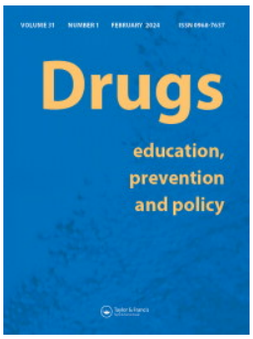

Drugs: Education, Prevention and Policy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/idep20

"I straight up criminalized myself on messenger": law enforcement risk management among people who buy and sell drugs on social media

Robin van der Sanden, Chris Wilkins & Marta Rychert

To cite this article: Robin van der Sanden, Chris Wilkins & Marta Rychert (20 Jun 2023): "I straight up criminalized myself on messenger": law enforcement risk management among people who buy and sell drugs on social media, Drugs: Education, Prevention and Policy, DOI: 10.1080/09687637.2023.2224497

To link to this article: https://doi.org/10.1080/09687637.2023.2224497

Published online: 20 Jun 2023.

DRUGS: EDUCATION, PREVENTION AND POLICY
https://doi.org/10.1080/09687637.2023.2224497

Taylor & Francis
Taylor & Francis Group

"I straight up criminalized myself on messenger": law enforcement risk management among people who buy and sell drugs on social media

Robin van der Sanden, Chris Wilkins and Marta Rychert

SHORE & Whāriki Research Centre, College of Health, Massey University, New Zealand

ABSTRACT

Background and Aim: Social media drug markets are likely to present people participating in these spaces with new vulnerabilities to law enforcement. There is currently limited research on how people perceive and manage the risk of exposure to law enforcement in social media drug markets. This is particularly notable considering widespread practices of user data collection and the normalization of surveillance as part of social media engagement.

Methods: We present a thematic analysis of data from anonymous online interviews with people who buy and sell drugs (N=33) via social media and messaging apps in New Zealand. We use the concept of "imagined surveillance" to explore how participants adapted existing understandings of online surveillance to online risk management strategies to avoid police.

Findings: Most participants reported low concern for exposure to law enforcement while using social media and messaging apps for drug trading. Nevertheless, almost all participants took active risk management measures. Examples of strategies used included limiting the accumulation of evidence via self-deleting messages or arranging drug trades using code language. Participants often also reported low concern for their digital trace data to be accessed by police.

Conclusions: Navigating law enforcement risk in social media drug markets is likely to be informed and shaped by more general perceptions of digital privacy risk and related management strategies, particularly in more normalized drug market contexts. The potential for broader and unexpected consequences to result from the use of drug-related digital trace data across public and private contexts is discussed.

ARTICLE HISTORY
Received 25 October 2022
Revised 9 May 2023
Accepted 7 June 2023

KEYWORDS
Law enforcement; social media drug markets; social media data collection; digital surveillance; digital security

Introduction

Social media and app-facilitated drug markets increasingly provide easily accessible, local pathways to buy and sell illegal drugs (Demant et al., 2019; Moyle et al., 2019). Social media can be defined as online platforms or services which facilitate networked connection, interaction and collaboration between people, groups, and organizations through the medium of easily accessed user-generated content (McCay-Peet & Quan-Haase, 2016). This definition can be expanded to include encrypted messaging platforms such as Wickr, Signal, and Telegram, based on their respective platform features.

Existing findings indicate that social media drug markets are likely to be most often used by young people to buy and sell small amounts of drug types like cannabis and MDMA (Oksanen et al., 2021; van der Sanden et al., 2021). As such, a high degree of normalization around recreational drug use, particularly cannabis, has been highlighted as a facilitator of the uptake of social media for drug procurement (Demant & Bakken, 2019), and has been reported in relation to other types of surface web drug-purchasing websites (Childs et al., 2022). As part of perceptions of certain forms of drug use as "normal," and the techniques of "neutralization" (Sykes & Matza, 1957) employed by both buyers and sellers, risk perceptions around the purchasing and supply of drugs may also be lower (Coomber et al., 2016). For example, Childs et al. (2022) found buyers using the website *LeafedOut* to buy cannabis in Australia were largely unworried about law enforcement, based on a belief that police were "not interested" in cannabis offenses and due to the small size of most transactions.

Despite evidence that social media drug trades may often be viewed as low-risk, there is currently little research exploring how participants in these markets perceive vulnerability to police as part of social media drug trading, and what strategies they employ to prevent detection by police. Both Moyle et al. (2019), and Childs et al. (2022) emphasize the importance of digital trace data "trails," including messages, photos, and additional data sources, to perceptions of law enforcement risk among buyers and sellers. Though Moyle et al. (2019) found that being caught by the police because of digital trace data was not a primary concern among respondents, they also found considerable differences in how respondents perceived themselves to be vulnerable to police on social media. Notably, respondents were at times

CONTACT Robin van der Sanden r.vandersanden@massey.ac.nz SHORE & Whāriki Research Centre, College of Health, Massey University, New Zealand

uncertain of whether or how they might be at risk of getting caught, suggesting they "couldn't be sure they were not being monitored" (Moyle et al., 2019, p. 108). Additionally, a recent paper from Bakken et al. (2022) exploring digital capital in social media drug selling demonstrated that sellers' digital risk management strategies often involve subjective perceptions of what constitutes digital security from law enforcement and may draw on factors beyond platform security features. These findings indicate the complexity of understanding and navigating law enforcement risk and digital security as part of social media drug trading. Further investigation of these risk perceptions and related risk management behaviors is important given the widespread awareness of social media surveillance by governmental institutions and the challenges of maintaining individual privacy in these spaces (e.g. Acquisti et al., 2015; Lyon, 2018). These broader factors are likely to play a substantial role in influencing how buyers and sellers in social media drug markets perceive law enforcement risk and their resulting risk management behaviors but have yet to be explored by researchers.

This paper contributes to existing understandings of how social media and messaging apps are navigated for drug trading purposes by demonstrating how perceptions of vulnerability to law enforcement and resulting social media risk management practices may be shaped by people's understandings of digital privacy and surveillance more generally. To illustrate this relationship, we explore these perceptions and behaviors in the context of social media drug trading characterized by substantial normalization, and therefore self-expressed low-risk perceptions around police. We acknowledge that explorations of law enforcement risk and risk management behaviors are often framed in terms of deterrence (Gibbs, 1975) or restricted deterrence (Moeller et al., 2016) theories. However, in this paper, we focus on exploring how broader understandings of visibility, digital trace data sources, and third-party data collection practices influence perceptions and inform strategies used to navigate law enforcement risk as part of social media drug trading. This focus allows us to explore some of the novel challenges that may arise as part of embedding drug trading behaviors into a social media context. In particular, the question of how digital trace data generated as part of social media drug trading may challenge 'traditional' links between being physically caught by police and the disadvantaging and harmful effects associated with having a criminal record (e.g. Uggen et al., 2014).

Background

Data persistence, divergent platform features and "imagined surveillance"

In this paper, we consider two interrelated characteristics of the social media environment as important factors in shaping buyers' and sellers' perceptions of and attempts to manage their risk of exposure to law enforcement: data persistence (Mayer-Schönberger, 2011), and "imagined audience" (Litt, 2012). Data persistence refers to the potential for online content, such as videos, messages, and photos to remain searchable and accessible online overtime (Boyd, 2014; Koops, 2011). Many contemporary social media platforms provide the capability to post temporary content (e.g. "stories" on Facebook, Instagram, or send disappearing messages on Snapchat), and most messaging platforms enable the use of message-timers to prevent the accumulation of chat logs over time. Additionally, end-to-end encryption helps to ensure that messages and content which are not automatically deleted are protected from snooping by third parties like the police (Endeley, 2018). These inbuilt features have been identified as important factors underpinning people's preference for social media drug trading (Moyle et al., 2019).

Existing research on social media drug trading highlights the practice of using different platforms for different parts of a drug transaction as a method used by sellers to maintain greater security from law enforcement (Bakken & Demant, 2019). Often this practice involves using multiple platforms to ensure that the most sensitive stage of the transaction is organized on a platform where messages are automatically deleted and/or end-to-end encrypted (Bakken & Demant, 2019; Childs et al., 2022; Demant et al., 2019). End-to-end encrypted messaging services such as Wickr have faced broad scrutiny for "insulating" drug sellers, among other criminal actors because of platform features that enable temporary, anonymous communication (Christou, 2018; Silva, 2015).

