-safer-private-messaging/*, accessed on 10 December 2024.

promote secure private messaging and prevent abuse on Meta's platforms.[56] In terms of this communique, Meta explicitly acknowledged the legitimate expectation of privacy of its users by stating that when its users connect on the platform, they 'expect their conversations to be private and secure, as most of us do'.[57]

By December 2023, Meta began the rollout of default end-to-end encryption for personal messages on its platforms.[58] This marked a significant milestone in Meta's privacy journey. Prior to this development and up until 2016, most of Meta's platforms only offered end-to-end encryption as an optional feature for private chats and calls.[59]

The introduction of default end-to-end encryption ensures that the contents of users' messages and calls are protected from the moment it leaves the user's device and up until it reaches the receiver's device.[60] This mechanism guarantees that no third party, not even Meta, is capable of accessing the message's content, thereby augmenting security and providing greater assurance to users.[61]

Other additional measures which Meta adopted to manage the sharing of information include preventing users from taking screenshots of profile pictures on platforms like WhatsApp Messenger and Facebook[62], two-factor authentication[63], disappearing messages[64] and, as of October 2024, blocking Instagram users from being able to screenshot or screen record 'view once'[65] or 'allow replay'[66] photos or videos sent via

---

[56] Ibid.
[57] Ibid.
[58] Meta 'End-to-End Encryption on Messenger Explained' available at *https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/#:~:text=End%2Dto%2Dend%20encryption%20helps,personal%20messages%20from%20other%20devices,* accessed on 11 December 2024.
[59] Meta 'Launching Default End-to-End Encryption on Messenger' available at *https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/,* accessed on 11 December 2024.
[60] TechTarget 'end-to-end encryption (E2EE)' available at *https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE*, accessed on 11 December 2024.
[61] Ibid note 59.
[62] Android Police 'WhatsApp now blocks you from taking screenshots of profile pictures' available at *https://www.androidpolice.com/whatsapp-blocks-you-from-taking-screenshots-profile-pictures/,* accessed on 11 December 2024.
[63] Two-factor authentication is a security process that requires users to provide two distinct forms of identification to verify their identity. The two factors are typically in the form of a password or pin that the user must input during the authentication process and a physical device that the user must possess to complete the authentication process.
[64] Disappearing messages affords users the option to set a timer to have messages disappear after they are seen by the recipient.
[65] View once messages allow the recipient to view the photo or video once.
[66] The allow replay feature loops the photo or video and permits the recipient to open and replay the photo or video one more time before it disappears.

private messages.[67] Despite these extensive measures, the practicality of Meta's policies has been challenged by the ease with which users can screenshot and share private messages.

Unsurprisingly, the Meta platform which has faced the most scrutiny to date is Facebook which is infamous for having a plethora of privacy and data breaches.[68] In *Largent v Reed and Pena* (Case No 2009-1823) 39th Judicial District of Pennsylvania, Franklin County (7 November 2011), the court acknowledged that Facebook 'has a detailed, ever-changing privacy policy'.[69] This observation perfectly describes the unpredictable and varying nature of privacy regulations on social media platforms.

Both Instagram and Facebook acknowledge that once content is shared, it can be further distributed by recipients[70] outside the intended audience.[71] This applies to direct and private messages as well.

Meta explicitly disclaims that '[f]or example, when you share a post or send a message to specific friends, they can download, screenshot or reshare it with anyone, on, across or off [Meta's] products.'[72]

This declaration was further reiterated by Whatsapp Messenger which notes that any user can capture screenshots of private chats or messages or make recordings of calls and circulate same via the platform.[73] Users are also at liberty to post these conversations on another social networking sites.[74]

In my view, the ability to screenshot and share content directly contradicts the privacy measures Meta have adopted. Messages exchanged between users are never entirely secure as purported when the end-to-end encryption was introduced. A recipient can screenshot and share these conversations without the sender's[75]

---

[67] BBC 'Instagram defends new teen safety features after criticism' available at *https://www.bbc.com/news/articles/cdd4vn6p601o,* accessed on 11 December 2024.
[68] Firewall Times 'Facebook Data Breaches: Full Timeline Through 2023' available at *https://firewalltimes.com/facebook-data-breach-timeline/*, accessed on 11 December 2024.
[69] *Largent v Reed and Pena* at 4.
[70] 'Recipient' shall mean a social media user that receives content.
[71] Meta Privacy Center 'Content that others share or reshare about you' available at *https://www.facebook.com/privacy/policy?subpage=3.subpage.2-ContentOthersShareOr,* accessed on 12 December 2024.
[72] Ibid.
[73] WhatsApp 'Whatsapp Privacy Policy' available at *https://www.whatsapp.com/legal/privacy-policy*, accessed on 12 December 2024.
[74] Ibid.
[75] 'Sender' shall mean a social media user that transmits content.

knowledge. For instance, a sender may share personal or confidential information with a recipient, believing it to be secure under Meta's end-to-end encryption, however, the recipient can screenshot the conversation and share it publicly or privately with third parties and on platforms not bound by Meta's guidelines and community standards. Grimmelman, when examining the effectiveness of Facebook's privacy policy correctly pointed out that 'to the extent that it has any binding effect at all, Facebook's privacy policy binds only Facebook. There are plenty of other actors, including other users, [a]pplication developers, and law enforcement agents, who can use Facebook's data to invade privacy.'[76]

In light of the aforementioned considerations, a pertinent question arises: what can users do to guard against screenshots being publicly shared?

Most social networking services include a feature that allows users to report content shared about them if they find it inappropriate. However, this remedy may be insufficient and impractical. If a screenshot is shared privately to a third party, the sender would have no knowledge that their information was shared in the first place. Moreover, in certain circumstances, the act of screenshotting and sharing private conversations may not directly constitute a privacy violation according to Meta's community standards.

Facebook allows users to report privacy violations if it falls within the ambit of the following categories:[77]

1. Report a photo or video on Facebook that violates a user's privacy. In these circumstances, if a user is tagged in content which is does not agree with, the user is encouraged to remove the tag. Alternatively, the user may submit a form which Facebook will consider.
2. Report a photo or video that violates the privacy of a child.
3. Report images that violate the privacy of a sick, hospitalised or otherwise incapacitated people.

