Crime, Law and Social Change
https://doi.org/10.1007/s10611-024-10168-4

Countering surveillance: using actor-network theory to understand how organised crime is displaced and harms arise as offenders become invisible to the gaze of electronic monitoring and law enforcement

Carl R. Berry[1] · **Mark A. Berry**[2]

Accepted: 22 August 2024

Abstract

The intensification of surveillance is claimed to have created a new era of crime control, which renders visible, activities that were once beyond the purview of justice agencies. Nevertheless, little data has been gathered concerning how offenders within organised crime groups navigate this optically penetrated terrain to become invisible and continue their illegal pursuits. This article compares ethnographic findings from two separate investigations: of offenders subject to the surveillant penalty of Electronic Monitoring and organised criminals under the investigative observation of law enforcement. It shows how organised offending becomes displaced and worse harms arise as they deploy counter-surveillance strategies, despite facing increased odds of detection. These findings are theorised through actor-network theory, an approach which asserts that objects have agency and can achieve/frustrate socio-technical goals, to highlight how surveillance becomes negotiable for organised offenders.

Keywords Organised crime · Electronic monitoring · Surveillance · Actor-network theory · Ethnography · Technology · Probation · Criminal justice · Law enforcement · Narcotics · Sex work

✉ Carl R. Berry
Carl2.Berry@uwe.ac.uk

Mark A. Berry
mberry@bournemouth.ac.uk

[1] Faculty of Health and Applied Sciences, University of the West of England, Bristol, UK

[2] Department of Social Science and Social Work, Bournemouth University, Bournemouth, UK

Published online: 20 September 2024

Introduction

That crime and punishment are at the boundaries of significant change, is an idea that is increasingly discussed in criminology. A 'Fourth Industrial Revolution' has, allegedly, begun and technological transformations have opened new concerns for lawmakers and lawbreakers alike (McGuire, 2012). Related especially to the evolution of Information Communication Technology, new techniques of surveillance have prompted much debate as they become integral to contemporary governance (Schuilenburg, 2015). These observational systems have also opened criminal opportunities: various types of cybercrime and online exploitation have become commonplace while traditional crimes take advantage of diverse surveillant technologies (McGuire, 2012). Rising to meet these challenges, new means of prevention and detection have emerged as crime control agencies try to cope with offences. These advancements often conjure dystopian imaginaries that portend new forms of control, which are fine-grained, decentralised and centred on risk prevention (Haggerty & Ericson, 2000; Zedner, 2007). Although the benevolent impacts of surveillance are noted in areas like public-health (Schuilenburg, 2015), how activities that were once unseen today become visible, raises much concern.

At the forefront of this trend, techno-correctional devices, like electronic-monitoring (EM), that use surveillance have become staple tools of justice agencies. EM enables curfews that restrict offenders to an address for fixed time-periods; following court sentencing, users will have a bracelet (or tag) fixed on their ankle that remotely connects to a monitoring unit installed in their home using radio-frequency technology, which, itself, connects to a remote monitoring station (Nellis, 2013). This 'socio-technical system' (Lianos & Douglas, 2000) is intended to visibilise their whereabouts and incapacitate them. Despite sparking concerns about new Orwellian forms of class control (Gacek, 2022), EM is, contrastingly, criticised for users continuing criminal activity, whilst sometimes helping to deter offending due to a perceived increased chance of detection (Hucklesby, 2013). Recent developments of GPS tracking and alcohol monitoring indicate more intensive types of monitoring alongside future incarnations potentially employing biometric chips, AI monitoring and even electric shocks (Nellis, 2019).

Digitised state surveillance has also made the pursuit of criminal gains through organised means increasingly risky, as offenders are forced to navigate a variety of investigative device-systems used by law enforcement (Berry, 2018). Here, mobile police 'webs' that redirect data from mobile phone communications, drones, the monitoring of online activity and passive CCTV systems have been mobilised to detect various offences. Nevertheless, this research on organised crime has indicated several techniques offenders use to circumvent enhanced detection, besides capitalising on new online markets for illegal goods/services. Monitoring technology has become especially central in street drug markets as various technologies spanning manufacture, communication and distribution require criminal innovators to diversify enterprises to reduce risk and maximise sales. Although EM uses overt surveillance to control spatial-temporality and organised crime groups must navigate covert/semi-covert monitoring (Marx, 1988), the disruption and detection of offending are central features of both regimes. This article demonstrates that comparable strategies

are employed by active offenders subject to them: they must manage risks and due to EM's common usage, organised criminals may have also encountered it.

