RISS Journal
Randwick International of Social Sciences (RISS) Journal
Vol. 6, No. 2, April 2025 | Page: 60-78
ISSN Online: 2722-5674 - **ISSN Print**: 2722-5666
https://www.randwickresearch.com/index.php/rissj

Privacy, Promotion, and Platform Pitfalls: The Case of How Telegram's Marketing Approach Inadvertently Attracted Illicit Actors

DOI: *https://doi.org/10.47175/rissj.v6i2.1127*

| Rabel B. Catayoc |

Mindanao State University – Iligan Institute of Technology, Philippines

rabel.catayoc@g.msuiit.edu.ph

ABSTRACT

This paper examines how Telegram's market positioning, digital marketing strategies, and privacy-oriented business model have unintentionally created an attractive environment for criminal activities. Applying established marketing frameworks—including the Segmentation, Targeting, Positioning (STP) model and the marketing mix (4Ps: Product, Price, Place, Promotion)—alongside consumer behavior theories of trust and anonymity, this study analyzes Telegram's business practices. A comprehensive literature review on platform marketing, digital anonymity, cybersecurity, and darknet market theory provides contextual grounding within broader academic discussions. The analysis reveals that Telegram's broad market positioning, minimal governance, and emphasis on user privacy significantly facilitate criminal activities, such as identity theft, drug trafficking, and dissemination of illicit materials. The paper proposes strategic and policy recommendations emphasizing the importance of achieving a balance between safeguarding user privacy and mitigating the exploitation of digital platforms for illicit purposes. This research uniquely integrates traditional marketing frameworks and consumer behavior theories with cybersecurity literature to evaluate Telegram's unintended role in enabling online criminal ecosystems.

KEYWORDS

marketing approach; privacy; cybersecurity; promotion; platform pitfalls; consumer behavior; digital marketing; 4 P's; Segmentation Targeting Positioning (STP)

INTRODUCTION

Telegram is a cloud-based messaging platform launched in 2013 that has grown into a major player in the digital communications ecosystem. It reported around 900 million monthly users by 2024 (Owen-Jackson, 2024), making it one of the most widely used messaging apps globally. Telegram's brand has been built on a promise of privacy, security, and user freedom. It offers end-to-end encrypted chats, self-destructing messages, large group channels, and the ability to hide one's phone number – features that appeal to privacy-conscious consumers. Unlike many competitors, Telegram long maintained a hands-off approach to content moderation, only acting on user reports and legitimate takedown requests for illegal content (Owen-Jackson, 2024). This positioning as a secure, anonymous, and minimally moderated platform has attracted millions of legitimate users – including activists, journalists, and communities seeking uncensored communication. However, the same characteristics have unintentionally made Telegram attractive to illicit actors. In recent years, it has been described as the "messaging app of choice" for cybercriminals engaging in activities like malware distribution, identity theft, drug trade,

and illegal content sharing (Owen-Jackson, 2024). Law enforcement and researchers have raised concerns that Telegram's platform features and broad marketing stance – while intended to champion privacy and free speech – have created vulnerabilities that criminals exploit.

This case analysis examines Telegram's marketing-related vulnerabilities that draw illicit actors. I analyzed how Telegram's Segmentation, Targeting, and Positioning (STP) strategy and marketing mix (4Ps) have inadvertently fostered an environment for identity thieves, drug traffickers, and purveyors of illegal content. I also considered digital marketing dynamics and network effects, illustrating how criminals leverage Telegram's vast reach and ease of use to "market" illicit goods and services. Furthermore, I applied consumer behavior theories related to trust and anonymity to understand how both criminals and users behave within Telegram's ecosystem. A review of relevant academic literature on platform marketing, digital anonymity, darknet markets, and network governance is integrated to provide theoretical insight. Finally, I offer recommendations – spanning marketing strategy, platform governance, and policy measures – aimed at mitigating illicit activity on Telegram while preserving its core value of user privacy.

This article explores these two methodologies, highlighting their key characteristics, purposes, and educational benefits. By doing so, it aims to clarify the distinct roles they play in both academic and professional settings. Ultimately, this paper underscores the importance of understanding how these approaches complement each other in fostering critical thinking and problem-solving skills.

Problem Identification

Telegram's core value propositions and business choices have unintentionally created an appealing haven for illicit activities. Several marketing-related factors contribute to this problem:

Privacy-Focused Positioning and Brand Ethos

Telegram has deliberately positioned itself as a champion of user privacy and free expression. Founder Pavel Durov cultivated a reputation as a defender of free speech (e.g. refusing to shut down dissenting groups on his earlier platform VKontakte) (Admin, 2024). Telegram's branding emphasizes that user data is secure and that the company resists censorship. For years, Telegram claimed it had *never* disclosed user data to any government and only processed "legitimate" removal requests for illegal public content (Waldman, 2024). This staunch privacy stance attracted users seeking confidential communication – including those "operating outside the law," such as drug dealers and fraudsters (Admin, 2024b). In effect, the brand's promise of secure messaging was a double-edged sword: it built user trust in the platform's safety from surveillance, which for criminals meant confidence that they could operate with anonymity and minimal risk of interception (Flare, 2024). Telegram's hands-off moderation policy reinforced this perception. The platform openly stated in its FAQ that private chats were off-limits to moderators and that content removal relied primarily on user reports (Owen-Jackson, 2024b). By contrasting itself with competitors that "invest heavily in moderating content and cooperation with law enforcement" (Owen-Jackson, 2024), Telegram inadvertently signaled to illicit actors that it would be a relatively unguarded venue. Indeed, these features made Telegram "the messaging app of choice for cyber-crime and other illegal activity," from selling illegal goods to coordinating cyberattacks (Owen-Jackson, 2024).

Platform Features Enabling Anonymity and Secrecy (Product Factors)

Several of Telegram's product features serve as *affordances* for criminal misuse. Telegram allows users to create accounts using just a phone number – and even supports signing up with "anonymous numbers" purchased via blockchain marketplaces, meaning no personally identifiable information is attached to an account (Owen-Jackson, 2024). This lowers barriers for criminals to join without identity linkage. In chats, users can remain pseudonymous via usernames, and recent updates let users hide their actual phone numbers from others (Flare, 2024b). End-to-end encryption is available (in Secret Chats) for confidential messaging, and all chats are encrypted in transit. This encryption prevents intermediaries from monitoring communications, which criminals exploit to discuss plans or trade illegal data securely (Flare, 2024). Telegram's ability to send large files (up to 2GB) and media facilitates the exchange of illicit digital goods (e.g. pirated content, malware, or sexual abuse material) with ease. Additionally, Telegram supports self-destructing messages and bot accounts, which can be used to automate illicit transactions or erase traces of conversations. Perhaps most consequential are Telegram's channels and groups: a single user can broadcast to massive audiences (public channels can have unlimited subscribers and groups can hold thousands). Such scalability, combined with anonymity, means a criminal actor can reach tens of thousands of people with an illicit offer while revealing little about themselves. These product features collectively create an environment where criminals can communicate, advertise, and distribute contraband with minimal oversight.