However, it is important to note that Facebook is notoriously known for often not

[76] James Grimmelmann 'Saving Facebook' (2009) 94 *Iowa Law Review* at 1183.
[77] Facebook Help Centre 'Reporting a Privacy Violation' available at *https://www.facebook.com/help/1561472897490627/?helpref=hc_fnav*, accessed on 12 December 2024.

considering reported content as a violation of its community standard and may not take action in certain circumstances.[78]

Instagram, on the other hand, provides users with a broader range of options for reporting posts or profiles. Users can report content for reasons such as spam, misinformation, or other content that they find disagreeable.[79]

Whatsapp Messenger affords users the remedy to report problematic content. Alternatively, users can block problematic users.[80] However, it remains unclear what would be considered 'problematic content' or a 'problematic user' in this context.

On Threads, a byproduct of Instagram, users have the option to share content with either a public or private audience.[81] With a private profile, only approved followers can see and interact with the shared content.[82] In contrast, a public profile allows anyone, both on and off the platform, to view and engage with the content.[83] Naturally, this implies that if a user with a public profile screenshots and shares a private conversation, any third party can access and spread this information. Moreover, it is implied that individuals with public profiles will have a reduced legitimate expectation of privacy in respect of their communications and interactions as compared to those with private profiles.

Thus, it can be seen that while Meta has made commendable progress in enhancing user privacy through its newly introduced security measures, the ease with which users can screenshot and share content remains a significant challenge. It can be argued that the current measures Meta have in place to address potential privacy breaches may be too little, too late.

In addition, Meta's lack of proactive measures to prevent unauthorised screenshotting means that if a screenshot is taken and shared, the sender of the message would remain unaware that their information is being circulated. This lack of control over the

---

[78] First Monday 'Report and repeat: Investigating Facebook's hate speech removal process' available at *https://firstmonday.org/ojs/index.php/fm/article/download/10288/8327,* accessed on 28 January 2025.

[79] Instagram Help Centre 'Report a post or profile on Instagram' available at *https://help.instagram.com/192435014247952,* accessed on 12 December 2024.

[80] WhatsApp Help Center 'About reporting and blocking someone on WhatsApp' available at *https://faq.whatsapp.com/414631957536067*, accessed on 12 December 2024.

[81] Instagram Help Centre 'Threads Supplemental Privacy Policy' available at *https://help.instagram.com/515230437301944*, accessed on 12 December 2024.

[82] Ibid.

[83] Ibid.

dissemination of their private communications may leave users vulnerable to privacy breaches.

Lastly, perhaps the most disconcerting aspect of Meta's privacy policies is the inconsistency across its various platforms, with each platform having different interpretations of what constitutes a breach of policies and guidelines. This highlights a critical gap in Meta's privacy framework, underscoring the necessity for more comprehensive solutions to safeguard user privacy and security across its widely used interconnected digital platforms.

5. THE EPHEMERAL REVOLUTION: SNAPCHAT'S IMPACT ON DIGITAL PRIVACY

'Just like in real life, there are some moments you want to share privately with your close friends, and others that you want to share publicly. That's why from day one our philosophy has been to delete content by default and to give Snapchatters[84] control by providing the tools that allow them to decide what happens with their content, like who to share it with or when to save it.' – Snapchat Inc.[85]

Snapchat, a revolutionary smart-phone application that encourages photo-sharing between users, was pioneered in 2011.[86] This introduction marked the beginning of a new era of communicating as it quickly began to carve out a unique niche in the social media landscape. The platform's distinctive feature of ephemeral messaging, where photos and videos disappear after being viewed, set it apart from other social media applications at that time and resonated with users seeking more private and transient forms of communication.[87]

One of Snapchat's most notable features is its screenshot notification system. This functionality alerts users when someone takes a screenshot of their message or story, thereby enhancing the sense of privacy and control over shared content.[88] This mechanism not only provides users with a sense of security but also underscores the application's commitment to encourage transparency amongst users.[89] Snapchat's screenshot notification system illustrates that social media platforms have the ability to effectively regulate and oversee the practice of screenshotting within their applications.

---

[84] 'Snapchatters' refers to persons who use the Snapchat platform to send and receive snaps, interact with users, and engage with the platform's various features.
[85] Snapchat Inc 'Privacy Policy' available at *https://values.snap.com/privacy/privacy-policy,* accessed on 20 December 2024.
[86] Justin C. Velton, Rauf Arif & Delane Moehring 'Managing Disclosure through Social Media: How Snapchat is Shaking Boundaries of Privacy Perceptions' (2017) 6 *The Journal of Social Media in Society* 224.
[87] GB Times 'Why do some Snapchat messages disappear?' available at *https://gbtimes.com/why-do-some-snapchat-messages-disappear/,* accessed on 20 December 2024.
[88] TDFTips 'Snapchat Screenshot Notifications: Navigating Privacy Concerns and Understanding Alert Features' available at *https://tdftips.com/blog/snapchat-screenshot-notifications-privacy-and-screenshot-alerts/,* accessed on 20 December 2024.
[89] Ibid note 85.

Other additional features which make Snapchat unique include, recipients must maintain tactile contact with the device's touch screen and content is only shared with the specific users selected by the sender.[90]

Unlike other social networking services, Snapchat explicitly mentions the practice of screenshotting on the platform and informs users that others may view content and 'can always screenshot that content, save it, or copy it outside the Snapchat app'.[91] Moreover, Snapchat goes on to caution users not to send messages or share content that they would not want someone to save or share.[92]

Snapchat places a pronounced emphasis on user privacy. In articulating the application's privacy principles, the platform states that content deletion is the default practice.[93] This means that once messages are viewed or have expired, they are removed from the server.[94] Even with these safeguards in place, the platform advises users that screenshots can be captured and content may be saved using third party applications.[95] Consequently, it is recommended that users only share 'need-to-know stuff' with other users that they unequivocally trust'.[96]

In addition, should there be a safety concern, a violation of Snapchat's community guidelines or breach of the terms of service, users are encouraged to report the content via Snapchat's in-app reporting.[97] According to Snapchat, only content which violates its community guidelines or terms of service will be removed from the platform.[98] For ease of reference, some of the actions that may be considered a violation on the platform include illegal activities, harassment and bullying and harmful, false or deceptive information.[99]

---

[90] Lukas Piwek & Adam Joinson '"What do they snapchat about?" Patterns of use in time-limited instant messaging service' 2016 *Computers in Human Behavior* 359.
[91] Ibid note 85.
[92] Ibid.
[93] Snapchat Inc 'Our Privacy Principles' available at *https://values.snap.com/privacy/privacy-principles*, accessed on 20 December 2024.
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Snapchat Inc 'Snapchat Safety Center' available at *https://values.snap.com/safety/safety-center,* accessed on 21 December 2024.
[98] Snapchat Inc 'Report a Safety Concern' available at *https://values.snap.com/safety/safety-reporting*, accessed on 21 December 2024.
[99] Snapchat Inc 'Community Guidelines' available at *https://values.snap.com/privacy/transparency/community-guidelines,* accessed on 21 December 2024.