Though social media offer their drug market participants a diversity of security features which can be combined to protect them from the police, similar platform features and functions can mask small but important differences across apps (Versus, 2022; Williams, 2022). This terrain makes it more likely that platform users may fail to fully understand how secure a given platform is, particularly concerning features such as end-to-end encryption (e.g. Abu-Salma et al., 2017). Indeed, Moyle et al. (2019) have highlighted that people using social media and messaging apps for drug trading make erroneous assumptions of security based on a faulty understanding of platform features. They found this was particularly the case around whether platforms end-to-end encrypted user messages, but also highlighted low awareness around the potential for self-deleting messages or pictures to be stored via third-party apps (Moyle et al., 2019).

Despite these security enhancements, perceptions of online data as permanently accessible often continue to guide people's perceptions of their online security and privacy (Kang et al., 2015). While messages or images may be increasingly easy to delete, other stored forms of online data remain available. For example, metadata such as geolocation tags, timestamps on communications, and EXIF data on images provide contextual information on users and their interactions. These can be used to identify and track users' activities with considerable accuracy, in lieu of direct access to messages (Newell & Tennis, 2014; Perez et al., 2018; Sarre, 2017).

Data persistence and the dynamic network nature of social media greatly challenge people's ability to control when, where, and how content is circulated, and in turn who can view or access it (Boyd, 2014; Litt, 2012; Litt & Hargittai, 2016). Social media data is easily spread beyond its intended recipients, or alternatively, online data generated by others can lead to personal information being shared or publicized irrespective of individual action or intent (Boyd, 2007; Marwick &

Boyd, 2014). Indeed, examples of people facing professional, family, political, and legal consequences resulting from the "leakage" of digital information from one context into another are increasingly common.

As a result, research findings suggest people have become accustomed to managing the potential for continuous surveillance from others on social media (Albrechtslund, 2008; Boyd, 2007; Marwick, 2012). Duffy and Chan (2019) introduce the concept of "imagined surveillance" to explain how young people are increasingly taught to assume their social media presence will be scrutinized by others, including family, prospective employers, and even the police (See also, Lyon, 2017, 2018). They argue that "imagined surveillance" results from the consideration of two interrelated factors: "imagined audience" and "imagined affordances" (Nagy & Neff, 2015). "Imagined audience" describes people's perceptions of who *could* view their social media presence, or messages and data, both now and in the future. "Imagined affordances" describe how people perceive platform features as either making them vulnerable to, or insulating them from, online surveillance (Duffy & Chan, 2019). Duffy and Chan (2019) suggest that young people actively respond to this continuously shifting potential for online surveillance by using both platform features and social practices to manage the outcomes of "imagined surveillance."

In this paper, we use the concept of "imagined surveillance" to explore how buyers and sellers transacting in social media drug markets perceive and respond to the potential for exposure to law enforcement. In doing so, we consider how people's more general perceptions of risks around digital exposure to others on social media come to inform both their perceptions of vulnerability to law enforcement and subsequent digital risk management behaviors.

Technology: New opportunities and new vulnerabilities for people who buy and sell drugs

The introduction of new digital communication technologies such as the mobile phone, and later the internet and smartphones, into drug selling practices represents both new opportunities to avoid detection by law enforcement, as well as new vulnerabilities. For example, the mobile phone facilitated greater seller adaptability and flexibility in the face of evolving policing strategies, allowing sellers to easily shift to secure physical locations for exchanges (Barendregt et al., 2006; Fader, 2016; VanNostrand & Tewksbury, 1999). On the other hand, this development also paved the way for the police practices of wiretapping and requesting text and call logs from mobile service providers as a means of gathering evidence (Diffie & Landau, 2010).

Darknet markets (otherwise known as cryptomarkets) also exhibit a similar trade-off between new opportunities for increased anonymity and security, and new vulnerabilities. These spaces facilitate anonymous drug transactions with participants protected by many different online security features such as anonymous accounts, cryptocurrency payment, and the marketplace's location on the un-indexed deep web (Aldridge & Décary-Hétu, 2016). However, the need to send and receive packages using postal services opens buyers to detection if packages are intercepted, leading to a proliferation of risk management strategies among buyers around "safely" receiving packages (Aldridge & Askew, 2017). Additionally, the success of several, increasingly sophisticated law enforcement operations and the resulting seizure and shutdown of large darknet marketplaces have undermined trust in these sites (Décary-Hétu & Giommoni, 2017; Ladegaard, 2020). Similarly, recent seizures of encrypted messages on platforms like SKY ECC (Soudijn et al., 2022), and the ANOM operation (Parkin, 2021) provide indications of evolving law enforcement capacities relating to encrypted communications (Greenberg, 2018).

Law enforcement agencies around the world use social media for a range of investigative and surveillance purposes (Trottier, 2012; Walsh & O'Connor, 2019). Social media companies generally provide channels through which both U.S.-based and international law enforcement agencies can make legal or emergency requests for access to user data (e.g. Discord, 2022; Meta, 2022d; Snap Inc., 2020). However, any legal requests must be made via U.S. courts, which can make this process more time-consuming for non-U.S. agencies such as the New Zealand Police. Meta's latest transparency report highlights a steady increase in legal requests for user information made by government agencies from 2013 onwards. Globally, governmental agencies made just under 215,000 requests to Meta for user data on more than 360,000 social media accounts in the last six months of 2021, of which 73% generated some "usable data" (Meta, 2022b). "Usable data" may refer to basic subscriber information such as name, duration of platform membership, email addresses, data on account activity such as IP addresses, and stored account content such as messages, photos, and location information. However, as Meta states, they *"produce only the information that is narrowly tailored to respond to each request"* (Meta, 2022a).

Public aspects of people's engagement with social media, such as user profiles and information including their social networks or tagged photos may be accessed by police as part of routine investigations of social media profiles (Egawhary, 2019). The seizure of devices such as phones and laptops as part of many contemporary police investigations, or the requesting of social media credentials and login information as part of cooperation with a police investigation (e.g. Espiner, 2021; Levin, 2021), can generate access to a person's social media presence. This can make it possible to gather significant social media information and data without filing legal requests (Arshad et al., 2019; Egawhary, 2019; Morrison, 2021). Additionally, police may be able to access social media data via third parties, such as data brokers or open-source intelligence platforms (Brayne, 2017). This latter point evidences the potential for social media data to be combined with other forms of digital trace data and accessed by companies and institutions beyond law enforcement (Brayne, 2020; Koops, 2011). These developments underscore the importance of considering the global data trade (Kitchin, 2014) in relation to social media drug trading. It may be that awareness of user data collection practices by social media companies, and the inclusion of these data sources in a broader data trade similarly influences how people understand and manage their digital security in relation to drug trading.

The New Zealand drug market context

Drug use patterns in New Zealand have historically been shaped by the country's small population and geographic isolation (Wilkins et al., 2017). This has meant that imported drug types like MDMA, cocaine, and heroin have often been of varying availability, potency, and price compared to locally grown and manufactured drug types like cannabis and methamphetamine (Wilkins et al., 2018). The annual Household New Zealand Health Survey (NZHS) estimates that past-year use of cannabis was 15%, MDMA was 4.3%, hallucinogens was 2.5%, and methamphetamine 1.3% in 2022 (Ministry Of Health, 2022). This is likely an underestimate of methamphetamine use owing to the drug's embeddedness in many marginalized, hard-to-reach populations in rural regions (Wilkins, Prasad, et al., 2018; Wilkins, Romeo, et al., 2018).

Cannabis use in New Zealand appears normalized among younger people (Robertson & Tustin, 2020). Indeed, cannabis was most often purchased from social media among 2020 New Zealand Drug Trends (NZDTS) respondents. Of respondents who had purchased cannabis in the prior six months, 24% had done so via social media (van der Sanden et al., 2021). Most respondents used Facebook (including Messenger) to purchase drugs (60%), followed by Snapchat (48%) and Instagram (20%) (van der Sanden et al., 2021). This indicates a high proportion of transactions taking place on so-called "low security" platforms (van der Sanden et al., 2022a). The development of novel, local social media drug market trends has also been documented in New Zealand in the form of Discord[1] drug servers (van der Sanden et al., 2022b).