Broad Market Appeal and Lack of Niche Targeting

From a segmentation and targeting perspective, Telegram has taken a broad-market approach – aiming to serve "everyone" from casual chatters to businesses, communities, activists, and beyond. Unlike platforms tailored for professional networking or children, Telegram's user base is heterogenous and global. This broad segmentation means that illicit actors can blend into Telegram's wide user population without standing out. The platform was not explicitly designed or marketed for criminals, but its open ethos ("a tool for all who value privacy") does not exclude them. Telegram's positioning as an alternative to mainstream messengers (like WhatsApp or Facebook Messenger) especially appealed to segments distrustful of authorities or big tech – a category that, besides activists and privacy enthusiasts, *also includes cybercriminals and extremists*. In marketing terms, Telegram's value proposition (secure**,** unmonitored communication) attracted multiple segments with that need, including those with malicious intent. The lack of strict onboarding or community gatekeeping (anyone can join via a download and a phone number) means Telegram effectively ended up "targeting" the entire spectrum of users, *including criminals by default*. This broad positioning has made it susceptible to becoming a "catch-all" platform where illicit sub-communities form under the radar.

Business Model and Pricing Strategy

Telegram's business model has been atypical – it forwent advertising for many years and only recently introduced optional premium subscriptions. The service remains free to use, with no direct cost to users. The "free" price and easy availability reduce any friction for bad actors who often operate many accounts or disposable accounts. Unlike a paid platform or one with rigorous identity checks, Telegram does not financially deter banned users from rejoining under new identities. Moreover, because Telegram does not monetize via targeted ads, it has less incentive to profile user behavior or content (which in an advertising model would at least impose some monitoring). Telegram's minimal revenue

model also meant leaner content oversight resources – there were no large moderator teams or AI filters aggressively scanning messages (since that would contradict their privacy stance and incur costs). In terms of "Place" (distribution), Telegram is readily accessible via mobile apps and web, and its cloud-based architecture ensures content shared can be accessed by users globally without localized servers. This global reach and persistence of content (channels act as long-lived repositories) help illicit material circulate widely. Furthermore, Telegram's promotion and PR have consistently highlighted its security advantages and disdain for censorship. The app's leaders frequently publicized that they stood up to government pressures (for example, resisting backdoor demands) – a promotional message that resonates with criminals seeking a haven. For instance, when Russia attempted to ban Telegram in 2018 for not sharing encryption keys, the incident arguably *enhanced* Telegram's appeal among those wanting to evade surveillance. In summary, Telegram's product, price, place, and promotion – free secure messaging for a global audience with little moderation – inadvertently provide an ideal infrastructure for illegal transactions to thrive.

Network Effects and Unmoderated Growth

As Telegram's user base expanded rapidly (with especially large influxes during periods when competing apps faced outages or policy controversies), it reached a critical mass that attracted illicit networks. The network effect principle in marketing suggests that a product's value increases as more people use it. In Telegram's case, its large user population became extremely valuable to criminals as a ready market and a recruitment pool. Organized crime groups have capitalized on Telegram as a "communication fabric" connecting criminals and service providers across borders (Uren, 2024). For example, a United Nations report found that transnational syndicates congregate on Telegram to trade malware, stolen data, money laundering services, and even coordinate violent crime, effectively building underground marketplaces within the platform (Uren, 2024b). The presence of established illicit channels in turn drew in more criminals (a classic network feedback loop) – if buyers know that Telegram hosts many sellers of drugs or fake IDs, they join the app, which then encourages more sellers to set up shop there. This self-reinforcing growth was facilitated by Telegram's lack of early strict governance. Pavel Durov acknowledged that the platform's "*growing pains*" – a surge in users – "made it easier for criminals to abuse our platform." (Irwin, 2025) In essence, Telegram's rapid, uncurated expansion outpaced its control mechanisms. With millions of users and an ideology of minimal intervention, Telegram struggled to police malicious activity, allowing illicit actors to embed themselves and leverage the network's scale for illicit marketing. By the time Telegram crossed hundreds of millions of users, it had inadvertently become host to a myriad of criminal communities: from carding rings selling stolen credit cards, to cartel operatives running drug delivery networks, to groups sharing illegal pornography.

Concrete examples illustrate the scope of the issue. Cybercriminal bazaars on Telegram openly trade leaked personal data and hacking tools. A public channel named "Combolist" amassed over 45,000 subscribers who traded stolen login credentials; only after a media report did Telegram shut it down (Flare, 2024). Researchers have observed Telegram channels selling malware, ransomware kits, and "malware-as-a-service" bots, effectively mirroring dark web markets (Irwin, 2025). Identity theft and financial fraud are rampant: entire marketplaces offer "fullz" (packages of stolen IDs, Social Security numbers, bank logins) for prices as low as $30–40 (Pymnts, 2024). One 2024 academic study described Telegram data markets where vendors auction huge dumps of personal data to buyers in

completely unregulated exchanges (*Stolen Data Markets on Telegram: A Crime Script Analysis and Situational Crime Prevention Measures - Security Insight*, 2024). Drug trafficking has likewise proliferated. Telegram is used in many countries as a storefront for narcotics, from recreational drugs to prescription pills. For instance, an analysis in the Netherlands counted over 5,600 drug-related posts in just two Telegram groups over ~7 months, with the vast majority being dealers' advertisements (only 6% were buyer queries) – indicating Telegram functions largely as a "sellers' market" for drugs (Blankers et al., 2021). Even child exploitation rings and extremists have reportedly used Telegram to share illegal content due to its encryption and lenient oversight (one factor behind legal action against Telegram's CEO in 2024). All these problems stem from the same root cause: Telegram's marketing promise of privacy and freedom, combined with its feature set and scale, created a fertile ground for illicit actors.

LITERATURE REVIEW

The observed phenomenon of Telegram attracting illicit actors can be contextualized with insights from academic literature on platform marketing, cybersecurity, and digital crime:

Platform Marketing Strategy and Unintended Audiences

Marketing scholarship acknowledges that the way a platform positions and governs itself can result in *unintended market segments* taking hold. Telegram's case exemplifies what might be called "brand hijacking" by unintended users – a concept akin to when a brand becomes popular with a group it didn't originally intend (sometimes seen benignly in fashion or tech, but here with criminal actors). Theoretically, this is an outcome of a value proposition that is too generic or universal. By offering the value of privacy to all users, Telegram created what economists might label a *public good* environment that bad actors can free ride on. Literature on two-sided markets and platforms (e.g., Parker & Van Alstyne, 2016) discusses how platforms must manage negative network externalities, where an increase in one type of user (illicit actors) can hurt the experience for others (law-abiding users, or the platform's reputation). In Telegram's history, the growth of criminal uses became a negative externality challenging its image and prompting belated policy responses (Irwin, 2025). Academic frameworks like Routine Activity Theory from criminology also align with Telegram's situation: Cohen and Felson's theory posits that crime occurs when a motivated offender, a suitable target, and lack of a capable guardian converge. Telegram's platform effectively removed "capable guardians" by having minimal moderation (no active guardian oversight in groups) and at the same time aggregated plentiful targets (users who can be defrauded or illicit products to be sold) and motivated offenders (criminals drawn in) (Hasan & Bangladesh University of Professionals, 2023; Gan et al., 2024). The platform's broad marketing and lack of guardianship thus inadvertently fulfilled the conditions for rampant online crime.