On interpretation of Snapchat's policies and documents, it can be seen that the platform places a significant emphasis on user responsibility, particularly regarding screenshotting of content. Snapchat's extensive warnings about the risks associated with screenshotting is refreshing and demonstrates the platform's awareness of the potential dangers and privacy violations that can occur if private conversations are captured and shared. Notwithstanding, Snapchat, albeit quite naively, places the responsibility squarely on users to avoid sharing content that they would not be comfortable having disseminated publicly. This could potentially undermine the safe and private environment that Snapchat aims to foster for its users.

Although users agree to respect the privacy of others as stipulated in the terms of service upon signup,[100] the platform's frequent warnings about screenshotting content indicates that reporting such actions may not be effective and may not directly violate Snapchat's community guidelines or terms of services. Depending on the content of the screenshot and given the numerous cautions issued by Snapchat concerning screenshots, it appears improbable that a sender can report a screenshot to Snapchat solely on the basis that screenshot was taken without the necessary consent. In such a case, the only available remedy to a user is to unsubscribe, hide the content, or unfriend or block the sender.[101]

Despite Snapchat's cautions, it has been argued that since content shared via Snapchat disappears within approximately ten seconds of receipt, users are encouraged to share data that they would not normally share.[102] This behaviour is even more risky and could lead to greater damage if the content is screenshotted and shared without the user's consent. The ephemeral nature of Snapchat's messaging system may create a false sense of security, prompting users to disclose sensitive or personal information that they might otherwise withhold on other social media platforms. The potential for such content to be captured and disseminated through screenshots may exacerbate the risk of privacy violations as, while Snapchat notifies users when a screenshot has been taken, it does not preclude the other party from capturing the screenshot.

---

[100] Snapchat Inc 'Snap Terms of Service' available at *https://www.snap.com/terms?lang=en-US*, accessed on 21 December 2024.
[101] Ibid note 85.
[102] Ibid note 86.

Notwithstanding, Snapchat stands as a testament to the power of innovation in addressing privacy concerns. Its ephemeral messaging and screenshot notification system has not only redefined how users share moments but also challenged the conventional norms of digital permanence. Snapchat's approach, while not without its flaws, offers a glimpse into a future where privacy and control are of paramount importance. It invites individuals to rethink their digital interactions, urging a more mindful and responsible engagement with technology.

6. TIKTOK: A GLOBAL PHENOMENON AND ITS PRIVACY PARADOX

Since its launch in 2016, TikTok has taken the world by storm with its viral lip-sync videos, dance trends and comedic skits.[103] The application is a short-form video sharing and social media platform that allows users to produce, share and discover content.[104] Users leverage the platform to express their creativity, participate in trending challenges and connect with a global community through engaging and entertaining videos.

According to TikTok's terms of service, users are permitted to upload, post, transmit or otherwise make content available through the platform.[105] The content can take the form of text, photographs, videos and sound recordings.[106] Users are further permitted to extract all or any portion of content created by other users to produce and disseminate further content.[107] Any content uploaded or transmitted through TikTok can be shared through third party social media platforms including, Instagram, Facebook, Youtube and X (formerly knowns as 'Twitter').[108]

Although the platform is known for its short-form videos, it does have a direct messaging feature. To this end, users can interact with each other, send messages and share content directly through this mechanism.[109] TikTok collects the information[110] users provide when they compose, send or receive messages through the platforms direct messaging functionalities.[111]

---

[103] Digital School of Marketing 'How TikTok has taken over social media' available at *https://digitalschoolofmarketing.co.za/social-media-marketing-blog/how-tiktok-has-taken-over-social-media-marketing/,* accessed on 3 January 2025.
[104] Binitie, Amaka Patience & Babatunde J. Obetayo 'Evaluating the privacy issues, potential risks and security measures associated with using social media platforms' (2024) 3 *International Journal of African Research and Sustainability Studies* at 114.
[105] TikTok 'Terms of Service' available at *https://www.tiktok.com/legal/page/row/terms-of-service/en*, accessed on 3 January 2024.
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] TikTok 'Direct Messages' available at *https://support.tiktok.com/en/using-tiktok/messaging-and-notifications/direct-message-settings,* accessed on 4 January 2024.
[110] This information includes the content of the message and information about the message, such as when it was sent, received, or read, and message participants.
[111] TikTok 'Privacy Policy' available at *https://www.tiktok.com/legal/page/row/privacy-policy/en*, accessed on 4 January 2025.

TikTok cautions its users that the messages they send to others on the platform will be accessible by those recipients and that TikTok will not be 'responsible for the manner in which those users use or share the messages.'[112] Unlike Meta, which has implemented an end-to-end encryption communication system, TikTok actively scans, analyses and reviews user content, messages and associated metadata to ensure safety, security and adherence of the policies on the platform.[113]

Interestingly, TikTok ambiguously disclaims that any content made available on the platform will be deemed non-confidential and non-proprietary.[114] One can assume that this would apply to the content shared via the direct messaging feature as well.

Accordingly, and to prevent unwarranted privacy invasions, users are urged not to share any content on the platform that they consider to be confidential or proprietary.[115] In my opinion, this statement is contradictory and does not align with TikTok's community principles, particularly those ideologies relating to the protection of individual privacy.

TikTok proclaims that it is 'committed to protecting and respecting the privacy of [its] community and of individuals who are shown in content on the platform. [TikTok] seeks to ensure that content shared on the platform does not expose anyone's personal information or invade their intimate privacy.'[116] Although this statement may initially appear reassuring, it is inherently problematic. First, TikTok does not state how it protects and respects the privacy of its users, nor does it mention any of the safeguards put in place to protect user privacy. Furthermore, and in any event, the platform explicitly disclaims that any content shared on the application is non-confidential. In this case, it is unclear whether users have a legitimate expectation of privacy when using the application or whether such expectation is vitiated upon sign up. If all the content on the application is deemed to be 'non-confidential', it is uncertain what 'privacy' TikTok is seeking to protect. It seems as though the direct messaging feature on the platform merely creates the façade of privacy without actually affording users such privilege.

---

[112] Ibid.
[113] Ibid.
[114] Ibid note 105.
[115] Ibid.
[116] TikTok 'Community Principles' available at *https://www.tiktok.com/community-guidelines/en/community-principles,* accessed on 4 January 2025.