The role played by social media platforms in facilitating arrests relating to drugs and other crimes in New Zealand is emergent. From June to December 2021, New Zealand agencies made a total of 259 legal requests for user data to Meta during this period – the largest number of requests to date – of which 82% generated some "usable data" (Meta, 2022c). Media reports commonly cite encrypted Wickr messages as part of incriminating evidence used to arrest drug traffickers or gang-related trials, but also cite simultaneous intercepting of voice calls and text messages among criminal communications (e.g. Bayer, 2022; Savage, 2022). Additionally, recent reports on a police operation in Queenstown where 12 people were arrested for their role in the local resale of darknet-sourced drugs cited police discovery of a "Facebook group" as the basis of the operation, though details of how subsequent evidence was gathered and how the group was infiltrated were not disclosed (Swift, 2022; Williams, 2023).

This paper explores how people who buy and sell drugs via social media perceive their vulnerability to law enforcement as part of social media drug trading, and the related behaviors and practices they develop to try and counter these perceived vulnerabilities.

Methods

This paper presents a thematic analysis (Braun & Clarke, 2012) of data gathered from anonymous qualitative online interviews with people who use social media to buy and/or sell drugs as part of a broader project exploring the use of social media for drug trading in New Zealand (van der Sanden et al., 2021; 2022b). Thirty-three people participated in synchronous online chat interviews (Bakken, 2022; Barratt, 2012; Gibson, 2022) via the encrypted messaging app Wickr me (Wickr) between July 2020 and September 2021. Interviews were semi-structured to ensure questions were adaptable across a range of different drug market roles and patterns of social media use. Semi-structured interviews provide greater flexibility in responding to issues or experiences raised by participants that might not have been planned for (Brinkmann & Kvale, 2015). Development of the initial interview schedules was based on a comprehensive literature review, and the results of an earlier large-scale quantitative survey of people who purchased drugs via social media in New Zealand (van der Sanden et al., 2021).

To encourage open disclosure by participants and address the anticipated difficulties of recruiting from a hard-to-reach population (Coomber, 2011), the research team used the encrypted messaging app Wickr to carry out interviews (see also, Bakken, 2022). We anticipated that prospective participants would be more willing to share their experiences anonymously via direct messaging (Barratt, 2012). The choice of direct messaging as the interview medium also reflected our assumption that many participants would be younger in age (e.g. < 25 years old). We recognized that many young people view direct messaging as more "relaxed" than in-person or phone conversations, particularly when talking to strangers (Gibson, 2022). Participants appeared comfortable using Wickr to complete interviews. However, whether this reflects more general trust in app security may be more complex, and likely reflects participant trust in Wickr's packaging together of different security features, particularly the ability to sign up anonymously. Wickr has been used in previous research with social media drug sellers internationally (Bakken, 2022; Demant et al., 2019), as well as with surface web cannabis sellers and buyers (Childs et al., 2022).

Participants were recruited using a targeted sampling approach (Watters & Biernacki, 1989) involving different social media channels (Facebook and Reddit) to promote the study, and by physically distributing flyers at the entrance to a dance music festival. New Zealand-based Facebook groups and subreddits focusing on dance music (Forsyth et al., 1997) or cannabis culture were targeted. Group administrators/moderators were approached for permission to post on these forums. Information promoting the study was also posted to social media (Facebook, Instagram, Twitter) by the New Zealand drug-checking service *Know Your Stuff*. Participants were required to be aged 16+ and have some experience using social media to buy and/or sell drugs in New Zealand. Interviews were completed over the course of several hours, or sometimes several days if there were breaks between ongoing messages. The longest interview duration was five days. Participants were offered a supermarket voucher as reimbursement for their time.

Eleven participants took part in a small follow-up interview (also via Wickr) six months after their initial interview. These interviews were aimed at further developing an understanding of social media drug markets by enabling clarification and checking of interpretations of responses and views. The follow-up interviews also provided an opportunity to ask

participants about additional topics that had emerged from previous interviews with other participants.

The analytical process followed Braun and Clarke's Six-step Thematic Analysis framework (Braun & Clarke, 2012, 2022). We developed the initial coding structures based on a combination of deductive elements drawn from the existing literature and inductive findings generated from initial interviews. Codes were refined as the data collection and analysis progressed. Interviews were initially read and coded by hand based on descriptive data such as apps used for drugs, drug market roles, and seller types, and perceived risk or negative experiences. For each code group, we maintained a memo detailing any development in thinking and noting interview transcripts or excerpts that were particularly important to the codes in that group. An overarching "project memo' was maintained to map developing themes and relationships between code groups. We combined this with ongoing concept mapping to refine relationships between data, codes, code groups, and themes.

The original language used by participants in the interviews has been retained as part of the presentation of findings in this paper. Clarification of slang terms in the interview excerpts is provided in non-italicized parentheses.

This research received ethics approval from Massey University Human Ethics Committee Southern A (application code: SOA 20/22).

Findings

Contextualization of sample

Most of the participants used social media only to buy drugs (n = 20), while the remainder (n = 13) had differing levels of experience in both buying and selling. The drug types most often purchased through social media were cannabis (n = 25), MDMA (n = 23), and LSD (n = 23). However, other drug types purchased and sold included ketamine (n = 9), cocaine (n = 6), pharmaceuticals such as Ritalin and benzodiazepines (n = 6), and, psilocybin (n = 4) occasionally also diverse novel psychoactive substances (n = 3). Cannabis, MDMA, and LSD were most often sold among participants with selling experience.

The median age of participants was 24 (IQR = 19.5–26), with the youngest aged 16 and the oldest 39. Twenty-two participants identified as male, 10 as female, and one as gender neutral. Most participants resided in New Zealand's more populous North Island (n = 23), with 10 living in the South Island. Among participants in the interview sample, Messenger and Snapchat were the platforms most often used to buy and sell drugs (both n = 17), followed by Wickr (n = 16), Discord (n = 12), Signal (n = 5) and Telegram (n = 4). In line with findings on the use of social media drug markets internationally (e.g. Demant et al., 2019), participants predominantly used these platforms to connect with sellers and arrange transactions, which were then completed largely via in-person pickup or delivery, and occasionally via post.

Transaction risks and concern for law enforcement

Most participants expressed little concern for law enforcement when using social media and messaging apps for drug transactions. Participants tended to be involved in buying via social media for personal consumption or occasionally supplying their friends, often using social media primarily to access cannabis. These participants considered themselves "small fish," rationalizing that they were of little interest to law enforcement:

> *I doubt police would be looking at my socials. Maybe naïve but I feel like they have bigger fish to fry.* (**P17**, F26, buyer)

Participants who expressed greater concern about exposure to law enforcement were more often involved in selling or buying larger quantities of drugs. Alongside drug quantity, drug type was also a factor in either increasing or decreasing participant concern. Class A or B substances like LSD and MDMA were viewed as higher risk because of higher legal penalties faced for their supply and possession versus a Class C drug type like Cannabis. Hence, for buyers buying upwards of 2 grams of a substance such as MDMA or Ketamine was considered more high risk, but for sellers this could be more variable. For example, one seller involved in selling $50 bags of cannabis in a more commercial local market context professed high concern for police. Another participant involved in the darknet import and social media resale of large amounts of MDMA (e.g. a half-pound, or 228 grams) within a friendship-oriented "social dealing" context had relatively low concern for police.

Participants often reported a lack of direct experience with law enforcement related to their involvement with either buying or selling drugs generally. Some participants had previous experiences with police related to cannabis and this appeared to reinforce their perception of cannabis as being a low priority for police:

> *Eh the police already have evidence of me buying and selling drugs from a few of my mates' phones when they got arrested and have seen weed lying out next to a bong in my flat before and not said anything so…* (**P10**, M21, buyer)

Despite this many participants still took steps to manage their risk of exposure to law enforcement. For many participants, the apparent contradiction between their perceptions of law enforcement as low risk, and their use of subsequent digital risk management strategies reflected an ingrained awareness of the pitfalls of online communication that could lead to unwanted exposure to others . In these instances, participants often referenced two core aspects of the social media environment which guided their use of digital security strategies: Data persistence, and imagined audience.