Cybersecurity and Digital Anonymity

Academic discussions on encryption and anonymity often highlight a duality: tools that protect legitimate users' privacy can equally shield criminals. An OCCRP report memorably stated, "Encryption: a godsend to all who seek privacy, even criminals." (*Encryption: A Godsend to All Who Seek Privacy, Even Criminals*, 2016). This underscores a widely recognized *unintended consequence of strong privacy technologies*: they empower those who wish to evade law enforcement. Telegram's strict privacy policies facilitated cybercrimes, noting that its refusal to share data or monitor content created jurisdictional and enforcement challenges (legal "safe havens" online). The "cybercriminal

migration" to Telegram observed around 2018–2021 has been documented in cybersecurity studies. For example, a Financial Times investigation in 2021 found a 100% increase in Telegram use by cybercriminals, as they moved off dark web forums to the platform (Flare, 2024). Scholars attribute this migration to convenience and perceived safety: unlike darknet sites that could be shut down or require technical expertise, Telegram provided plug-and-play anonymity (Flare, 2024). The concept of "trustless trust" is relevant here – criminals operate in a zero-trust environment (they don't trust each other or authorities), so they place trust in the technology (encryption, platform reliability) as a substitute. Telegram's design gave them that trust in technology, as evidenced by their extensive adoption for coordinating operations (Owen-Jackson, 2024).

From a literature standpoint, Telegram became an example in debates on encryption policy: law enforcement agencies have cited Telegram as a reason they need ways to pierce encrypted communications (the so-called "going dark" problem). Meanwhile, privacy advocates point out that millions of legitimate users benefit from these features, raising the classic security vs. privacy trade-off discussion (Solove, 2011; Schneier, 2015). Telegram's situation during 2013–2023 often comes up as a case where *absolute privacy* led to a proliferation of abuse, highlighting the need for nuanced solutions that academics in security and ethics continue to explore.

Darknet Marketplaces and Digital Crime Migration

Criminology and sociology research on illicit online markets provides insight into why Telegram became attractive compared to traditional darknet sites. Studies of darknet drug markets (Barratt & Aldridge, 2017) show that when enforcement or trust issues disrupt those markets, sellers and buyers seek alternative platforms. Telegram has been described in industry and academic commentary as a "new dark web frontier" (Flare, 2024) because it replicated many of the darknet's advantages (anonymity, global reach) on a mainstream interface. A 2023 report by Flare explicitly asked if Telegram will *"make the dark web redundant"*, concluding that many threat actors prefer Telegram due to easier anonymity and operations (Flare, 2024). Academic literature on social organization of cybercrime notes that cybercriminals gravitate to platforms where they can efficiently find resources and collaborators. Telegram's group chats essentially function as criminal networking hubs, which aligns with the finding by the UN Office on Drugs and Crime that Telegram became a key venue for transnational crime syndicates to "congregate, connect, and conduct business online" (Uren, 2024). This reflects the theory of networked criminal structures – technology enabling loose networks of criminals to form ad-hoc groups for specific crimes. The *organizational efficiency* of Telegram (large group coordination without needing a centralized forum site) is a theme in recent crime research. For instance, T. Garkava et al. (2024) in *Trends in Organized Crime* detail how stolen data markets on Telegram operate with thousands of members, internal rules, and advertising tactics (*Stolen Data Markets on Telegram: A Crime Script Analysis and Situational Crime Prevention Measures - Security Insight*, 2024). Their crime script analysis indicates these markets are robust because Telegram doesn't impose the disruption that darknet sites face (like server seizures or exit scams). This supports the academic view of crime as adaptive: criminals will exploit any new communication channel that lowers risk and cost. Telegram's case is frequently compared to past examples like BlackBerry Messenger being used by UK rioters in 2011 or WhatsApp encryption enabling certain criminal communications – in each, the common factor is strong privacy in a widely available tool leads to illicit adoption. Thus, Telegram's issues exemplify broader criminological patterns observed when technology leaps ahead of governance.

Network Effects and Platform Governance

In the realm of information systems and governance studies, Telegram's trajectory highlights issues of scaling without sufficient governance mechanisms. Researchers like Gillespie (2018) have discussed how platforms often start with idealistic free-speech principles but face pressure as they scale to moderate harmful content – a tension clearly seen with Telegram. The platform's growth to hundreds of millions created network effects that outpaced its moderation resources. Literature on platform governance suggests that as user-generated content networks grow, they can reach a tipping point where harmful content explodes if not checked. Telegram arguably hit this tipping point: its "growing user base made it easier for criminals to abuse" it, as Durov himself admitted (Irwin, 2025). Network effect theory (Katz & Shapiro, 1985) also introduces the idea of negative network effects where above a certain size, additional users can decrease overall value due to congestion or bad actors. For Telegram, the presence of bad actors began to threaten the platform's standing with app stores and governments (diminishing its value for lawful users who might fear it as a haven for crime). Academic discussions on social media governance (e.g., Dolata, 2019) emphasize that companies must implement rules and enforcement proportionate to their network size and impact. Telegram's very limited content policy was arguably a misalignment once the network grew huge. Another concept is external governance pressure–indeed, Telegram's eventual policy shift in 2024 (agreeing to share some data and moderate more) was precipitated by external legal pressure (the arrest of its CEO and potential bans) rather than proactive internal policy (Owen-Jackson, 2024). This aligns with regulatory theories that platforms often self-regulate only when faced with the threat of formal regulation or loss of market access. Network effect also played a role in criminals' reaction: when Telegram tightened policies, many cybercriminal groups announced migration to smaller platforms like Signal, showing that they will follow the path of least resistance in the ecosystem (Owen-Jackson, 2024). This dynamic is noted in literature as well-he displacement of crime from one platform to another ("whack-a-mole" effect) if underlying demand isn't addressed. Finally, from a marketing perspective, the brand governance aspect in literature suggests Telegram now must re-position slightly to shed its reputation as a "shady" platform (Roth, 2024). Maintaining user trust among legitimate users while cutting off illegitimate ones is a branding challenge noted in case studies of other platforms (like how Craigslist had to ban certain sections to avoid being known chiefly for illicit services).