The vagueness displayed in TikTok's policies and guidelines is unsettling. Although the platform purportedly has measures in place to protect the privacy of its users, it remains unclear how these measures are enforced and regulated.

In addition, TikTok does not cater for the potential risk of screenshotting and sharing conversations. Whilst the platform does send inbox notifications for new followers, latest messages and other activities, it does not notify a user when a screenshot has been taken of their private messages.[117] This may be an unanticipated risk seeing as content on TikTok tends to go viral quicker compared to any other social media platforms currently available.[118] Naturally, this means that if private messages are screenshotted and shared on TikTok, they possess the potential of reaching a larger audience which may result in detrimental consequences for the users involved.

TikTok's rapid rise has not been without controversy. The platform has raised significant privacy law and security concerns, particularly regarding data security which has led to calls for a ban of the platform in several countries including the United States of America, India and Uzbekistan.[119] The recent ruling in *TikTok, Inc. v. Garland*, 604 U.S. (2025) (Supreme Court of the United States decision) further emphasises the platform's ongoing privacy and security challenges by mandating a ban on TikTok's operations in the US unless it severs ties with its Chinese parent company. The platform's reluctance to adopt a proactive approach to user privacy may reflect its primary purpose and usage. TikTok might be better suited for creating and sharing public content rather than engaging in private conversations. This would ultimately render its direct messaging feature largely redundant. It seems as if the platform's design and policies are more aligned with fostering public engagement and content creation, rather than ensuring the confidentiality and privacy of user communications. As a result, users should exercise caution when using TikTok for private interactions as the platform's infrastructure and policies may not provide adequate protection for sensitive information.

---

[117] Context 'US TikTok ban: Which other countries have banned the app?' available at *https://www.context.news/big-tech/us-tiktok-ban-which-other-countries-have-banned-the-app,* accessed on 4 January 2025.

[118] Front Row 'The power of TikTok virality' available at *https://www.frontrowgroup.com/insight/the-power-of-tiktok-virality/,* accessed on 4 January 2025.

[119] Newsweek 'TikTok Ban 2025 Explained: What is actually happening?' available at *https://www.newsweek.com/tiktok-ban-2025-supreme-court-2012881,* accessed on 4 January 2025.

7. BEYOND THE SCREENSHOT: A FORTHCOMING PERSPECTIVE FOR STRENGTHENING USER PRIVACY ON SOCIAL MEDIA

The effortlessness in which screenshots can be captured and shared has precipitated significant concerns regarding user privacy on social media platforms. Despite the pervasive nature of this issue, many digital platforms have not implemented adequate measures to protect users from the potential privacy violations associated with screenshotting and sharing private conversations. This oversight underscores a critical gap in the privacy frameworks of these social networking services and highlights the need for more robust and proactive strategies to safeguard user privacy on these applications.

It appears that numerous social media platforms, rather than adopting a preventative stance to protect its users from the risks involved in the unauthorised screenshotting of private conversations, merely assert that users should refrain from sharing sensitive information on the application. If this approach is to be adopted, social media platforms must cease perpetuating the illusion of privacy online and refrain from marketing these applications as tools for facilitating connections and private conversations amongst its users.[120] Regrettably, individuals frequently neglect to review social media policies, thereby rendering themselves vulnerable and uninformed about which platforms prioritise their privacy.[121]

Notwithstanding, it is widely recognised that social media is the predominant medium for communication nowadays. In contemporary society, individuals use social media platforms to not only communicate with friends and family but also their healthcare providers, legal advisors, and mental health professionals, all of whom are likely to gain access to sensitive information about the sender during communication. Naturally, privacy should not be lost when a person confides in someone and in these situations, a legitimate expectation of privacy should continuously exist.[122] Therefore,

[120] For example, WhatsApp Messenger is marketed as 'simple, reliable, private messaging and calling for free, available all over the world' whilst Instagram states that its aim is to bring people closer together.
[121] Jonathan A. Obar & Anne Oeldorf-Hirsch 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' 2018 *Information, Communication & Society* 132.
[122] Ingber op cit note 33 at 3.

whilst users should be mindful of their online interactions, the assertion that they should only share non-private information on these platforms is patently ignorant.

Given the everyday role of these interactions, it is imperative to consider potential measures that can effectively safeguard user privacy online. Garg adopts a stringent position, advocating for the complete prohibition of the screenshotting feature on social media platforms.[123] Considering the proliferation of the screenshotting phenomenon, this approach may represent a prudent measure to enhance user privacy and mitigate the risk of potential online privacy violations, especially those risks relating to the cross-platform transfer of screenshotted information. Meta, whilst it has not implemented a comprehensive ban, has imposed restrictions on screenshotting certain features, such as profile pictures, on its platforms. Whilst the proposition advanced by Garg may soon become a reality for users, it is important to acknowledge that the implementation of such a ban across all social media platforms is unlikely given that each application addresses user privacy differently. Moreover, the feasibility of enforcing such a ban raises questions about the balance between user convenience and privacy protection online.

Meta, TikTok, and Snapchat have implemented varying degrees of privacy measures to address the issue of unauthorised screenshotting. In comparison of these social networking services, it can be seen that Meta and TikTok have implemented some privacy measures, but do not offer the same level of protection as Snapchat which specifically caters to the act of screenshotting content.

TikTok has not implemented specific measures to prevent or notify users of unauthorised screenshotting. On the other hand, Meta, whilst it has introduced several privacy features, these measures are reactive rather than proactive.

Snapchat currently offers the most comprehensive safeguards, providing users with greater control and awareness over their private conversations. Upon the recipient taking a screenshot of a private message, Snapchat instantaneously notifies the sender of this action. Snapchat's screenshot feature demonstrates that social media platforms have the technological capabilities to detect and notify participants in a conversation when a screenshot is taken. Furthermore, it illustrates that it is possible

[123] Ritvik Garg 'Privacy v Social Media' (2019) 12 *Supermo Amicus* at 5.

to inform parties to the conversation that a screenshot has been taken (which is a deterrent in itself).

Snapchat's screenshot notification feature is particularly interesting from a legal standpoint as individuals are enabled to initiate legal proceedings for privacy infringement upon becoming aware of the intrusion.[124] Since a Snapchat user is promptly informed of any privacy violation through the screenshot notification system, they may immediately resort to legal recourse to remedy the possible privacy infringement. Snapchat's notification feature not only serves as a deterrent against unauthorised screenshotting but also empowers users by providing them with the necessary information to take timely action.