Factors influencing vulnerability to law enforcement on social media

Data persistence

Data persistence was often referenced by participants as a principal drawback of using social media and messaging platforms for drug trading. Participants articulated a belief that their online data and messages remained "online forever":

> *I guess you have to factor in that anything you put on the internet is essentially out there for good and you can't take it back. So knowing*

there is a paper trail of messages etc is a downside and a risk. (**P17**, F26, buyer)

The availability of incriminating messages over time was viewed as an accumulation of evidence. Some participants had knowledge of people who were incriminated because of permanent messages, often involving the use of Facebook Messenger:

I know someone who got busted via facebook messages during a raid. I think they got their phone and just went through it… it was taken from them. (**P19**, F26, buyer).

For this reason, consideration of data persistence was a key factor in how participants looked to manage their risk of exposure to law enforcement, and one which guided how they used other risk management strategies or juggled different platforms for drug trading purposes.

Broad audience

In combination with the problem of data persistence over time, many participants articulated the difficulty of controlling their social media audience as a point of vulnerability to police exposure. For participants, situating the risk of exposure to law enforcement as part of social media drug trading involved acknowledging the continuous potential for information to be made visible to the "wrong" people, either through their interaction with different platforms, or because of others viewing their phone screens:

The fact the wrong person could be looking at my phone at the wrong time, so cautious with that too… if I leave my phone sitting around. (**P24**, M31, buyer/seller)

I think them (the seller) *getting caught and the police going through their social media contacts or the police pretending to be them…* (**P30**, F17, buyer)

When you sign up to Signal it alerts all your contacts that also have Signal! I got a notification that my boss had joined signal… the information feels insecure and could either be leaked to cops or friends. (**P19**, F26. Buyer)

These excerpts underscore how participants tended to experience vulnerability to law enforcement on social media in ways that merged exposure to police with the potential for surveillance and scrutiny from others in their social networks. As the example from P19 illustrates, exposure to one's employer on social media could easily be extrapolated to serve as a general "proxy" for increased risk of exposure to other groups, including the police.

Digital trace data and social media data collection

Many participants were aware of social media data harvesting, and the potential for this data to be accessed by third parties. The availability of this data and the potential for police access to it was sometimes viewed with a sense of resignation and indifference:

My data's been bought and sold a thousand times by now I don't care which company has it anymore. (**P10**, M21, buyer)

However, when it came to thinking about the likelihood of their data being accessed by law enforcement or requested using a warrant, most participants rationalized this level of effort as not likely to be justified by their "small fish" status:

If someone wanted to collect all my digital trail and bust me I'm sure they could, but I think a huge portion of people my age don't think any cop cares enough about that kind of stuff to do anything. (**P27**, M23, seller)

The level of effort participants assumed it would cost police to request their data from social media companies then meant this was a threat that predominantly affected sellers or people more heavily involved in their local drug trade. Among participants who were more concerned about exposure to law enforcement, data collection by social media companies such as Meta was viewed as another reason to avoid these platforms for drug trading, regardless of actual practice, and a strong incentive to use encrypted messaging apps:

Oldmate Zuck [Mark Zuckerberg] *can just look for a couple keywords and send in what he finds to law enforcement. Stands true for any big social media. Which is why sellers should move away from social media and use applications with privacy in mind.* (**P32**, M19, buyer/seller)

If you want to be secure and private use something like wickr or the dark web… but Facebook and other social media platforms? You give them the right to see your data when you sign up. (**P8**, M23, buyer/seller)

Following this, the first risk management strategy turned to by many participants to insulate themselves from possible police surveillance was the strategic use of different platforms to facilitate greater security around the most high-risk drug transactions.

Perceptions of platform security: Platform ownership and shifting "locations"

Most participants made use of platforms for drug trading that had one or more of three key "security" features: (1) message timers or self-deleting data; (2) username-based sign-up; and (3), end-to-end encryption. The more security features a particular platform had, the more appropriate it was perceived to be for drug transactions involving a higher risk of legal penalties, such as large quantity purchases, selling drugs, or transactions involving Class A drug types. Participants often used platforms such as Wickr to add security to more "high stakes" drug transactions that would result in more severe legal penalties, while conversations about "low risk" transactions could take place in less-secure settings like Snapchat. Though buyers often followed sellers to high-security platforms in commercial drug trading contexts, this could be complicated in a normalized drug market involving social supply, where low-risk perceptions could prevent sellers from shifting to more secure encrypted messaging apps. Additionally, platforms like Wickr occupied a position well outside participants' day-to-day social media engagement which helped them keep their drug trading practices separate from their day-to-day social media use. In this vein, encrypted messaging apps helped participants manage their "imagined audience" more effectively, by serving as platforms used specifically for drug trading.

However, perceptions of platform security could extend beyond platform features. For example, encrypted messaging apps and their association with a need for secrecy made some participants feel as though they were "advertising" their involvement in drug trading to others. In this instance, participants considered what the using encrypted messaging apps "said" about them from the perspective of an onlooker. In this vein, using platforms like Snapchat for drug trading could *also* function as a risk management strategy by allowing buyers and sellers to transact on an inconspicuous, mainstream platform:

> **P21:** *I think Wickr is great but it's less commonly used and definitely for your more paranoid user. I think there would be a certain level of suspicion if other people saw it on your phone.*
>
> **Interviewer:** *So Snapchat is kind of like a "normal" app to have on your phone, and you already use it to chat with mates so it doesn't feel as dodgy?*
>
> **P21**: *Yeah exactly.* (M17, buyer)

Participants with a more comprehensive understanding of app features and online security tended to stress the need to consider additional platform features when thinking about their suitability for drug trading. For example, several participants placed importance on platform ownership, and prior knowledge of company cooperation with law enforcement as important factors to consider when engaging with social media drug markets:

> *Telegram is such a good app and I don't trust Facebook. The fact that they've been pressured by governments to hand over data and haven't. That's a pretty big tick… if Telegram aren't handing over any data at all then I don't worry about my account being tied to my username or my phone number.* (**P9**, M29, buyer/seller)
>
> *ASW* [Amazon Web Services] *bought Wickr so some people rumour about it but I trust it… Wickr has a good rep and validation by third parties. I wouldn't trust the Bezoses of this world as far as I could throw them… in saying that ANOM has taught the world it's good to know who owns your software.* (**P25**, M27, buyer)

These examples highlight the importance of broader consideration of platform security beyond platform features. This type of understanding was often lacking among participants involved in small-scale buying or social supply behaviors. Participants with a deeper understanding of online security often also considered using, or made use of additional online security features such as VPNs or removing EXIF data from images they posted or sent as part of social media drug trades. However, ultimately, even participants in this group appeared to balance their need for additional online security with the principal reason they used social media for drug trading to begin with – convenience:

> *I'm also lazy so don't take all the precautions I should* [such as] *separate Discord for social and drugs, not sending direct to myself, VPN. But in reality the way I use Discord I find a nice compromise between safety/anonymity and convenience.* (**P23**, M21, buyer)

Managing exposure to law enforcement on "low security" platforms and drug markets

Despite the emphasis placed on staying away from low security platforms such as Messenger for drug trading, many participants continued to use these platforms for small-scale trades between friends. Additionally, some participants made use of large, more "public" social media drug markets such as "lower tier" Discord drug servers, which are characterized by a high level of accessibility and a large size. In these settings, participants felt at risk of exposure to "undercover" police. In these environments, platforms lacked many of the features participants equated with greater security from police. As a result, they developed tailored risk management strategies which were geared towards managing "imagined surveillance" in lieu of these platform protections.