In sum, theoretical and empirical literature from multiple fields corroborates and elucidates Telegram's situation. Platform marketing strategy theory explains how broad positioning and lack of segmentation opened the door to unintended users. Cybersecurity and anonymity research highlight the trade-offs and criminal adaptations to secure platforms. Studies of darknet markets and organized cybercrime provide evidence that criminals intentionally migrated to Telegram for its practical advantages, effectively making it a mainstream alternative to dark web forums. And network governance literature frames Telegram's struggle as part of the growing pains of platforms that champion openness and then encounter the realities of misuse at scale. These scholarly perspectives reinforce the insight that Telegram's vulnerabilities are not isolated – they reflect systemic challenges at the intersection of marketing, technology, and social control in the digital age.

RESEARCH METHODS

This study applies a qualitative case analysis using established marketing frameworks, notably the Segmentation, Targeting, and Positioning (STP) model, to evaluate Telegram's unintended attraction of illicit actors.

Table 1. the Segmentation, Targeting, and Positioning (STP) model

Segmentation Analysis	Telegram pursued a mass-market segmentation strategy based on the core user need for secure and versatile messaging. Its broad demographic and psychographic segmentation approach encompassed diverse user groups, including teenagers, political dissidents, and business users, all unified by the common value placed on privacy and secure communication. The absence of stringent niche segmentation allowed the inadvertent inclusion of illicit actors who share overlapping privacy needs with legitimate users. The lack of explicit segmentation strategies to exclude high-risk users opened Telegram to unintended criminal infiltration.
Targeting Analysis	Telegram's targeting strategy was inclusive, aiming at maximizing global user adoption without meaningful barriers to entry or differentiated marketing to dissuade illicit groups. Its targeting of privacy-conscious users implicitly attracted cybercriminals and other illicit actors who equally prioritize anonymity. This broad targeting strategy treated all users equally concerning encryption and minimal oversight, unintentionally creating an environment attractive to threat actors. From the perspective of criminals, Telegram's platform actively welcomed them through its emphasis on user autonomy and minimal policing of private behavior.
Positioning Analysis	Telegram distinctively positioned itself on privacy, security, and freedom from control, emphasizing its superiority in data security compared to competitors like WhatsApp and Facebook. This positioning resonated strongly with users distrustful of surveillance, notably criminals alongside political dissidents. Telegram's promotional emphasis on what it doesn't do—such as data sharing and content monitoring—unintentionally advertised it as a secure platform for illicit activities. By positioning itself as a communication platform where user activities remained largely unchecked and untraceable, Telegram inadvertently attracted users explicitly requiring secrecy for criminal endeavors. Through applying this structured STP analysis, the study reveals how Telegram's marketing approach unintentionally aligned with criminal actors' needs, highlighting significant vulnerabilities within its strategic marketing practices.

RESULTS AND DISCUSSION

Segmentation, Targeting, Positioning (STP) Analysis

Telegram's susceptibility to criminal abuse can be examined through the lens of STP to understand how its broad positioning enabled unintended user segments.

Segmentation

Rather than focusing on a specific niche, Telegram pursued a mass-market segmentation strategy centered on a core user need – secure, versatile messaging. Its user base spans various demographics and psychographics (from teenagers to political dissidents to business users), unified by the appeal of control over privacy. This broad segmentation meant that Telegram did not exclude or heavily restrict any group. Notably, individuals engaged in illicit activities share overlapping needs with legitimate privacy-seekers – both value anonymity, encrypted communication, and freedom from oversight. Thus, the

segment of "illicit actors" naturally found their way into Telegram's user population. In marketing terms, they represent an unintended sub-segment attracted by the same platform attributes marketed to mainstream segments. Because Telegram segmented its market primarily by user *needs* (privacy, freedom) rather than by user *identity or purpose*, it inevitably drew in users who have nefarious needs for privacy. The lack of explicit segmentation to keep risky users out (unlike, say, a workplace messaging app that segments only professional teams) left Telegram open to criminal infiltration.

Targeting

Telegram's targeting strategy was essentially broad and inclusive – aiming to maximize user adoption globally. The platform did not implement meaningful barriers to entry or differentiated marketing campaigns that might dissuade unwanted groups. In fact, Telegram's early adopter targeting included tech-savvy users, activists, and those fleeing other platforms over privacy concerns. This target audience – "privacy-conscious communicators" – implicitly included threat actors. Cybercriminals are among the most privacy-conscious users (for self-preservation), so Telegram's marketing appealed to them by offering "secure messaging that *even law enforcement can't access*." Telegram's **o**ne-size-fits-all targeting treated all users equally in terms of product features and policies. For example, *every* user, whether a student or a cybercriminal, gets the same encryption options and the same near-zero oversight in private chats. By not explicitly excluding or limiting high-risk user groups, Telegram effectively *targeted the entire market of internet users*. This inclusive targeting helped Telegram grow, but it also meant criminal elements were courted by the same campaign. From the criminals' perspective, Telegram's brand actively *welcomed* them by emphasizing user autonomy and refusing to "police" private behavior (Owen-Jackson, 2024). Thus, Telegram's targeting strategy – or lack of selective targeting – created a haven segment within its user base, comprised of identity thieves, drug dealers, terrorist propagandists, and others who realized they were as welcome as any other user.

Positioning

Telegram has positioned itself distinctively against rival services on the attributes of privacy, security, and freedom from control. Its brand messaging stresses that it is "safer" and more private than WhatsApp (due to not sharing data with a parent company) and freer than Facebook (due to rejecting censorship and ads). The positioning can be summarized as: Telegram = Secure, independent communication for everyone. This positioning strongly appeals to users who distrust surveillance – a trait common to political dissidents *and* criminals alike. By emphasizing *what it doesn't do* (no data sharing, no spying on chats) in its positioning, Telegram inadvertently made itself attractive to those who explicitly *require secrecy*. In effect, Telegram's brand positioned it as the platform where you won't get caught. For example, an Australian harm-reduction group noted that *"Telegram's promise of secure messaging undoubtedly made it attractive to those operating outside the law"* (Admin, 2024b). The platform also positioned itself as an uncensored, global communication tool, implicitly tolerating edgy or controversial content if it stayed out of public view. This "harbinger of freedom" image (as some academics dubbed Telegram) signaled a lax stance on content policing, further cementing its appeal among hate groups and traffickers who had been deplatformed elsewhere. In summary, Telegram's positioning in the market – while not intended to condone illegal conduct – mapped perfectly to the needs of illicit actors. The very differentiators that Telegram used to carve out a market niche (strong encryption, refusal to bow to government pressure,

user-controlled groups) translated into competitive advantages for criminals compared to other platforms. In STP terms, Telegram positioned on *privacy and liberty* and thus attracted a segment of "customers" (criminals) that value those attributes to carry out illegal enterprises.