Unfortunately, it is well known that taking legal action is time consuming, expensive and taxing. This may discourage most users from acting upon a potential privacy violation. Moreover, most social media platforms, like Snapchat, do not stop the act of screenshotting itself but merely offer assistance once a privacy violation has already occurred. This approach is insufficient in addressing the root cause of the problem and often leaves users feeling vulnerable and unsupported.

In my opinion, a pre-emptive way to address the unauthorised screenshotting of private conversations, without resorting to the complete prohibition suggested by Garg, would be to require explicit consent from the parties engaged in the conversation before a screenshot is taken. This could be implemented through technological measures that prompt users to request permission from the other party before capturing a screenshot. Such a feature would empower users to control the dissemination of their private conversations and reduce the risk of unauthorised sharing. Furthermore, mandating explicit consent prior to capturing a screenshot would enhance users' autonomy over their private interactions and mitigate any ambiguity regarding the authorisation to screenshot or document a conversation. The court in *Tshabalala-Msimang and Medi-Clinic Ltd v Makhanya* 2008 (3) BCLR 338 (W) noted that where a person seeks publicity and consents to it, this individual cannot object when his or her actions are publicised.[125] In essence, this consent-based

[124] Carter- Ruck 'Defamation and Privacy Law in South Africa' available at *https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-south-africa/*, accessed on 18 January 2025.
[125] *Tshabalala-Msimang v Makhanya* para 40.

approach will assist in developing a culture of approval and mutual respect on social media platforms.

To effectively mitigate the risk of screenshotting conversations, a clear and explicit demand must be made to social media platforms. This demand should facilitate a dialogue on the technical measures required to address this issue. It is insufficient for platforms to solely promote functionalities like end-to-end encryption without making a genuine effort to rectify this apparent loophole. If social media platforms are unable to address the issue of screenshotting conversations, they should provide a clear and detailed explanation to users regarding the reasons for their inability to do so. To this end, it is essential that platform developers assume the responsibility of creating a digital ecosystem that values and protects user privacy.

8. THE LEGAL STANCE ON SCREENSHOTTING PRIVATE MESSAGES IN SOUTH AFRICA

In South Africa, the judiciary has yet to resolve whether the act of screenshotting and sharing private conversations online infringes upon the right to privacy. However, this conundrum is likely to be one that our courts will have to consider in the near future.

In *Botha v Smuts* the Constitutional Court in briefly encountered a situation where the first respondent published a WhatsApp Messenger conversation between himself and the applicant on Facebook.[126] Regrettably, the court did not thoroughly examine the implications of sharing the screenshotted conversation nor did the court take into account that WhatsApp Messenger operates as an end-to-end encrypted platform. Nevertheless, a court would have to address this issue on a case by case basis with due consideration given to the specific context and facts of each case.

The level at which a person expects privacy is circumstantial and dependable on the existence of legal interest.[127] For example, within the context of online environments, privacy encompasses the right to determine the degree to which one's personal data is shared and made accessible on social media platforms.[128] This correlates with section 14(*d*) of the Constitution which provides that everyone has the right not to have the privacy of their communications infringed. Whilst the courts have not yet dealt with the specific issue of screenshotting and sharing private conversations, they have viewed privacy as 'an individual condition of life characterised by seclusion from the public and publicity'.[129]

Applying this legal framework to the issue at hand, imagine a situation where a sender transmits a private message to a recipient via WhatsApp Messenger. The recipient, who maintains a public Instagram profile, captures an unauthorised screenshot of this message and subsequently shares it on Instagram, publicly shaming and embarrassing the sender. Would the sender succeed with a privacy infringement claim?

---

[126] *Botha v Smuts* supra note 30 para 8.
[127] Mashinini op cit note 14 at 661.
[128] Senthil Kumar N, Saravanakumar K & Deepa K 'On Privacy and Security in Social Media – A Comprehensive Study' (2016) 78 *Procedia Computer Science* at 118.
[129] *Bernstein v Bester* supra note 17 para 68.

The above situation could give rise to two possible invasions of privacy in one cause of action in that the recipient screenshotted the conversation without the sender's consent and then proceeded to post same on the internet.[130]

As previously established, it is trite law that privacy rests on a continuum. Accordingly, the more a person interacts with the public, the more their scope of privacy decreases.[131] The judicial inquiry to determine whether the conduct in question constitutes an infringement of an individual's right to privacy entails both subjective and objective assessments.[132] In so far as the subjective test is concerned, the court will evaluate the sender's conduct and the circumstances surrounding the alleged unauthorised disclosure of private information.[133] The court in *National Media Ltd and Another v Jooste* 1996 (2) All SA 510 (A) was of the view the 'a person is entitled to decide when and under what conditions private facts may be made public.'[134] In the context of screenshotting private messages to fulfil the requirement of the subjective test, it is prima facie reasonable to assert that the sender holds a subjective expectation of privacy when sending a private message to the recipient. In most circumstances, the sender's subjective expectation would not have been that the conversation would be revealed to the public at large by the recipient. This is particularly heightened when the message is transmitted via an end-to-end encrypted platform such as WhatsApp Messenger or a social media application that speaks to protecting user privacy. Moreover, during a private conversation on a social media platform, it is not the sender who is interacting with the public but rather the recipient who shared the messages online.

Objectively, the court will assess whether society acknowledges the subjective expectation of privacy as reasonable.[135] This test is particularly intriguing given the increasing prevalence of screenshots transitioning from the private sphere to the public domain.[136]

---

[130] In *Bernstein v Bester,* the court found that a 'breach of privacy could occur either by way of an unlawful intrusion upon the personal privacy of another, or by way of unlawful disclosure of private facts about a person.'
[131] *Bernstein v Bester* supra note 17 para 67.
[132] De Vos et al op cit note 24.
[133] Mashinini op cit note 14 at 660.
[134] *National Media Ltd and Another v Jooste* para 15.
[135] De Vos et al op cit note 24.
[136] Dazed 'Receipts culture has gone too far' available at *https://www.dazeddigital.com/science-tech/article/56366/1/receipts-culture-has-gone-too-far,* accessed on 20 January 2025.

The court would likely take into account the sender's public status, such as whether the sender is an influencer[137], celebrity, or public figure.[138] Historically, the courts have exhibited greater stringency in safeguarding the privacy of private individuals, while adopting a more relaxed approach towards the privacy of public figures.[139] As it stands, it is unclear whether a public figure with a significant social media presence has a reduced expectation of privacy when sending a private message as compared to a private individual.