Managing law enforcement risk in "lower tier" Discord servers

Discord drug servers enabled buyers and sellers to transact using pseudonyms. Though this feature was useful as a means of providing some protection from police, it also challenged people's ability to "survey their surroundings" for law enforcement, as is characteristic of risk management strategies in offline, street drug markets for example. As a result, market members were often highly sensitive to perceived shifts in the drug server environment, as well as to nuances in their interactions with others on the drug servers:

> *There was a lot of paranoia and finger-pointing around any perceived shift in culture within the servers. One server had a mass exodus after the admins sold it on to an anonymous buyer, after which they immediately started requesting photo ID with verifications*[2]*… It was the biggest server at the time too, so it just came across as really suspicious.* (**P15**, F31, buyer/seller/ex-drug server admin)
>
> *I got a message like this "Need a 50 outdoor indica to dome, free late night drop." Feel like now one really talks like that lol* (**P6**, F19, buyer)

These excerpts underscore how server members used available online cues such as the structure of messages they received or visible changes to drug server features to make judgements around the potential for exposure to police.

Notably, drug servers also contained channels where members could post warnings to others of police checkpoints or arrests involving other market members, creating a community-based awareness of local police presence. The sharing of knowledge related to police activities potentially helped server administrators to address the risk of police infiltration, and also helped members to avoid police as part of completing transactions offline:

> *It's building up quite a community feel ATM* [at the moment] … *someone got stopped by the police and their phone was taken (I'm assuming they were arrested), once people were aware of that, the person's access to servers were stopped.* (**P7**, M39, buyer)

On Discord drug servers, managing the risk of exposure to law enforcement primarily meant focusing on the attributes of other market members, and of the servers themselves. Considering the actual security of the platform appeared to be almost an afterthought for most participants in this setting. This represents an important point of contrast to the importance of platform security features (or lack thereof) to risk management in other social media drug market environments.

Using "code" to talk about drugs on Messenger

While some participants in Facebook selling groups mentioned the use of emojis by sellers to advertise drugs, sellers on Discord servers did not tend to use code, instead opting to advertise drugs more openly. However, almost every interviewee who made use of Messenger for drug trades, often with friends or social connections, emphasized the importance of using code language to "disguise" drug trading conversations. In these contexts, the social nature of buyer and seller contacts allowed them to construct more personalized code words and language to disguise drug trades:

> *It was usually people asking if they'd come over, or asking for colors, or coded substances in a message… When stuff arrived it would usually be a "hey you should come over for a sesh" and they'd know.* (**P12**, Gender neutral, 25, buyer/seller)

> *I never did the "hey have you got any bottles of milk/crayfish/whatever" sort of thing… I always thought that was pretty stupid and obvious. I would say the vast majority of the time if someone unlocked my phone it would be indistinguishable from a normal conversation.* (**P18**, M26, buyer)

In keeping with the above excerpts, interviewees' perceptions of what counted as effective code language varied. The aim of using code language was primarily to mask drug trading conversations, as well as to limit the amount of obviously incriminating evidence that accrued in Messenger chats. This meant thinking about how messages would be visible to others in the event a phone was taken, or messages were read by the wrong person and exemplify the evolving social practices that can characterize responses to "imagined surveillance."

There were instances where participants neglected to use code when using platforms like Messenger. For example, the quote featured in the title of this paper refers to **P32's** (M19, buyer/seller) experience using Messenger to both buy and sell drugs without using code or the secret chats feature. For some participants, a gradual shift away from using code on platforms like Messenger reflected the challenges of managing a general accumulation of drug-related messages and content as part of group chats with friends, which made using code specifically to talk about small transactions seem pointless:

> *These days I don't have really a formal code with anyone. If someone got my messenger chats there would definitely be some stuff in there, but there's literally photos of me doing lines in some group chats, so I think you just don't worry too much at a certain point.* (**P27**, M23, seller)

In some instances, participants who felt they had left a trail of incriminating messages behind on Messenger made the effort of combing back through their chat history and manually deleting drug trading conversations.

The perceived need to use "code" language tended to decrease as participants shifted to more secure platforms offering features like end-to-end encryption and self-deleting messages. However, even on "more secure" platforms like Snapchat, participants were still aware of the potential for drug-related messages and snaps to spread beyond their intended audience. To minimize the unwanted spread of incriminating evidence, sellers often avoided posting photos of their stock, opting to keep "adverts" vague, or not use them at all:

> *Hahaha, no way! No stories at all… I have had experience with people like this in Aussie. But they seem to get arrested or busted a lot. In my opinion I think it's a risky and stupid way to do it. You can be a lot safer and make the same money.* (**P24**, M31, buyer/seller)

Despite the ability to post private stories, visible to only selected contacts on Snapchat, P24 continued to feel that the only guaranteed way to avoid incriminating stories being spread to the wrong people was not to post them at all. He insisted on only communicating one-to-one with his buyers, and only via snap (images/photos), explaining that messages were far easier to save on Snapchat.

Discussion

This paper has explored how understandings of digital privacy and the potential for surveillance as part of broader day-to-day engagement with social media and messaging apps influence how law enforcement risk is perceived and managed among people involved in small-scale social media drug trading. In this context, the concept of "imagined surveillance" (Duffy & Chan, 2019), helps to explain the apparent contradiction between participants' self-expressed low-risk perceptions around exposure to law enforcement, and their subsequent use of diverse digital risk management behaviors. Our participants were often young people involved in low-risk market roles and using social media drug markets largely to access these drug types amid reportedly low risk perceptions around law enforcement. However, low risk perceptions were paralleled by the use of a range of risk management strategies that addressed what participants perceived to be digital risk areas that could become potential sources of exposure to others such as employers or family members. This is in keeping with "imagined surveillance," where social media users often already assume people beyond their immediate social networks are scrutinizing their social media presence and factor this into how they use different platforms (Duffy & Chan, 2019). We have suggested that perceptions of digital data as permanently accessible, lack of control over digital audience, and digital surveillance by others help inform participant perceptions of how they could be caught by police, and subsequently what constitutes "good" digital security practice as part of drug trades.

Low risk perceptions around being caught by police among people who use digital drug markets, particularly for buying purposes have been documented by researchers (e.g. Aldridge & Askew, 2017; Childs et al., 2022). Though people often reported concern for their digital trace data as a potential source of law enforcement risk, they often continued to perceive this as difficult for the police to access, or not a policing priority (Childs et al., 2022; Moyle et al., 2019). Although law enforcement risk appears to be of low concern to many involved in small-scale digital drug market transactions, there continues to exist considerable uncertainty and ambiguity around precisely how, where and when exposure

to law enforcement could occur. Our findings suggest that this uncertainty may in part be understood and responded to via people's established understandings and practices of navigating a broader social media landscape and its implications for personal privacy and security.

Cherbonneau and Copes (2006) have suggested that many people involved in crime base their perceptions of policing practices and priorities on partial heuristics which may not be reflective of actual policing practice. These partial heuristics are likely to be exacerbated in a social media environment, where the pathways through which people can be exposed to or watched by others are seemingly endless, and often beyond individual control (e.g. Lyon, 2018; Marwick & Boyd, 2014). The embedding of drug trading behaviors into this social media environment may then mean that people take a more *general* approach to managing the potential for digital exposure to outsiders. Among our interview sample direct experience of actual police practice was low and resulting "knowledge" was often based on anecdotal reports from others. But participants *were* highly aware of how they could be exposed through social media features such as permanent chat logs or by receiving notifications on their phone screens. This reflects the way that thinking about and managing the potential for unwanted surveillance on social media generally, translates into risk perceptions and management strategies that can be applied to drug trading (Duffy & Chan, 2019). In this sense, though participants might not have been overly concerned about exposure to law enforcement, they could easily situate police as part of their general perceptions of "imagined audience" (Litt, 2012) on social media. This more general perception of digital audience helps to explain why participants often conflated exposure to an employer, or family members with increased vulnerability to police.

Participants varied considerably in what they perceived to constitute adequate digital security for drug trading, as well as how they interpreted and prioritized platform security features. These findings can be tied to the importance of "imagined affordances" in shaping participant perceptions of vulnerability to "imagined surveillance" (Duffy & Chan, 2019). Nagy and Neff (2015) argue that people's perceptions of platform affordances are not per se "true" or "right," but rather are often the result of a process of "imagination" that encompasses user beliefs and expectations as well as direct knowledge. This helps to explain why participants tended to base their perceptions of security around consideration of a broad range of variables beyond simply platform features, for better or for worse (See also, Bakken et al., 2022). For example, participants' consideration of factors like platform ownership and past cooperation with law enforcement could sometimes *trump* the need for certain security features. Ladegaard (2018) has suggested people using darknet drug markets place their trust in "expert systems," whereby reliance on technologies the individual does not fully understand can make them oblivious to the potential for police exposure. This perspective links back to the uncertainties of both perceiving and navigating law enforcement risk in social media drug trading. Though social media and messaging platforms are by design easy-to-use, people's familiarity with them and established understandings of their features may not per se translate into more accurate perceptions of platform security (See also, Moyle et al., 2019).