4Ps Marketing Mix Analysis (Product, Price, Place, Promotion)

Each element of Telegram's marketing mix has facets that inadvertently facilitate illicit transactions and communities:

Product

Telegram's product features are at the heart of its appeal – and its misuse. Key product attributes include: robust encryption, which protects message contents from interception; secret chats with self-destruct timers, which leave no trace of sensitive exchanges; large group chats and broadcast channels, which enable wide dissemination of information (or contraband) efficiently; user aliases (usernames) that allow interaction without revealing one's identity; the ability to share files up to 2GB, which supports trading of things like pirated movies, databases of stolen data, or software tools; and an open API/bot platform that lets users create bots for tasks like automated posting or even illicit service delivery. From a criminal's perspective, these features constitute an ideal "toolkit" for running illegal operations. For example, drug dealers have leveraged Telegram channels to post menus of products and use self-deleting messages to send delivery instructions to buyers, thereby using product features to execute an entire supply chain covertly. Likewise, hackers selling stolen credit card dumps utilize Telegram's file-sharing to distribute data and its anonymity to negotiate sales without exposing their identities (*Stolen Data Markets on Telegram: A Crime Script Analysis and Situational Crime Prevention Measures - Security Insight*, 2024). In marketing terms, the core product (secure messaging) and augmented product (features like bots, channels) provide *utility that aligns with illicit use-cases*. Telegram's decision to prioritize high security in its product design (to differentiate from competitors) inadvertently built a platform that mirrors the capabilities of darknet forums but with a superior user interface. Unlike on dark web markets where criminals must handle encryption (e.g., PGP for messages) and site uptime themselves, Telegram's product handles encryption automatically and offers a stable infrastructure (Flare, 2024). The convenience and reliability of the product thus make criminal operations "easier, faster and safer," to borrow phrasing from a social science study on drug dealing via Telegram.

Price

Telegram is free of charge, which significantly lowers the barrier for illicit actors to join and operate multiple accounts or channels. There is no financial cost to scale up illicit activities on the app – a drug trafficker can create dozens of group chats for different cities without any fees, and a fraud ring can register new accounts if old ones get banned, incurring only the negligible cost of acquiring new SIM cards or using the anonymous number feature. The freemium pricing (with most features available free and an optional Premium tier) means that core security features are not behind a paywall. This universality ensures criminals have equal access to all protective features (e.g. none of the privacy tools are exclusively for paying users – a deliberate marketing choice by Telegram to uphold privacy for all). Additionally, Telegram does not monetize user data, so criminals face no risk of their activity being sold or flagged to third parties by any analytic processes, unlike on some ad-supported platforms where unusual behavior might be detected through data mining. In essence, Telegram's free pricing and non-reliance on surveillance for profit give

criminals a *"free ride."* The platform's business model (formerly funded by the founders and investors, now supplemented by user premiums) placed user growth and engagement as the top priority, implicitly tolerating that some of that engagement was illicit since it didn't directly hurt revenue. From a marketing mix perspective, Telegram treated privacy as a built-in value at no extra cost, which meant even the lowest-effort criminal could utilize high-grade encryption and global messaging gratis. This stands in contrast to some underground communication tools that charged for usage or required technical setup (like paid VPNs or bulletproof hosting services). Thus, Telegram's price point and business model inadvertently subsidized criminal operations on the platform.

Place (Distribution and Accessibility)

Telegram's distribution strategy focuses on being accessible anytime, anywhere. The app is available across mobile (Android, iOS) and desktop, and it syncs seamlessly across devices (Flare, 2024). This ubiquity is a boon for illicit actors: they can manage their "business" on Telegram from multiple devices, stay in touch with international partners, and quickly move communications from one device to another if needed. Telegram's messages are cloud-stored (except Secret Chats), meaning even if a device is seized or destroyed, the chat history in groups/channels remains available from another login – a resilience that legitimate users appreciate, but so do criminals who want continuity of their marketplace. Moreover, Telegram is distributed through mainstream app stores and is legal in most jurisdictions, making it a far more convenient "place" to meet than hidden darknet sites. Buyers and sellers of illegal goods do not need special browsers or networks; they only need the Telegram app, which is not suspicious by itself on one's phone. This *mainstream availability* has made Telegram a new arena for illicit commerce, effectively bringing black markets into a widely used social space (Flare, 2024). In marketing terms, Telegram extended the "place" where transactions happen from obscure corners of the internet to a user-friendly messenger. Additionally, Telegram's in-app search and invite links function as distribution channels for content. Until recently, users could find some public channels by searching keywords (Telegram has since limited searching of obvious illicit terms after abuse was noted (Reporter, 2024)). Before crackdowns, this meant a curious user could type "buy drugs" or "credit cards" in Telegram's search and potentially discover a illicit channel – effectively an *internal marketing channel* for criminals to acquire customers. Even now, invite links shared on forums or social media act as referral links guiding new "customers" into Telegram groups where illegal services are offered. The ease of joining via a simple link (no vetting required) exemplifies how Telegram's frictionless distribution mechanisms facilitate the growth of illicit groups. The concept of "place" in the 4Ps thus encompasses not only Telegram's wide availability, but also the unrestricted reach content can achieve on the platform.

Promotion

Telegram's own promotional communications and community ethos have inadvertently promoted it as a haven for illicit activity. Officially, Telegram markets itself on features (speed, security) and has relied heavily on word-of-mouth and media coverage. The public discourse around Telegram often highlights its encryption and independence from government control, which serves as indirect promotion to criminals. For instance, every time Telegram touted that it doesn't cooperate with mass surveillance or that it withstood government bans, those news stories acted as advertising to threat actors that "Telegram is safe for secret dealings." In addition, Telegram's minimal enforcement of rules in the past functioned as a promotional signal – the fact that extremist groups, piracy channels, and

black markets persisted on Telegram became known in underground circles, effectively marketing Telegram as a "safe zone" compared to heavily moderated platforms. Cybercriminal forums and darknet sites began actively recommending Telegram as a communication method. In the cybercrime ecosystem, vendors would include their Telegram contact in advertisements for illicit products on other platforms, thus using Telegram as a promoted channel. This led to Telegram's logo and name becoming entwined with the marketing of illicit goods (e.g., a listing on a hacking forum might say "Contact us on Telegram at @BlackMarketBot for purchase"). Such cross-promotion greatly expanded Telegram's role in illicit trade. From Telegram's perspective, this was an unintended consequence – they did not endorse these uses, but by allowing a permissive environment, they effectively crowdsourced promotion among criminal users. Furthermore, Telegram's community culture – encouraging creation of public channels on any topic and emphasizing user privacy rights – promoted the idea that "anything goes" on Telegram as long as you stay in your channel. The lack of promotional messaging about safety or cooperation with authorities (until very recently) meant there was little deterrence communicated to bad actors. In summary, while Telegram's formal promotion was about privacy and fun stickers, the *brand image* that proliferated was that of a platform where one could engage in illicit behavior with impunity. This image, spread via media reports and criminal word-of-mouth, has been a powerful attractor for illicit actors.