Additionally, it is prudent for the court to consider the social media presence of the recipient who captured and disseminated the conversation. If the recipient is a public figure with a significant social media following, it is probable that the post reached a wider audience. The status of both parties will be a critical factor, particularly in relation to the post's potential to go viral and the degree to which it engages viewers.[140]

The nature of the post is also an important consideration. If the recipient shared the content as an Instagram story, it would typically disappear after twenty four hours, thereby limiting its visibility and potential impact.[141] However, if the content was posted on the recipient's Instagram feed, it would remain accessible to their followers and the broader public until the recipient chooses to remove it.[142] This distinction is significant as it affects the duration and extent of the post's exposure. Posts on an Instagram feed, for example, can accumulate likes, comments, and shares over time, thereby increasing their reach and potential influence.

Having regard to the above it can be seen that the legal stance on screenshotting private messages in South Africa remains an evolving area of law. The judiciary has yet to definitively address whether such actions constitute an infringement of the right to privacy. As this area of law continues to develop, it is crucial for the courts to provide

---

[137] An influencer is a person who has the ability to affect the decisions of others because of his or her authority, knowledge, position, or relationship with his or her audience on social media.
[138] Mashinini op cit note 14 at 662.
[139] *H v W* supra note 7 para 45.
[140] This is problematic from a journalistic aspect. As journalism is becoming democratised, anyone can claim to be a journalist online.
[141] Instagram 'Instagram Stories' available at *https://about.instagram.com/features/stories#:~:text=at%20the%20bottom.-,Stories%20disappear%20from%20your%20profile%2C%20Feed%20and%20Direct%20inbox%20after,will%20appear%20as%20one%20clip,* accessed on 20 January 2025.
[142] Keyhole 'Instagram Posts vs Instagram Stories: Is one better than the other?' available at *https://keyhole.co/blog/instagram-posts-vs-instagram-stories/#:~:text=Instagram%20posts%20are%20evergreen.,pretty%20great%20Instagram%20post%20guide,* accessed on 20 January 2025.

clear guidance on the privacy rights of social media users and to address the complexities of privacy in the context of modern communication technologies.

9. CONCLUSION

The primary aim of this research report was to reflect on the practice of screenshotting and sharing conversations on social media within the context of South Africa's legal landscape. This exploration sought to understand how this prevalent digital behaviour intersects with the right to privacy in South African law. This issue has been addressed through a detailed examination of the evolution of privacy rights, an exploration of the screenshot feature, an analysis of the policies and guidelines of major social media platforms, and an evaluation of the current legal stance on screenshotting private messages.

Initially, the historical development of the right to privacy in South Africa was discussed, highlighting its constitutional and common law foundations. The analysis revealed that the right to privacy has evolved significantly, however, the advent of digital technology and social media is posing new challenges to its enforcement.

The technical aspects of screenshots and its role in modern communication were then explored. It was shown that screenshots, while useful for preserving information and sharing moments, raise critical questions about consent and the boundaries of personal privacy. The ease with which social media users can capture and share digital content has fundamentally altered perceptions of privacy, necessitating a re-evaluation of legal frameworks.

Thereafter, the privacy policies and guidelines of Meta, Snapchat, and TikTok regarding screenshotting and sharing private conversations were critically examined. Each platform's approach to user privacy was analysed, revealing varying degrees of protection and highlighting the need for more robust measures. Meta's introduction of end-to-end encryption was noted as a significant step towards enhancing user privacy. However, it was also found that despite Meta's efforts to secure user privacy, users are still able to capture and share screenshots without the sender's knowledge, undermining the effectiveness of these privacy measures. Snapchat's screenshot notification system was identified as a proactive measure that enhances user control and awareness. In contrast, TikTok's lack of proactive measures to prevent unauthorised screenshotting was highlighted as a significant shortcoming.

I have argued that implementing a consent-based mechanism would be a proactive step towards enhancing user privacy on social media. This feature would prompt users to request permission from the other party before capturing a screenshot, thereby fostering a culture of consent and mutual respect.

A legal analysis was conducted focusing on a judicial inquiry into whether screenshotting and sharing private messages could potentially lead to an infringement of privacy. Both subjective and objective assessments were considered based on an illustrative scenario. It was contended that the public status of both the sender and recipient, as well as the virality of the post and follower engagement are crucial factors in determining privacy violations. It was argued that the act of screenshotting and disseminating private messages can lead to significant privacy infringements. The analysis further revealed that the current legal framework is unclear on whether screenshotting and sharing private conversations may infringe upon the right to privacy.

Despite these insights, several shortcomings remain: the pervasive cultural norm where individuals feel it is acceptable to screenshot and publish private conversations online (often without consent), the inconsistency in privacy policies across different platforms and the lack of proactive measures to prevent unauthorised screenshotting are significant challenges and the current legal framework, as it stands, does not provide sufficient protection for individuals' privacy rights.

Looking to the future, it is imperative for the judiciary to provide clear guidance on balancing privacy rights with pervasive use of social media. Legal reform is necessary to implement more stringent measures to prevent unauthorised screenshotting of private conversations and to provide clear legal consequences for privacy violations. Social media platforms must adopt technological safeguards that require explicit consent before capturing a screenshot, empowering users to control the dissemination of their private conversations. Ongoing dialogue between lawmakers, the judiciary, and technology experts is essential to ensure that privacy laws remain relevant and effective. By fostering a culture of consent and mutual respect, social media platforms can create a safer and more trustworthy environment for digital communication.

In conclusion, the issue of screenshotting private messages presents a significant challenge to the right to privacy in the digital age. The judiciary has yet to fully address

this issue and there is a pressing need for legal clarity to protect user’s privacy rights. By implementing more stringent measures, providing clear legal consequences, and ensuring that the legal framework can adapt to future technological advancements, the courts can better protect individuals' privacy in the digital age. Without the implementation of these necessary changes, individuals remain vulnerable to privacy infringements through the act of screenshotting.

BIBLIOGRAPHY

BOOKS

De Vos P et al *South African Constitutional Law in Context* (2022: Oxford University Press).

Loubser M et al *The Law of Delict in South Africa* (2018: Oxford University Press).

Neethling J, Potgieter J & Roos A *Neethling on Personality Rights* (2019: Lexis Nexis).

Papadopoulos S & Snail S *Cyberlaw@SA III: The Law of the Internet in South Africa* (2012: Van Schaik Publishers).

Papadopoulos S & Snail ka Mtuze S *Cyberlaw@SA the law of the internet in South Africa* (2022: Van Schaik Publishers).

JOURNAL ARTICLES

Corry F 'Screenshot, save, share shame: Making sense of new media through screenshots and public shame' (2021) 26 (4) *First Monday* at 1 – 11.