On Discord drug servers for example, the more "open" nature of many drug servers meant that interview participants were primarily concerned with the "imagined affordance" (Nagy & Neff, 2015) of pseudonymity. They felt this feature both made them vulnerable to potential undercover police officers operating pseudonymously on the drug server, but also felt it insulated them from police. The resulting reliance on visual cues to decipher whether a potential transaction partner was legitimate or not bears similarities to risk management strategies documented among people involved in drug sales or other types of crime involving mandatory interactions with strangers (e.g. Holt et al., 2014; Jacobs, 1996). However, in social media drug market settings, the infrastructure through which transactions are organized is an additional parameter people need to factor into their risk management practices. Discord's pseudonymity could make participants feel secure, but digital forensics experts have in the past illustrated that the platform offers its users little data security, allowing law enforcement to easily recover a range of user data including plain-text messages and images (Moffitt et al., 2021). Hence, in this case, a focus on particular "imagined affordances" can obscure deeper issues around platform security which may have ramifications for law enforcement risk.

Many participants in this study expressed a sense of resignation about the collection of their digital trace data by social media companies, though many continued to view the likelihood that police would access this data as low risk (e.g, Childs et al., 2022). Though these perceptions may not be inaccurate in a context of small-scale drug trades and law enforcement risk, drug-related digital trace data sources may lead to broad and unexpected future repercussions as they flow into user profiles and data products social media companies sell to third-parties (Elmas, 2021; Hern, 2022). As one interviewee neatly put it: *"Facebook probably knows that I sell drugs"* (**P9**, M29, buyer/seller). Indeed, growing awareness of police use of social media data sources as part of big data policing practices (e.g. Brayne, 2017, 2020; Ferguson, 2017) may increasingly be paralleled by the potential for drug-related digital trace data to impact future opportunities across a person's life regardless of whether legal sanctions are faced. The potential for such broad impacts reflects the likelihood that these data sources will be reused and combined for different purposes by a range of actors in sectors such as advertising, employment, education and insurance (e.g. Kitchin, 2014; Zuboff, 2019). As younger age groups "grow up digital," they are increasingly likely to bear the brunt of the evolving and unpredictable ways in which their digital trace data may impact their future lives.

Limitations

Our findings are based on a non-representative sample of people who buy and sell drugs via social media and their self-report experience. Most of the participants in this study predominantly used social media to purchase small amounts

of drugs, often cannabis and MDMA, within personal and extended social networks, rather than for large-scale drug selling for profit. These sample characteristics no doubt influenced their reports of low-risk perceptions and fragmented risk management strategies. Larger-scale drug sellers are likely to have different risk perceptions related to law enforcement and more comprehensive risk management strategies. It is also likely that law enforcement agencies will be more focused on large-scale drug selling on social media rather than small quantity purchases, reflecting the very large number of small-scale trades and small legal penalties involved.

Conclusion

Our study participants using social media and messaging platforms for small-scale illegal drug trades reported low levels of concern about law enforcement risk. Yet these participants were well-versed in thinking about and responding to many of the privacy risks of online social media communication, such as data persistence and the potential for content and messages to be easily spread beyond their intended recipients. This paper suggests that an understanding of these factors may guide people involved in small-scale purchasing of illegal drugs via social media and messaging platforms, regardless of whether they perceive this risk as high. Our participants largely focused on minimizing the likelihood of exposure to law enforcement by seeking to control factors like message visibility, language, and exposure to unknown market members. They expressed resignation regarding the collection of their data by social media companies, and the potential for it to be shared with law enforcement. In this sense, people who use social media drug markets engage with these markets despite an awareness that their digital trace data may be enough to incriminate them.

The embedding of illegal drug trading within social media may have important implications for the risk of drug market involvement impacting other areas of people's lives. This is noteworthy, particularly as there is mounting evidence of policing approaches in many western countries shifting towards alternatives to punishment for minor drug offenses such as possession (e.g. Abbott, 2019; Bacon, 2022; Mannheim & Frost, 2022). The integration of digital trace and social media datasets across a growing range of sectors may mean that people who interact with social media drug markets face negative reputational consequences beyond legal repercussions and criminal records. Criminal records for minor offences such as drug possession have negative impacts on employment prospects (Uggen et al., 2014), and educational opportunities (Stewart & Uggen, 2020), compounding social and economic inequalities. However, in the future data linkages between individuals and the purchase, sale and consumption of illegal drugs may serve as invisible "proxies" for criminal involvement in the absence of an official criminal record. In this vein, drug-related digital trace data may perpetuate many of the same stigmas and harms associated with legal sanctions, shaping employment, educational and travel opportunities, housing, and insurance coverage throughout a person's life. As such, though perceptions around drug use and minor drug offenses may be softening in many western societies, it may equally be that the long-term repercussions of having a drug-linked "digital footprint," (Koops, 2011) become more invisible, far-reaching, and entrenched.

Notes

1. Discord is a social media platform which enables users to create online customizable communities, joinable via 'invite link' – known as 'servers' – which they can use to message, voice, and video call with other server members.
2. To buy and sell on a Discord server, buyers and sellers often had to 'verify' themselves to server administrators. This often referred to a process of posting a picture of drugs or drug paraphernalia, the date, and their Discord username and four-digit account tag.

Acknowledgements

We would like to thank Monica J. Barratt for providing feedback on a final draft of this paper.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was funded by a New Zealand Royal Society Marsden Grant (contract number: MFP-MAU1812)

ORCID

Chris Wilkins http://orcid.org/0000-0002-5564-6226
Marta Rychert http://orcid.org/0000-0003-4170-1615

References

Abbott, M. (2019, September 9). New law gives NZ police discretion not to prosecute drug users, but to offer addiction support instead. *The Conversation*. https://theconversation.com/new-law-gives-nz-police-discretion-not-to-prosecute-drug-users-but-to-offer-addiction-support-instead-122323

Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017, May 22-24). *Obstacles to the Adoption of Secure Communication Tools 2017 IEEE Symposium on Security and Privacy*, San Jose, CA.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3) https://doi.org/10.5210/fm.v13i3.2142

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *The International Journal on Drug Policy*, *41*, 101–109. https://doi.org/10.1016/j.drugpo.2016.10.010

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *The International Journal on Drug Policy*, *35*, 7–15. https://doi.org/10.1016/j.drugpo.2016.04.020

Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation*, *28*, 126–138. https://doi.org/10.1016/j.diin.2019.02.001

Bacon, M. (2022). Desistance from criminalisation: police culture and new directions in drugs policing. *Policing and Society*, *32*(4), 522–539. https://doi.org/10.1080/10439463.2021.1920587

Bakken, S. A. (2022). App-based textual interviews: interacting with younger generations in a digitalized social reality. *International Journal of Social Research Methodology*, *0*(0), 1–14. https://doi.org/10.1080/13645579.2022.2087351

Bakken, S. A., & Demant, J. J. (2019). Sellers' risk perceptions in public and private social media drug markets. *The International Journal on Drug Policy*, *73*, 255–262. https://doi.org/10.1016/j.drugpo.2019.03.009

Bakken, S. A., Oksanen, A., & Demant, J. (2022). Capital in illegal online drug markets: How digital capital changes the cultural environment of drug dealing. *Theoretical Criminology*, *0*(0), 136248062211433. https://doi.org/10.1177/13624806221143365

Barendregt, C., van der Poel, A., & van de Mheen, D. (2006). The rise of the mobile phone in the hard drug scene of Rotterdam. *Journal of Psychoactive Drugs*, *38*(1), 77–87. https://doi.org/10.1080/02791072.2006.10399830

Barratt, M. J. (2012). The efficacy of interviewing young drug users through online chat. *Drug and Alcohol Review*, *31*(4), 566–572. https://doi.org/10.1111/j.1465-3362.2011.00399.x

Bayer, K. (2022, 20 August). Kingpin bowled: Inside the downfall of a kiwi drug lord. *NZ Herald*. https://www.nzherald.co.nz/nz/big-read-christchurch-drug-lord-sami-zagros-and-his-dramatic-downfall/TDT6V7HXELVHWED6JC6RGWUQJM/

Boyd, d. (2007). Why youth <3 social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, Identity and Digital Media*. (pp. 119–142). The MIT Press.