Digital Marketing & Network Effects

Criminals have leveraged Telegram as a digital marketing platform in its own right, exploiting both network effects and the app's design for virality. Telegram's structure with channels (broadcast to many) and groups (many-to-many discussion) is analogous to social media feeds and forums, which allows criminals to treat illicit commerce like e-commerce. They apply digital marketing tactics: for example, a drug vendor might create a branded channel with a catalogue of products, complete with images and descriptions, essentially marketing illegal goods to an audience of subscribers. They may run limited-time offers or loyalty programs (some channels offer discounts to repeat buyers or referral bonuses for inviting new members – classic promotional tactics adapted to contraband). Network effects amplify their reach; as a channel's subscriber count grows, its perceived legitimacy and visibility grow, attracting more subscribers in a feedback loop. One academic study found Telegram illicit drug markets to be very seller-driven, where dealers continually post ads and updates to maintain interest (Blankers et al., 2021b). This constant posting is akin to content marketing to keep the "audience" engaged. Criminal groups also use viral growth hacks – sharing channel invite links widely, using niche hashtags or codewords to evade detection while still being discoverable by those in the know. Because Telegram communities can swell to tens of thousands of members quickly, an illicit service can achieve in weeks the kind of audience that on the darknet might take months or require reputation building on multiple forums.

The scale of Telegram's user network dramatically lowers customer acquisition costs for criminals. Instead of needing to find buyers one by one in obscure forums, a seller can join an existing large group (say, a 10,000-member "fraud bazaar" group) and instantly have a marketplace. In this sense, criminals piggyback on Telegram's network effect – the app's large active user base means at any given time, there are willing counterparts for illegal transactions online. Indeed, analysts note that with nearly a billion users, Telegram "*still has the massive audience that large-scale cybercriminal operations… need to expand their reach*" (Owen-Jackson, 2024). This reach is global. A fraudster in one country can easily find victims or buyers overseas through Telegram's international network,

effectively using the platform to bypass physical market constraints (an illustration of the long-tail markets enabled by digital platforms).

Telegram also exhibits a cross-network effect in that content can be forwarded and shared between groups/channels. An illicit post in one group can be forwarded by users into other groups, cascading the exposure – a dynamic criminals exploit to increase visibility of their offerings (like how viral marketing works for legitimate content). Additionally, criminals utilize Telegram's broadcast and bot features for marketing automation. For instance, a bot can send a welcome message and instructions to every new subscriber of a channel – akin to an automated email responder in digital marketing, but here used to onboard new illicit customers.

Another network dynamic is community trust building. Digital consumer behavior theory suggests that online communities rely on trust signals and peer feedback in the absence of formal regulation. On Telegram, despite anonymity, illicit actors create trust via reputation within groups (e.g., satisfied buyers vouching for a seller, or admins curating a list of "verified" vendors). This mimics the review systems of e-commerce. In fact, some Telegram channels function as illicit marketplace hubs with their own governance rules, moderators (often the criminals themselves) who remove scammers to keep the "customer base" loyal, and escrow bots for payments. These emergent behaviors show criminals applying digital marketing principles – customer relationship management, branding, and user experience – within Telegram's network. They treat their illegal enterprise like a startup, leveraging the platform's reach and social features.

In summary, Telegram's network effect – its large and growing user network – combined with digital marketing-friendly features (channels, sharable content, bots) have been weaponized by illicit actors to promote their activities. What was intended as a tool for large-scale communication and community-building is used for scaling black markets. The result is a network of illicit exchanges that grows almost organically within Telegram, difficult for authorities to track because it is fragmented across thousands of private groups yet highly efficient due to the underlying network connectivity.

Consumer Behavior (Trust and Anonymity) on Telegram's Ecosystem

The behaviors of both criminals (as "sellers") and their "customers" (or victims) on Telegram can be understood through consumer behavior theories, especially around trust, risk, and anonymity in digital contexts.

First, consider the criminal actors as consumers of Telegram's service. Their adoption of Telegram can be partly explained by perceived risk reduction and trust in the platform's promises. Perceived anonymity plays a crucial role: theories of online disinhibition suggest that when users feel anonymous and untraceable, they are more likely to engage in risky or norm-violating behavior. Telegram's design offers *dissociative anonymity* (one's actions are not easily linked to real identity), which lowers criminals' fear of getting caught and thereby emboldens them to carry out illicit acts. As one cybersecurity analysis noted, Telegram has "no traditional admins monitoring" chats and allows hiding phone numbers, which is highly attractive for anonymity (Flare, 2024). This anonymity gives criminals a sense of safety and even a form of *trust in the platform* – they trust Telegram to keep their secrets. Indeed, Telegram cultivated user trust by repeatedly assuring it would not spy on chats or give out data. This created a *paradoxical situation* in consumer behavior: a legitimate brand building trust by protecting privacy ends up earning criminals' trust for the same reason. In essence, criminals behave like regular consumers who are brand-loyal; they congregate on Telegram because they believe in its reliability and privacy ethos (some hacking groups even publicly lamented Telegram's recent policy changes as a "betrayal"

of that trust (Owen-Jackson, 2024)).

From the angle of users who buy or engage in illicit content, their behavior also hinges on trust and perceived security. Purchasing drugs or stolen data online is fraught with risk – of fraud, of law enforcement, of moral guilt. Telegram's platform mitigates some of these factors: the *informality and familiarity* of a chat app can lull users into seeing illicit transactions as casual social interactions rather than serious crimes. Consumer behavior research shows that environment and medium can normalize certain actions; on Telegram, buying a fake ID via a chat might *feel* less illicit than navigating a hidden Tor marketplace, because the latter's very context signals illegality and danger. Telegram, by contrast, looks and feels like any other social app where one chats with friends, which can normalize the act of transacting illegal goods from a psychological standpoint. The social proof of seeing thousands of other subscribers in a channel can also reduce a buyer's fear – "so many others are doing it, it must be working." This herd behavior is a known influence on consumer decision-making online, where popularity can be mistaken for legitimacy.

Another relevant consumer behavior concept is trusting signals in anonymous markets. Since Telegram lacks an official rating or escrow system, users have developed alternative trust mechanisms: reputation of pseudonyms, longevity of a channel, and external verification (some channels advertise that they have "approved vendor" status on well-known forums or have admin endorsements). These signals help overcome the inherent lack of trust in anonymous dealings – aligning with theories from darknet market studies, which find that vendors and buyers rely on community-based trust when institutional trust is absent (Holt et al., 2016). Ironically, Telegram's simplicity (one account = one persona) means a vendor's username can build brand-like recognition over time if they don't change it. Thus, criminals engage in relationship marketing unwittingly – fostering a base of repeat customers who trust them due to prior satisfactory deals or word-of-mouth in groups.

On the victim side (e.g., targets of scams or identity theft), criminals exploit the consumer trust in the Telegram brand to deceive. Phishing scams on Telegram often involve messaging users pretending to be official support or popular services (Irwin, 2025), banking on the trust users place in Telegram as a communication channel. Consumers who are less tech-savvy might assume that if a message comes through the trusted Telegram app, it's more legitimate than an email from a stranger.