DeVries W 'Protecting Privacy in the Digital Age' (2003) 18 (283) *Berkeley Technology Law Journal* 283 - 311.

Garg R 'Privacy v Social Media' (2019) 12 (2456-9704) *Supermo Amicus* at 1 - 5.

Grimmelmann J 'Saving Facebook' (2009) 94 (5) *Iowa Law Review* 1137 - 1206.

Ingber A 'Protecting Privacy Communications through Law and Policy: The Case of the Screenshot Feature' (2024) 29 *Communications Law and Policy* 1 - 23.

Mashinini N 'Unauthorised use of images in memes: Revisiting the privacy and identity debate' (2022) 33 (4) *Stellenbosch Law Review* 657 - 670.

Obar J & Oeldorf-Hirsch A 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2018) 23 (1) *Information, Communication & Society* at 128 - 147.

Patience B & Obetayo B ‘Evaluating the privacy issues, potential risks and security measures associated with using social media platforms’ (2024) 3 (2) *International Journal of African Research and Sustainability Studies* at 105 - 119.

Piwek L & Joinson A ‘“What do they snapchat about?” Patterns of use in time-limited instant messaging service’ (2016) *Computers in Human Behavior* 358 - 366.

Roos A ‘Privacy in the Facebook era: A South African legal perspective’ (2012) 129 (2) *South African Law Journal* 375 - 401.

Senthil Kumar N, Saravanakumar K & Deepa K ‘On Privacy and Security in Social Media – A Comprehensive Study’ (2016) 78 *Procedia Computer Science* 114 - 119.

Velton J, Arif R & Moehring D ‘Managing Disclosure through Social Media: How Snapchat is Shaking Boundaries of Privacy Perceptions’ (2017) 6 (1) *The Journal of Social Media in Society* 220 - 245.

THESES AND DISSERTATIONS

Neethling J ‘*Die Reg op Privaatheid’* (LLD thesis, University of South Africa, 1976).

SOUTH AFRICAN CASES

Bernstein and Others v Bester NO and Others 1996 (4) BCLR 449 (CC)

Botha v Smuts and another (Campaign for Free Expression NPC as *amicus curiae*) 2024 (12) BCLR 1477 (CC)

H v W 2013 (5) BCLR 554 (GSJ)

Heroldt v Wills (2014) JOL 31479 (GSJ)

Khumalo & others v Holomisa 2002 (5) SA 401 (CC)

Mistry v Interim National Medical and Dental Council of South Africa and Others 1997 (7) BCLR 933 (D)

National Media Ltd and Another v Jooste 1996 (2) All SA 510 (A)

The Investigating Directorate: Serious Economic Offences and others v Hyundai Motor Distributors (Pty) Ltd and others: In re: *Hyundai Motors Distributors (Pty) Ltd and Others v Smit NO and Others* (2000) JOL 7338 (CC)

Tshabalala-Msimang and Medi-Clinic Ltd v Makhanya 2008 (3) BCLR 338 (W)

INTERNATIONAL CASES

Largent v Reed and Pena (Case No 2009-1823) 39th Judicial District of Pennsylvania, Franklin County (7 November 2011)

Moroccanoil, Inc. v. Marc Anthony Cosmetics, Inc., 57 F. Supp. 3d 1203 (C.D. Cal. 2014)

TikTok, Inc. v. Garland, 604 U.S. (2025)

United States v. Vayner, 769 F.3d 125 (2d Cir. 2014)

Voxson Pty Ltd v Telstra Corporation Limited (No 10) (2018) 134 IPR 99; [2018] FCA 376

LEGISLATION

Constitution of the Republic of South Africa, Act 200 of 1993

Constitution of the Republic of South African, 1996

Electronic Communications and Transactions Act 25 of 2002

Protection of Personal Information Act 4 of 2013

INTERNET SOURCES

Android Police 'WhatsApp now blocks you from taking screenshots of profile pictures' available at *https://www.androidpolice.com/whatsapp-blocks-you-from-taking-screenshots-profile-pictures/,* accessed on 11 December 2024.

BBC 'Instagram defends new teen safety features after criticism' available at *https://www.bbc.com/news/articles/cdd4vn6p601o,* accessed on 11 December 2024.

Carter- Ruck 'Defamation and Privacy Law in South Africa' available at *https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-south-africa/*, accessed on 18 January 2025.

Context ‘US TikTok ban: Which other countries have banned the app?’ available at *https://www.context.news/big-tech/us-tiktok-ban-which-other-countries-have-banned-the-app,* accessed on 4 January 2025.

Dazed ‘Receipts culture has gone too far’ available at *https://www.dazeddigital.com/science-tech/article/56366/1/receipts-culture-has-gone-too-far,* accessed on 20 January 2025.

Digital School of Marketing ‘How TikTok has taken over social media’ available at *https://digitalschoolofmarketing.co.za/social-media-marketing-blog/how-tiktok-has-taken-over-social-media-marketing/,* accessed on 3 January 2025.

Facebook Help Centre ‘Reporting a Privacy Violation’ available at *https://www.facebook.com/help/1561472897490627/?helpref=hc_fnav*, accessed on 12 December 2024.

Firewall Times ‘Facebook Data Breaches: Full Timeline Through 2023’ available at *https://firewalltimes.com/facebook-data-breach-timeline/*, accessed on 11 December 2024.

First Monday ‘Report and repeat: Investigating Facebook’s hate speech removal process’ available at *https://firstmonday.org/ojs/index.php/fm/article/download/10288/8327,* accessed on 28 January 2025.

Forbes ‘Can screenshots of text messages be used as digital evidence in court?’ available at: *https://www.forbes.com/sites/larsdaniel/2024/11/13/think-that-screenshot-is-proof-heres-why-it-might-not-hold-up-in-court/,* accessed on 10 December 2024.

Front Row ‘The power of TikTok virality’ available at *https://www.frontrowgroup.com/insight/the-power-of-tiktok-virality/,* accessed on 4 January 2025.

GB Times ‘Why do some Snapchat messages disappear?’ available at *https://gbtimes.com/why-do-some-snapchat-messages-disappear/,* accessed on 20 December 2024.

Information Regulator (South Africa) ‘Information Regulator warns against the processing of personal information of data subjects without their consent’ available at: *https://inforegulator.org.za/wp-content/uploads/2020/07/ms-20210713-ProcessingPersonalInfo.pdf,* accessed on 10 December 2024.