Although discussion exists about techniques to neutralise surveillance (Marx, 2003), first-hand data on how offenders achieve this to continue illicit gains is rare and requires serious criminological consideration, prompting the following research questions in this article:

1. How do organised crime groups avoid visibility from state surveillance?
2. How does surveillance displace organised crime?
3. What harm arises as organised crime is displaced/invisibilised?

This article explores several criminal actors who achieve this by taking data from two separate ethnographies: firstly, of EM users who offend in an organised manner; and secondly, active organised criminals yet to be caught for current crimes but who negotiate broader police surveillance and intelligence gathering. It shows how both similarly thwart detection systems/manipulate them for new opportunities.

Surveillance and displacement

Deluzian thinkers critically discuss how new observational techniques tighten social control (Haggerty & Ericson, 2000). Contrastingly, Ekblom's (2017) concept of evolutionary criminal adaptation sees these measures as necessary to tackle offending. This article uses Bruno Latour's perspective of actor-network theory (ANT) (2005), to, instead, understand criminal activity that challenges both positions: it shows how through the continued illicit enterprises of offenders, 'regimes of surveillance' are resisted yet why attempts at criminalisation fail. Criminologists have, indeed, demonstrated how reactive crime control measures often *displace crime*, when offenders innovate new offences, change offending patterns or move into more serious offences (Guerette, 2009).[1] ANT avoids pre-drawn explanations and urges researchers to ethnographically 'follow the work of related actors' (including non-humans) in achieving governance but emphasises how they often fall short. Accordingly, it is well-placed to understand how problem-orientated justice policy fails; nonetheless, ANT is rarely applied directly to offenders and faces criticism. This article considers its strengths by examining how active offenders on EM and organised criminal groups deploy similar strategies to negotiate, resist and exploit surveillant device-systems, resulting in displaced offending. It demonstrates that forms of counter-surveillance emerge from the re-deployable nature of surveillance technologies, criminogenic associations and opportunities afforded within offenders' extended socio-technical networks, which crime control approaches cannot defeat. Furthermore, it highlights that justice policy

[1] Displacement is discussed in more detail in this work, besides its contra-process 'diffusion' (Guerette, 2009).

can create serious social harm for victims, the community and offenders as they fail (Tombs, 2018).[2]

In-depth accounts from the two ethnographies are compared in this article, using a dual tripartite framework. (1), *manipulation/redeployment*, refers to how offenders exploit limitations within surveillant systems to invisibilise their actions while sometimes re-using device-systems to further criminal agendas; (2) *deceiving/distracting*, describes the tactics used to fool watchers by appearing compliant/diverting attention away from criminal pursuits; (3), *disappearing/blocking* relates to how targets of observational systems disappear from view or use device-systems to shield their operations. Notably, this framework is not discreet and several tactics may be used within organised crime groups (see below). It is applied to EM users living under a regime of penal surveillance and organised crime groups operating within a regime of surveillant investigation; each section of the analysis compares an in-depth offender narrative from both studies.

Theorising observation, technology and crime

Deleuze's (1992) work on surveillance advances Foucault's later theories on control (1984). Recent uses of this perspective, however, claim that current observational tools allow for levels of connectivity which far exceed previous eras. For Deleuze, regulation is no longer achieved through disciplining individual subjects. Alternatively, behaviour is shaped through surveillant systems (like identity documents (IDs), CCTV and EM tagging) that monitor abstracted data flows (Haggerty & Ericson, 2000). By rendering visible that which once went unseen, activities are made knowable to the various agencies responsible for this, who are now invisible themselves. Hiding their practices, they, allegedly, function at a 'molecular-level' within 'assemblages' of loosely connected nodes rather than static centralised arrangements (Hui, 2014).

Although often accurately conceptualising the decentred nature of contemporary surveillance, similar top-down interpretations of Deleuze are criticised for forgetting his emphasis on resistance and failures in governance (Berry, 2019). Other thinkers consider how new devices democratise the ability to watch (Lyon, 2007); indeed, Foucault's claim that 'power defines itself through resistance', was also central to Deleuze (Rao et al. ,2015). In this vein, work that discusses how invisibility is achieved despite intensifying observation has contemplated counter-surveillance strategies from those being monitored. Marx (2003) classifies several moves: '*discovery*, *avoidance*, *piggybacking*, *switching*, *distorting*, *blocking*, *masking*, *breaking*, *refusal*, *cooperative and counter-surveillance'*, which emerge as the watched resist their watchers. Still, this important work is isolated and less concerned about crime or its causes.