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Braun, V., & Clarke, V. (2012). Thematic Analysis. In H. Cooper (Ed.), *APA Handbook of Research Methods in Psychology: Vol. 2. Research Designs*. (pp. 57–71). American Psychological Association.

Braun, V., & Clarke, V. (2022). Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, *9*(1), 3–26. https://doi.org/10.1037/qup0000196

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, *82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Brayne, S. (2020). *Predict and Surveil: Data, discretion and the future of policing*. Oxford University Press.

Brinkmann, S., & Kvale, S. (2015). *Interviews: Learning the craft of qualitative research interviewing.* (3rd ed.). SAGE.

Cherbonneau, M., & Copes, H. (2006). 'Drive it like you Stole it' auto theft and the illusion of normalcy. *The British Journal of Criminology*, *46*(2), 193–211. https://doi.org/10.1093/bjc/azi059

Childs, A., Bull, M., & Coomber, R. (2022). Beyond the dark web: Navigating the risks of cannabis supply over the surface web. *Drugs: Education, Prevention and Policy*, *29*(4), 403–414. https://doi.org/10.1080/09687637.2021.1916439

Christou, L. (2018, 30 January). What is Wickr, the new favourite app of dark net drug dealers? *Verdict*. https://www.verdict.co.uk/what-is-wickr/

Coomber, R. (2011). Using the internet for qualitative research on drug users and drug markets: the pros, cons and the progress. In J. Fountain, F. V. Asmussen, & D. J. Korf (Eds.), *Markets, methods and messages: dynamics in European drug research*. (pp. 85–103). Pabst Science Publishers.

Coomber, R., Moyle, L., & South, N. (2016). The normalisation of drug supply: The social supply of drugs as the "other side" of the history of normalisation. *Drugs: Education, Prevention and Policy*, *23*(3), 255–263. https://doi.org/10.3109/09687637.2015.1110565

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous. *Crime, Law and Social Change*, *67*(1), 55–75. https://doi.org/10.1007/s10611-016-9644-4

Demant, J., & Bakken, S. A. (2019). Technology-facilitated drug dealing via social media in the Nordic countries,background paaper commissioned for EU Drug Markets Report 2019, *European Monitoring Centre for Drugs and Drug Addiction* .

Demant, J., Bakken, S. A., Oksanen, A., & Gunnlaugsson, H. (2019). Drug dealing on Facebook, Snapchat and Instagram: A qualitative analysis of novel drug markets in the Nordic countries. *Drug and Alcohol Review*, *38*(4), 377–385. https://doi.org/10.1111/dar.12932

Diffie, W., & Landau, S. (2010). *Privacy on the line: The politics of wiretapping and encryption*. The MIT Press.

Discord. (2022). *Working with law enforcement*. Retrieved 2 August 2022 from https://discord.com/safety/360044157931-Working-with-law-enforcement

Duffy, B. E., & Chan, N. K. (2019). "You never really know who's looking": Imagined surveillance across social media platforms. *New Media & Society*, *21*(1), 119–138. https://doi.org/10.1177/1461444818791318

Egawhary, E. M. (2019). The surveillance dimensions of the use of social media by UK police forces. *Surveillance & Society*, *17*(1/2), 89–104. https://doi.org/10.24908/ss.v17i1/2.12916

Elmas, M. (2021, 17 July). Children treated like data farms by platforms like TikTok, Snapchat and Instagram, experts warn. *The New Daily*. https://thenewdaily.com.au/life/tech/2021/07/17/tiktok-instagram-data-children/

Endeley, R. E. (2018). End-to-end encryption in messaging services and national security—case of WhatsApp messenger. *Journal of Information Security*, *09*(01), 95–99. https://doi.org/10.4236/jis.2018.91008

Espiner, G. (2021, 10 November). Police try to assume people's online identities. *RNZ*. https://www.rnz.co.nz/news/national/455331/police-try-to-assume-people-s-online-identities

Fader, J. J. (2016). "Selling smarter, not harder": Life course effects on drug sellers' risk perceptions and management. *The International Journal on Drug Policy*, *36*, 120–129. https://doi.org/10.1016/j.drugpo.2016.04.011

Ferguson, A. G. (2017). *The rise of big data policing: surveillance, race, and the future of law enforcement*. New York University Press.

Forsyth, A. J. M., Barnard, M., & McKeganey, N. P. (1997). Musical preference as an indicator of adolescent drug use. *Addiction*, *92*(10), 1317–1325. https://doi.org/10.1111/j.1360-0443.1997.tb02850.x

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier.

Gibson, K. (2022). Bridging the digital divide: Reflections on using WhatsApp instant messenger interviews in youth research. *Qualitative Research in Psychology*, *19*(3), 611–631. https://doi.org/10.1080/14780887.2020.1751902

Greenberg, A. (2018, March 8). Operation Bayonet: Inside the sting that hijacked an entire dark web drug market. *Wired*. https://www.wired.com/story/hansa-dutch-police-sting-operation/

Hern, A. (2022, July 20). TechScape: suspicious of TikTok? You're not alone. *The Guardian*. https://www.theguardian.com/technology/2022/jul/20/tiktoks-privacy-problem-isnt-what-you-think

Holt, T. J., Blevins, K. R., & Kuhns, J. B. (2014). Examining diffusion and arrest avoidance practices among johns. *Crime & Delinquency*, *60*(2), 261–283. https://doi.org/10.1177/0011128709347087

Jacobs, B. A. (1996). Crack dealers and restrictive deterrence: Identifying narcs. *Criminology*, *34*(3), 409–431. https://doi.org/10.1111/j.1745-9125.1996.tb01213.x

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015, July 22-24). *"My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, Ottawa, Canada.

Kitchin, R. (2014). *The data revolution: big data, open data, data infrastructures & their consequences*. SAGE.

Koops, B.-J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice. *SCRIPTed*, *8*(3), 229–256. https://doi.org/10.2966/scrip.080311.229

Ladegaard, I. (2018). We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets. *The British Journal of Criminology*, *58*(2), 414–433. https://doi.org/10.1093/bjc/azx021

Ladegaard, I. (2020). Open secrecy: How police crackdowns and creative problem-solving brought illegal markets out of the shadows. *Social Forces*, *99*(2), 532–559. https://doi.org/10.1093/sf/soz140

Levin, S. (2021, September 8). Revealed: LAPD officers told to collect social media data on every civilian they stop. *The Guardian*. https://www.theguardian.com/us-news/2021/sep/08/revealed-los-angeles-police-officers-gathering-social-media?CMP=Share_iOSApp_Other

Litt, E. (2012). Knock, knock. Who's there? The imagined audience. *Journal of Broadcasting & Electronic Media*, *56*(3), 330–345. https://doi.org/10.1080/08838151.2012.705195

Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. *Social. Media + Society*, *2*(1), 205630511663348. https://doi.org/10.1177/2056305116633482

Lyon, D. (2017). Surveillance culture: engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, *11*, 824–842.

Lyon, D. (2018). *The Culture of Surveillance: Watching As a Way of Life*. Polity Press.

Mannheim, M., & Frost, H. (2022, 9 June). ACT government agrees to decriminalise small amounts of illicit drugs, such as ice, heroin and cocaine. *ABC News*. https://www.abc.net.au/news/2022-06-09/small-amounts-of-illicit-drugs-to-be-decriminalised-in-canberra/101139060

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Mayer-Schönberger, V. (2011). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.

McCay-Peet, L., & Quan-Haase, A. (2016). What is social media and what questions can social media research help us answer?. In L. Sloan & A. Quan-Haase (Eds.), *The SAGE Handbook of Social Media Research Methods*. (pp. 13–26). SAGE.