The theme of "trust and anonymity" thus cuts both ways: Telegram's environment creates *trust for the wrong stakeholders* (criminals trusting the platform) and *insufficient safeguards for user trust* (users may misplace trust in contacts or content on Telegram). In consumer behavior theory, trust is crucial for transactions; Telegram provided the *platform trust* (privacy, security) that allowed illegal transactions to occur without participants fearing immediate consequences. Additionally, the anonymity and lack of accountability diminish social and legal deterrents that normally curb deviant behavior. Individuals who might refrain from crime in a face-to-face setting (due to reputation risks or direct law enforcement presence) may feel disinhibited and less ethically constrained on Telegram, viewing their actions as just lines of text in an impersonal app. This aligns with the concept of the online disinhibition effect, where anonymity and invisibility can reduce adherence to social norms.

In summary, consumer behavior on Telegram's illicit side is characterized by *high trust in platform privacy, creative establishment of peer trust, normalized risk-taking due to anonymity,* and *social proof dynamics*. These factors enable criminals and their customers to engage in illegal exchanges in a manner that feels "safe" and routine, perpetuating the use of Telegram for illicit purposes.

Discussion

The findings of this study highlight the unintended consequences of Telegram's broad and inclusive market strategy, underscoring how its segmentation, targeting, and positioning inadvertently facilitated criminal activities. Telegram's approach to segmentation, focused on user needs rather than specific user identities or intentions, attracted a diverse user base unified primarily by a demand for secure, private communication. This broad segmentation approach inadvertently opened avenues for criminal groups seeking similar privacy protections. The literature supports this outcome, indicating that when segmentation focuses broadly on universal needs such as privacy, platforms risk inadvertently welcoming unintended and potentially harmful user segments (Blankers et al., 2021; Holt et al., 2016).

Telegram's targeting approach further compounded this issue. Its global, inclusive targeting strategy aimed at maximum user acquisition without differentiated messaging or entry barriers inherently lacked measures to deter or dissuade illicit actors. This aligns with theoretical frameworks of market targeting which suggest that an undifferentiated targeting approach might unintentionally attract malicious or high-risk segments that share fundamental platform features valued by legitimate users (Owen-Jackson, 2024). The implicit message communicated through Telegram's marketing—that all user behaviors are equally private and protected—became a significant draw for threat actors seeking anonymity and security from law enforcement scrutiny.

Moreover, Telegram's clear positioning as a secure, independent communication tool, notably contrasting itself with platforms like WhatsApp and Facebook, inadvertently reinforced its attractiveness to illicit actors. By emphasizing its non-cooperation with surveillance authorities and its resistance to censorship, Telegram implicitly communicated to criminals that the platform provided a safe space for illegal activities. As noted by external observers, such positioning served as a tacit marketing message, unintentionally promoting Telegram's suitability for clandestine operations (Admin, 2024b).

The 4Ps (Product, Price, Place, Promotion) framework further illuminates how Telegram's marketing mix inadvertently facilitated illicit use. The platform's robust encryption, secret chat capabilities, and user anonymity features provided a perfect toolkit for illicit activities, effectively replicating—and in some ways surpassing—the capabilities of traditional darknet markets. Telegram's free pricing model removed barriers for criminals to scale their activities, thereby lowering transaction and operational costs significantly, contrasting sharply with costlier, complex tools commonly used by illicit networks.

The 'place' dimension illustrates how Telegram's widespread availability and frictionless user experience enabled rapid and extensive dissemination of illicit content and services. Its distribution through mainstream app stores removed any technological or logistical barriers that previously limited illicit activity primarily to niche darknet communities. Telegram's ubiquitous presence, along with its seamless cross-device functionality, ensured continuous accessibility and operational resilience for criminal enterprises.

Furthermore, Telegram's implicit promotional strategies—particularly its emphasis on privacy and resistance to government oversight—served as indirect marketing signals, effectively promoting the platform as safe for illicit activities. The resultant public perception, fueled by media narratives and reinforced through word-of-mouth among illicit communities, cemented Telegram's image as a haven for criminal operations. The widespread informal promotion among cybercriminal forums further elevated Telegram's

attractiveness for illicit use, perpetuating its unintended brand image as a permissive environment for criminal activities.

Digital marketing dynamics, particularly network effects and viral propagation inherent in Telegram's design, significantly accelerated the growth of illicit marketplaces. The ease of joining groups, viral sharing of content, and trust-building mechanisms borrowed from conventional e-commerce practices allowed criminals to rapidly establish and scale their operations. Such mechanisms normalized illicit transactions, diminishing psychological barriers typically associated with explicit criminality. The phenomenon mirrors what consumer behavior literature describes as the online disinhibition effect, wherein anonymity and lack of perceived accountability foster increased willingness to engage in norm-violating behaviors (Suler, 2004). This discussion integrates the marketing theory with empirical observations of Telegram's operational realities, revealing how a platform's intentional marketing strategies can inadvertently cultivate an environment attractive to illicit actors. The findings emphasize the need for platforms to balance aggressive market growth with responsible segmentation and targeted strategies to avoid unintended harmful consequences.

CONCLUSION

Telegram's rise as a premier private messaging app illustrates the complex interplay between marketing an open, privacy-centric service and the emergence of illicit misuse. The platform's broad positioning ("secure messaging for everyone"), feature-rich product, and lack of early moderation created a fertile ground that attracted criminals alongside legitimate users. In this case analysis, I explored how Telegram's STP strategy inadvertently included criminal elements in its user base, and how its 4Ps – especially product and place – enabled a range of illegal enterprises. I discussed how criminals leveraged Telegram's network effects and consumer behavior dynamics, effectively turning a mainstream app into a conduit for black market activities. Theoretical perspectives from academic literature affirmed that Telegram's challenges are emblematic of larger issues in digital platform governance, anonymity, and network externalities.

Key insights from this analysis include recognizing that privacy-first platforms face a dual responsibility: to uphold user rights while preventing those rights from shielding harm to society. Telegram's experience shows that marketing decisions (like emphasizing privacy absolutely) carry ethical and safety implications. A completely hands-off approach is not tenable once a platform reaches global scale; some degree of content governance and clearer positioning are necessary to avoid becoming a sanctuary for criminals. At the same time, heavy-handed crackdowns can drive away the core user base and simply shift illicit actors elsewhere, so solutions must be nuanced.

Moving forward, Telegram and similar platforms should integrate safety by design into their growth strategies. This includes building in abuse reporting and moderation as a standard feature set, much as encryption was built in. It also means actively engaging with user communities and external experts to evolve policies that address emerging threats (such as new scams or trafficking methods on the app). For policymakers, Telegram's case highlights the importance of working with tech companies to strike a balance where privacy and public safety co-exist – overly punitive measures could undermine the former without effectively curbing crime in the long run.