Contrastingly, the concept of a 'technological arms race' between criminals and justice agencies is forward by Ekblom when discussing new technologies that

[2] Harms-based approaches like zemiology make several important theoretical claims for criminology concerning how current crime control approaches fail; they are used here, briefly, to critique current responses.

monitor. Ekblom (2017) explains how strategies of 'evolutionary adaptation' arise between these competing forces and angles toward reducing displacement. In this rational-choice perspective, new device-systems develop when previous 'design-scripts' break e.g., when offenders innovate ways to defeat CCTV. However, Ekblom has been challenged for implicitly adopting the perspective of authorities, under-theorising how complex sets of extended relations lead to criminal adaptations and how devices shape outcomes (Berry, 2018).

ANT tries to understand how socio-technical systems function through the activity of connected human and non-human actors, from the 'bottom up. Consequently, it has advantages for investigating how the objects of control (i.e., offenders) defeat surveillance, besides these circumstances. Asserting that constant work is needed for networks to function correctly, for Latour, components must *translate* their objectives into action, which is far from given. He uses the concept of the 'oligoptigon' to describe how contemporary surveillant tools achieve this through multiple controllers that monitor many small areas with great precision. By 'constructing the realities they watch', multiple local realities subsequently arise for allied actors (2005).

Further arguing that 'technologies make society durable', ANT sees non-human actors as equal to humans in constructing social associations: technological devices are said to allow the 'folding' of time/space by physically coupling the past, present and future (as in buildings, computers or surveillant equipment) (Latour, 2005). Still, despite objects executing their 'design-scripts' more reliably than people, their 'fluidity' is emphasised -surveillant devices may fail to visibilise targets. As offending becomes more technologically dependent, ANT may help to understand criminal displacement by emphasising the reusability of devices/platforms and the abundance of offending opportunities within technologically mediated organised crime networks. By not privileging humans over non-humans (or vice versa), it better explains criminal innovation than Ekblom; technological fluidity allows device-systems to become repurposed despite their objectives of disrupting crime.

Though, gathering increasing prominence, ANT faces notable criticisms. It has been pulled up for, allegedly, under-appreciating patterns of social exclusion, leaning toward voluntarism and sometimes taking a 'managerial position' (Vandenberghe, 2002). Research on EM users, however, uses ANT to show how surveillance acquires 'tangible qualities' that are *physically felt* by this marginalised group, leading to contrasting experiences and offending outcomes (Berry, 2019). Its ideas are also used in studies on organised crime to show how technological know-how allows surveillance technologies to be deceived (Berry, 2018). Still, various social harms may arise as crime becomes displaced within these networks. ANT has explored victimisation (Van Der Wagen & Pieters, 2018) but could be expanded to understand how it occurs as offending is concealed.

This article considers these ideas to understand how offenders overcome risks created by surveillant technologies designed to show them to the criminal justice system. We argue that as offenders subject to the penalty of EM and organised criminals avoid detection from law enforcement, forms of counter-surveillance that displace crime and create new harms emerge. Much criminological theory is concerned with identifying the causes of crime or determining sanction effectiveness (Young, 2011). ANT uses a more neutral approach that simply *describes* how outcomes arise from

interconnected activities (Latour, 2005). Given the centrality of technology in this article, ANT is well-suited to capture these interactions and will be advanced by applying it to an unexplored area.

Counter-surveillance is shown to emerge from: (1), how gaps within the technical-systems of the CJS allow for negotiation; (2), how technologies are used by criminals to innovate new practices and exploit surveillant systems; (3), how embeddedness within wider assemblages of criminogenic practices/circumstances lead to continued offending. It is accepted that continued offending despite sanctioning and detection is hardly new and that counter-surveillance is not always 'hi-tech'; nevertheless, these activities are shown to be thoroughly mediated by new monitoring capabilities.

Methods

ANT's ethnographic approach advocates 'following key actors' (including non-humans) to uncover how they expedite socio-technical systems. From a constructivist perspective, it compels researchers to merely record this activity while outlining influencing factors (Latour, 2005). It further attempts to understand how research settings lead to particular performances from actors (including influences from researchers and recording equipment), and how investigators sometimes -unwittingly- assist network maintenance (Law, 2004). Accordingly, when/how the authors temporarily became part of their respective surveillant networks is noted in this article.