Meta. (2022a). Further asked questions: Our data disclosure process. Retrieved 18 October 2022 from https://transparency.fb.com/data/government-data-requests/further-asked-questions

Meta. (2022b). Government requests for user data: Global overview. Retrieved 29 September 2022 from https://transparency.fb.com/data/government-data-requests/

Meta. (2022c). Government requests for user data: New Zealand. Retrieved 29 September 2022 from https://transparency.fb.com/data/government-data-requests/country/NZ/

Meta. (2022d). Information for law enforcement authorities. Retrieved 2 August 2022 from https://www.facebook.com/safety/groups/law/guidelines

Ministry Of Health. (2022). New Zealand Health Survey 2021/22: Annual data explorer. Retrieved 12 January 2023 from https://minhealthnz.shinyapps.io/nz-health-survey-2021-22-annual-data-explorer/_w_e3667d6e/#!/explore-indicators

Moeller, K., Copes, H., & Hochstetler, A. (2016). Advancing restrictive deterrence: A qualitative meta-synthesis. *Journal of Criminal Justice*, *46*, 82–93. https://doi.org/10.1016/j.jcrimjus.2016.03.004

Moffitt, K., Karabiyik, U., Hutchinson, S., & Yoon, Y. H. (2021). *Discord Forensics: The Logs Keep Growing 2021 Ieee 11th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV. https://doi.org/10.1109/CCWC51732.2021.9376133

Morrison, S. (2021, 31 July). Here's how police can get your data - even if you aren't suspected of a crime (and you may never know they did it). *Vox*. https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *The International Journal on Drug Policy*, *63*, 101–110. https://doi.org/10.1016/j.drugpo.2018.08.005

Nagy, P., & Neff, G. (2015). Imagined affordance: Reconstructing a keyword for communication theory. *Social Media + Society*, *1*(2), 205630511560338. https://doi.org/10.1177/2056305115603385

Newell, B. C., & Tennis, J. (2014, 4–7 March). *Me, my Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs Proceedings of the 2014 iConference*, Berlin, Germany.

Oksanen, A., Miller, B. L., Savolainen, I., Sirola, A., Demant, J., Kaakinen, M., & Zych, I. (2021). Social media and access to drugs online: a nation-wide study in the United States and Spain among adolescents and young adults. *The European Journal of Psychology Applied to Legal Context*, *13*(1), 29–36. https://doi.org/10.5093/ejpalc2021a5

Parkin, S. (2021, 11 September). 'Every message was copied to the police': the inside story of the most daring surveillance sting in history. *The Guardian*. https://www.theguardian.com/australia-news/2021/sep/11/inside-story-most-daring-surveillance-sting-in-history?CMP=Share_iOSApp_Other

Perez, B., Musolesi, M., & Stringhini, G. (2018, June 25–28) *You are your metadata: Identification and obfuscation of social media users using metadata information*. Twelfth International AAAI Conference on Web and Social Media.

Robertson, K. J., & Tustin, K. (2020). Control of recreational cannabis in a New Zealand university sample: perceptions of informal and formal controls. *Substance Abuse: research and Treatment*, *14*, 1178221820953397. https://doi.org/10.1177/1178221820953397

Sarre, R. (2017). Metadata retention as a means of combatting terrorism and organised crime: a perspective from Australia. *Asian Journal of Criminology*, *12*(3), 167–179. https://doi.org/10.1007/s11417-017-9256-7

Savage, J. (2022, 4 December). 'Back in the game' - inside the police investigation that brought down Comanchero gang boss. *NZ Herald*. https://www.nzherald.co.nz/nz/back-in-the-game-inside-the-police-investigation-that-brought-down-comanchero-gang-boss/SILKXRY5NBCJBKQSOAS7BETJPU/

Silva, K. (2015, August 11). Queensland drug dealers using messaging app Wickr. *Brisbane Times*. https://www.brisbanetimes.com.au/national/queensland/queensland-drug-dealers-using-messaging-app-wickr-20150811-giwn5o.html

Snap Inc. (2020). Law enforcement guide. Retrieved 2 August 2022 from https://support.snapchat.com/en-US/article/law-snapchat

Soudijn, M. R., Vermeulen, I. J., & van der Leest, W. P. (2022). When encryption fails: a glimpse behind the curtain of synthetic drug trafficking networks. *Global Crime*, *23*(2), 216–239. https://doi.org/10.1080/17440572.2022.2086125

Stewart, R., & Uggen, C. (2020). Criminal records and college admissions: A modified experimental audit. *Criminology*, *58*(1), 156–188. https://doi.org/10.1111/1745-9125.12229

Swift, M. (2022, 27 October). Police bust huge online drug operation using Facebook to sell illegal substances in Otago. *Newshub*. https://www.newshub.co.nz/home/new-zealand/2022/10/police-bust-huge-online-drug-operation-using-facebook-to-sell-illegal-substances-in-otago.html

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670. https://doi.org/10.2307/2089195

Trottier, D. (2012). *Social Media as Surveillance: Rethinking visibility in a converging world*. Routledge.

Uggen, C., Vuolo, M., Lageson, S., Ruhland, E., & Whitham, H. K. (2014). The edge of stigma: An experimental audit of the effects of low-level criminal records on employment. *Criminology*, *52*(4), 627–654. https://doi.org/10.1111/1745-9125.12051

van der Sanden, R., Wilkins, C., Romeo, J. S., Rychert, M., & Barratt, M. J. (2021). Predictors of using social media to purchase drugs in New Zealand: Findings from a large-scale online survey. *The International Journal on Drug Policy*, *98*, 103430. https://doi.org/10.1016/j.drugpo.2021.103430

van der Sanden, R., Wilkins, C., Rychert, M., & Barratt, M. J. (2022a). 'Choice' of social media platform or encrypted messaging app to buy and sell illegal drugs. *The International Journal on Drug Policy*, *108*, 103819. https://doi.org/10.1016/j.drugpo.2022.103819

van der Sanden, R., Wilkins, C., Rychert, M., & Barratt, M. J. (2022b). The use of discord servers to buy and sell drugs. *Contemporary Drug Problems*, *49*(4), 453–477. https://doi.org/10.1177/00914509221095279

VanNostrand, L.-M., & Tewksbury, R. (1999). The motives and mechanics of operating an illegal drug enterprise. *Deviant Behavior*, *20*(1), 57–83. https://doi.org/10.1080/016396299266597

Versus. (2022). Messaging app comparison. Retrieved 4 August 2022 from https://versus.com/en/messaging-app

Walsh, J. P., & O'Connor, C. (2019). Social media and policing: A review of recent research. *Sociology Compass*, *13*(1), e12648. https://doi.org/10.1111/soc4.12648

Watters, J. K., & Biernacki, P. (1989). Targeted sampling: Options for the study of hidden populations. *Social Problems*, *36*(4), 416–430. https://doi.org/10.1525/sp.1989.36.4.03a00070

Wilkins, C., Prasad, J., Romeo, J., & Rychert, M. (2017). *Recent trends in illegal drug use in New Zealand, 2006-2016*. Massey University.

Wilkins, C., Prasad, J., Rychert, M., Romeo, J. S., & Graydon-Guy, T. (2018, March). *Which regions reported higher levels of methamphetamine and cannabis dependency and need for help with substance use problems?* [Media Release]. https://shoreandwhariki.ac.nz/

Wilkins, C., Romeo, J. S., Rychert, M., Prasad, J., & Graydon-Guy, T. (2018). Determinants of high availability of methamphetamine, cannabis, LSD and ecstasy in New Zealand: Are drug dealers promoting methamphetamine rather than cannabis? *The International Journal on Drug Policy*, *61*, 15–22. https://doi.org/10.1016/j.drugpo.2018.09.007

Williams, G. (2023, 31 January) First two sentenced in drug bust. *Otago Daily Times*, https://www.odt.co.nz/regions/queenstown/first-two-sentenced-drug-bust

Williams, M. (2022). *Secure Messaging Apps Comparison*. Retrieved 4 August 2022 from https://www.securemessagingapps.com

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power*. Profile Books.