Instagram ‘Instagram Stories’ available at *https://about.instagram.com/features/stories#:~:text=at%20the%20bottom.-,Stories%20disappear%20from%20your%20profile%2C%20Feed%20and%20Direct%20inbox%20after,will%20appear%20as%20one%20clip,* accessed on 20 January 2025.

Instagram Help Centre ‘Threads Supplemental Privacy Policy’ available at *https://help.instagram.com/515230437301944*, accessed on 12 December 2024.

Instagram Help Centre ‘Report a post or profile on Instagram’ available at *https://help.instagram.com/192435014247952,* accessed on 12 December 2024.

Investopedia ‘Top 3 Companies Owned by Facebook (Meta)’ available at *https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp*, accessed on 10 December 2024.

Keyhole ‘Instagram Posts vs Instagram Stories: Is one better than the other?’ available at *https://keyhole.co/blog/instagram-posts-vs-instagram-stories/#:~:text=Instagram%20posts%20are%20evergreen.,pretty%20great%20Instagram%20post%20guide,* accessed on 20 January 2025.

Know Your Meme ‘Jonah Hill’s “Boundaries” Texts’ available at *https://knowyourmeme.com/memes/events/jonah-hills-boundaries-texts*, accessed on 10 December 2024.

Mac-History.Net ‘The History of the Apple Macintosh’ available at *https://www.mac-history.net/2021/02/10/history-apple-macintosh/*, accessed on 10 December 2024.

Meta ‘End-to-End Encryption on Messenger Explained’ available at *https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/#:~:text=End%2Dto%2Dend%20encryption%20helps,personal%20messages%20from%20other%20devices,* accessed on 11 December 2024.

Meta ‘Launching Default End-to-End Encryption on Messenger’ available at: *https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/,* accessed on 11 December 2024.

Meta ‘Our Approach to Safer Private Messaging’ available at *https://about.fb.com/news/2021/12/metas-approach-to-safer-private-messaging/*, accessed on 10 December 2024.

Meta Privacy Center ‘Content that others share or reshare about you’ available at *https://www.facebook.com/privacy/policy?subpage=3.subpage.2-ContentOthersShareOr,* accessed on 12 December 2024.

Newsweek ‘TikTok Ban 2025 Explained: What is actually happening?’ available at *https://www.newsweek.com/tiktok-ban-2025-supreme-court-2012881,* accessed on 4 January 2025.

Newsweek ‘What is Meta, Exactly? What Facebook’s rebrand means’ available at *https://www.newsweek.com/facebook-meta-rebrand-stock-prices-explained-1643779#:~:text=Not%20only%20does%20the%20company,more%20than%20just%20social%20media*, accessed on 10 December 2024.

Snapchat Inc ‘Community Guidelines’ available at *https://values.snap.com/privacy/transparency/community-guidelines,* accessed on 21 December 2024.

Snapchat Inc ‘Our Privacy Principles’ available at *https://values.snap.com/privacy/privacy-principles*, accessed on 20 December 2024.

Snapchat Inc ‘Privacy Policy’ available at *https://values.snap.com/privacy/privacy-policy,* accessed on 20 December 2024.

Snapchat Inc ‘Report a Safety Concern’ available at *https://values.snap.com/safety/safety-reporting*, accessed on 21 December 2024.

Snapchat Inc ‘Snapchat Safety Center’ available at *https://values.snap.com/safety/safety-center,* accessed on 21 December 2024.

Snapchat Inc ‘Snap Terms of Service’ available at *https://www.snap.com/terms?lang=en-US*, accessed on 21 December 2024.

TDFTips ‘Snapchat Screenshot Notifications: Navigating Privacy Concerns and Understanding Alert Features’ available at *https://tdftips.com/blog/snapchat-screenshot-notifications-privacy-and-screenshot-alerts/,* accessed on 20 December 2024.

TechTarget ‘end-to-end encryption (E2EE)’ available at *https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE*, accessed on 11 December 2024.

TechSmith ‘What is a Screenshot? The Basics’ available at *https://www.techsmith.com/blog/screenshot/#:~:text=A%20screenshot%2C%20sometimes%20referred%20to,a%20reference%20point%20later%20on*, accessed on 7 December 2024.

The Canandian Encyclopedia ‘Amanda Todd Case’ available at *https://www.thecanadianencyclopedia.ca/en/article/amanda-todd-case,* accessed on 20 January 2025.

The Guardian ‘Privacy no longer a social norm, says Facebook founder’ available at *https://www.theguardian.com/technology/2010/jan/11/facebook-privacy#:~:text=The%20rise%20of%20social%20networking,to%20Facebook%20founder%20Mark%20Zuckerber.,* accessed on 29 August 2024.

TikTok ‘Community Principles’ available at *https://www.tiktok.com/community-guidelines/en/community-principles,* accessed on 4 January 2025.

TikTok ‘Direct Messages’ available at *https://support.tiktok.com/en/using-tiktok/messaging-and-notifications/direct-message-settings,* accessed on 4 January 2024.

TikTok ‘Privacy Policy’ available at *https://www.tiktok.com/legal/page/row/privacy-policy/en*, accessed on 4 January 2025.

TikTok ‘Terms of Service’ available at *https://www.tiktok.com/legal/page/row/terms-of-service/en*, accessed on 3 January 2024.

Vice ‘How the Screenshot Became One of the Internet’s Most Powerful Tools’ available at: *https://www.vice.com/en/article/history-of-the-screenshot/#:~:text=The%20screenshot%20moved%20toward%20the,to%20send%20in%20their%20pictures,* accessed on 7 December 2024.

WhatsApp ‘Whatsapp Privacy Policy’ available at *https://www.whatsapp.com/legal/privacy-policy*, accessed on 12 December 2024.

WhatsApp Help Center ‘About reporting and blocking someone on WhatsApp’ available at *https://faq.whatsapp.com/414631957536067*, accessed on 12 December 2024.

Webwise ‘How to Take a Screenshot on your PC, phone or Tablet’ available at *https://www.webwise.ie/parents/take-screenshot/#:~:text=A%20screenshot%20or%20screen%20capture,using%20particular%20keyboard%2Fbutton%20shortcuts,* accessed on 7 December 2024.

World Jurisprudence ‘The Impact of Technology on Law: Transforming Legal Frameworks’ available at *https://worldjurisprudence.com/impact-of-technology-on-law/,* accessed on 22 August 2024.

World Economic Forum ‘The law can’t keep up with new tech. Here’s how to close the gap’ available at *https://www.weforum.org/stories/2018/06/law-too-slow-for-new-tech-how-keep-up/,* accessed on 22 August 2024.