The data comes from two separate doctoral investigations undertaken between 2014 and 2020 within a major city in England. One study is an ethnography on EM users that interviewed and observed 21 participants serving various sentences and bail orders; they were gathered through purposive sampling by visiting the local magistrates' court and convenience/snowball sampling from acquaintances currently serving EM sentences. It discovered that despite many reducing criminal activity due to its surveillant capacities, some continued seriously offending. The other study is an ethnography on illicit drug distribution, conducted on 26 criminals from local dealers to international traffickers who were gathered through convenience/snowball sampling from personal networks; it investigated offline/online drug markets, risk management, recruitment pathways and emergent technologies.

For this chapter, the data was re-analysed for similar cases and the comparative framework was developed through a process whereby repeating patterns were coded into the overarching themes: *(1) manipulation/redeployment*, *(2) deceiving/distracting*, *and (3) disappearing/blocking*. These themes were generated adaptively through a detailed examination of the data and relevant theoretical ideas (Braun & Clarke, 2014; Layder, 1998). The first study selected cases that most closely fit the definition of organised crime; from the second, cases related to surveillance and technology. This cross-section allows for comparisons into how serious offenders on EM and tech-savvy organised crime groups become invisible, using similar strategies.[3]

[3] Offenders on tag were, arguably, subject to more monitoring and mitigated this besides potential police surveillance; nonetheless, both samples indicated very similar temporospatial adaptations, shown below.

This methodological strategy, nevertheless, raises epistemological issues: ANT ethnographies construct highly particular accounts of socio-technical phenomena, thus, problematising comparisons of data (Law, 2004). Rather than developing generalisable claims from this research, this article addresses the issues found within rational choice and critical surveillance theories. It deploys relevant ANT concepts concerning how organised activity is facilitated by technologies to understand how criminals negotiate surveillance in appropriate cases. Given how the studies were conducted in the same city during the same timeframe and had overlapping aims/objectives, comparing data from both is also felt justifiable notwithstanding some context-dependent factors sometimes influencing the findings, which are reflexively acknowledged.[4]

Manipulation/Redeployment

In our era of ubiquitous surveillance, committed offenders may overcome risks by finding gaps within monitoring systems or repurposing technologies to continue generating illicit revenue. The following section, '*manipulation/redeployment'*, refers to how offenders exploit limitations within surveillant systems to invisibilise their activities and how device-systems can unintentionally advance criminal goals. It compares the cases of Idris who was serving his EM sentence in the community and Liam who provided private security for the owners of a chain of illegal brothels. Both cases demonstrate how criminal enterprises circumvent and appropriate surveillant technologies.

Idris

Idris was on a stand-alone EM sentence for common assault following a fight outside a nightclub related to his enforcement activities (selling narcotics). This observation highlights Idris' continued criminal activity:

I walk into my local barber and Idris is sitting in the chair smiling. The establishment attracts well-known tough guys and figures from EM City's underworld; Idris is one such character. He's in his late 20s, *heads a street-level cocaine distribution outfit and has a reputation for extreme violence*, *however*, *surprisingly*, *has only a couple of minor convictions for assault. He often uses runners for his dirty work and talks openly about his recent activities amongst the clientele*, *appearing unconcerned about his tag*, *visible around his ankle.*

Idris: 'So there I am, in broad daylight chasin' this cunt down Bridge Hill high street with a baseball bat in me hand ana' tag swingin' round' me fuckin' ankle… It was a bit silly now really thinking about it (laughs).'

[4] Per ANT, these accounts are treated as location and spatially dependent performances that emerge as offenders, researcher, equipment and setting interact (Law, 2004). Furthermore, although the outcomes of object-human interactions are variable, Latour acknowledges how design objectives often direct technological usage, becoming 'black boxed' (see below).

Despite being under the surveillant gaze of EM, Idris' testimony illustrates how organised crime groups negotiate socio-technical systems deployed by the state to observe and control crime. While seriously offending, Idris' technologically mediated curfew required him to adjust his operations to avoid becoming visible to the authorities and he moved his enforcement activities (described in the assault above) to daytime hours, whilst relying upon his network of criminal associates for distribution during the evening. This, however, created different risks; the odds of arrest increased due to more witnesses being present during the daytime, yet there were lower chances of being caught selling narcotics as random police stops were less likely. Idris even seemed to benefit from his ankle bracelet boosting his reputation, which he temporarily posted on social media.