In conclusion, Telegram's marketing-related vulnerabilities have taught the industry a valuable lesson: an open platform's strength can become its weakness when exploited maliciously. By applying marketing frameworks, I dissected how a value proposition intended to attract users broadly also attracted threat actors. Yet, with thoughtful

adjustments and collaborative governance, Telegram can correct course. The platform has already begun implementing changes post-2024, signaling a future where it can maintain its ethos of secure communication while shedding the inadvertent role of "digital safehouse" for illicit activity. The challenge and opportunity for Telegram is to continue growing as a trusted brand for privacy – but one aligned with legal and ethical norms, ensuring that the freedom it offers is not freedom to victimize or violate the law. Achieving this balance will be crucial for Telegram's sustainability and could serve as a model for responsible marketing of privacy technology in the years ahead.

REFERENCES

Admin, N. (2024, December 19). *Is Telegram safe for drug users? — Users News (UN)*. Users News (UN). https://www.usersnews.com.au/home/is-telegram-safe-for-drug-users#:~:text=Durov%E2%80%99s%20reputation%20as%20a%20defender,at%20the%20helm%20of%20VK

Admin, N. (2024b, December 19). *Is Telegram safe for drug users? — Users News (UN)*. Users News (UN). https://www.usersnews.com.au/home/is-telegram-safe-for-drug-users#:~:text=Last%20month%2C%20Telegram%20founder%20and,rife%20on%20the%20messaging%20app

Barratt, M. J., & Aldridge, J. (2017). Everything You Always Wanted to Know About Drug Cryptomarkets. *International Journal of Drug Policy*, *35*, 1-6.

Blankers, M., Van Der Gouwe, D., Stegemann, L., & Smit-Rigter, L. (2021). Changes in Online Psychoactive Substance Trade via Telegram during the COVID-19 Pandemic. *European Addiction Research*, *27*(6), 469–474. https://doi.org/10.1159/000516853

Blankers, M., Van Der Gouwe, D., Stegemann, L., & Smit-Rigter, L. (2021b). Changes in Online Psychoactive Substance Trade via Telegram during the COVID-19 Pandemic. *European Addiction Research*, *27*(6), 469–474. https://doi.org/10.1159/000516853

Dolata, M. (2019). The sources of competitive advantage from the perspective of project management – results of empirical studies," Management, Sciendo, 23(1).

Encryption: a godsend to all who seek privacy, even criminals. (2016, May 20). OCCRP. https://www.occrp.org/en/feature/encryption-a-godsend-to-all-who-seek-privacy-even-criminals

Flare. (2024, November 11). *Illicit Telegram Groups: a new dark web frontier?* Flare | Cyber Threat Intel | Digital Risk Protection. https://flare.io/learn/resources/blog/telegram-dark-web/#:~:text=Illicit%20Telegram%20Groups%20Provide%20Better,Anonymity

Flare. (2024b, November 11). *Illicit Telegram Groups: a new dark web frontier?* Flare | Cyber Threat Intel | Digital Risk Protection. https://flare.io/learn/resources/blog/telegram-dark-web/#:~:text=Cybercriminals%20doubt%20just%20how%20much,phone%20numbers%20on%20the%20service

Gan, C. L., Lee, Y. Y., & Liew, T. W. (2024). Fishing for phishy messages: predicting phishing susceptibility through the lens of cyber-routine activities theory and heuristic-systematic model. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-04083-1

Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. Yale University Press.

Hasan, Md. N. & Bangladesh University of Professionals. (2023). Unveiling the Shadows: Exploring Cyber Criminology and the Plight of Cyber victimization in Bangladesh. In

Jus Corpus Law Journal, *3*(4), 139–141. [Journal-article]. https://www.juscorpus.com/wp-content/uploads/2023/08/25.-Md.-Nazmul-Hasan.pdf#:~:text=An%20offender%20becomes%20motivated%20to,article%20applies%20this%20theory%20to

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, tyw007. https://doi.org/10.1093/cybsec/tyw007

Irwin, K. (2025, January 7). Telegram reports huge spike in data sharing with law enforcement. *PCMAG*. https://www.pcmag.com/news/telegram-reports-huge-spike-in-data-sharing-with-law-enforcement#:~:text=France%20%20over%20allegations%20that,criminals%20to%20abuse%20our%20platform

Katz, M. L. & Shapiro, C. (1985) Network Externalities, Competition, and Compatibility. The American Economic Review, 75, 424-440.

Owwn-Jackson, C. (2024, November 6). *What Telegram's recent policy shift means for cyber crime*. Security Intelligence. https://securityintelligence.com/articles/what-telegrams-recent-policy-shift-means-for-cyber-crime/

Parker, G. G., & Van Alstyne, M. W. (2016). Platform Revolution: How Networked Markets are Transforming the Economy. WW Norton & Company.

Pymnts. (2024, September 9). *Telegram's Criminal Use Spotlighted After CEO's Arrest*. PYMNTS.com. https://www.pymnts.com/cybersecurity/2024/telegrams-criminal-use-spotlighted-after-ceos-arrest/#:~:text=Telegram%27s%20Criminal%20Use%20Spotlighted%20After,same%20time%2C%20Lewis%20noted%2C

Reporter, G. S. (2024, September 24). Telegram's Pavel Durov announces new crackdown on illegal content after arrest. *The Guardian*. https://www.theguardian.com/technology/2024/sep/23/telegram-illegal-content-pavel-durov-arrest#:~:text=Telegram%27s%20Pavel%20Durov%20announces%20new,told%20the%2013%20million

Roth, E. (2024, September 23). Telegram will now hand over your phone number and IP if you're a criminal suspect. *The Verge*. https://www.theverge.com/2024/9/23/24252276/telegram-disclose-user-data-legal-requests-criminal-activity

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. WW Norton & Company.

Solove, D. J. (2011). Nothing to Hide: The False Tradeoff between Privacy and Security. Yale University Press.

Stolen Data Markets on Telegram: a crime script analysis and situational crime prevention measures - Security Insight. (2024, April 15). Security Insight. https://securityinsight.nl/blog/stolen-data-markets-on-telegram-a-crime-script-analysis-and-situational-crime-prevention-measures#:~:text=Illicit%20data%20markets%20have%20emerged,bid%20for%20these%20valuable%20assets

Uren, T. (2024, October 11). *How Telegram turbocharges organized crime*. Default. https://www.lawfaremedia.org/article/how-telegram-turbocharges-organized-crime#:~:text=Telegram%20acts%20as%20a%20communication,fabric%20for%20this%20criminal%20ecosystem

Uren, T. (2024b, October 11). *How Telegram turbocharges organized crime*. Default. https://www.lawfaremedia.org/article/how-telegram-turbocharges-organized-crime#:~:text=A%20new%20report%20highlights%20the,and%20even%20murder%20for%20hire

Waldman, A. (2024, September 17). *Infosec experts detail widespread Telegram abuse*. Search Security. https://www.techtarget.com/searchsecurity/feature/Infosec-experts-detail-widespread