Still, Idris further explained that integrating into the EM network had disrupted his operations unanticipatedly by allowing other criminals to manipulate his temporal-spatial movements. Indeed, he believed that the person he attacked (who was a former associate) had informed the police about the supply of cocaine coming from an alternative address Idris' organised crime group used because of his restrictions. He was, subsequently, arrested under suspicion of possession with the intent to supply narcotics but, ironically, was released without charge after the police raided the address at the wrong time. He was entirely exonerated when the digital timestamp from his equipment created an unintentional digital alibi, which showed him in his own home during his alleged time in their stash house. Claiming to have seen the informant's name on a statement after interrogation, he decided to: '*pay him a visit'.* The quote above shows how worse harm arose as his offending was temporally displaced; nevertheless, the observation below highlights how Idris' EM regime sometimes took a different life:

We leave and walk across the street to a café. The place begins to fill up with parents and young children, *leading Idris to markedly change from his earlier braggadocios. He looks around suspiciously and covers his tag when we sit in the corner*, *then drops his voice with the appearance of the recorder.*

Although Idris' EM equipment was intended to control his movements, his behaviour in a different setting suggests it acquired multiple roles (despite not preventing his offending). In contrast to his earlier swaggering performance, during this part of the meeting, Idris explained that he also hid the ankle bracelet from his mother who was unaware of his criminal activity, creating an intensely negative emotional state as it became difficult to visit her as she cared for his sick brother. Notwithstanding boastfully sharing pictures of himself at court during a breach hearing, around other parents, Idris spoke about his worsening depression and reliance on cocaine: visiting his newborn daughter who lived across the country risked seriously violating his curfew. Paradoxically, his surveillant regime acquired a punitive quality yet galvanised his nefarious operations. Very aware he was unlikely to face harsher sanctioning for his many minor breaches, Idris became increasingly nihilistic and violent in the period. The rest of this section examines the case of Liam, who provided private security in the sex trade:

Liam

Liam was in his early 30s and had a criminal record for assaulting a police officer.[5] Sometime after, he got a job providing private security for a family firm that owned a chain of illegal brothels. Below, he explains how commercially available surveillant tools may be repurposed by criminals to protect/extort businesses:

Liam is currently staying between several brothels and is working as a minder for the establishments, which operate low-profile. Due to their secret nature, I'm unable to observe his work; we chat on the phone while he sits monitoring the CCTV system for signs of trouble (including the police) as the workers conduct their business in different rooms. He's concerned about talking too long because the pimp of the establishment -who he describes as an 'annoying little prick'- moans if he uses his phone and Liam believes secret cameras are spying on him.

Mark: 'So did you have any issues looking after the house, were there any incidents?'

> Liam: 'Yeah there was a drone flying above the house, which to me meant people were looking at the house to see if they had money there. Like they're gonna be parked in a car around the corner, or they're gonna see if there are security here to break in. I found out that the drone belonged to one of the stepson's 'friends…'.
> Mark: 'Sure?'
> Liam: 'The guy doing the security beforehand… he was like… heating up the situation and scaring 'em, said he had information that some people were gonna rob 'em.'
> Mark: 'Oh… right?'
> Liam: '…Anyway, the police came and they found a car full of people, balaclavas and baseball bats just around the corner… they were obviously gonna come in and try and rob them. But… it could've been this bloke was setting things up… because these people in their house were scared, they were cash cows for him…'.
> Mark: 'Ah, he was getting a lot of money for it?' (protection services).
> Liam: 'Cash money, yeah. So it served him to have those people shit scared.'
> Mark: 'So you think that maybe it was some of the thugs he knew that were flying the drone maybe?'
> Liam: 'I know it was thugs, some local drug dealer.'

Liam's testimony shows how organised crime groups can craftily redeploy law enforcement technologies that visibilise targets. Brought in to protect the illegal enterprise after the former security provider was removed because he was extorting it, Liam's candid description shows how the insertion of the drone was intended to disrupt its operations (creating a demand for protection without the victims initially knowing who was responsible). Besides paying extra money, it became necessary to augment the security of the setting with further surveillance: CCTV and intercom to

[5] For which he received a suspended sentence with EM.

check the identity of customers who were required to book appointments and be vetted. In worst-case scenarios, the locations could be switched.[6]

When further discussing how it became necessary to thwart predatory voyeurs, Liam's account indicates how the risk calculus of the prostitution network was remodelled while these factions competed. Ultimately, Liam's physical presence and significant reputation had allowed the re-invisibilisation of the location and he surmised that the previous security guard – who was well connected with other crooks– paid someone to fly the drone, fabricating fear of a police raid or robbery while minimising suspicion on himself.

Liam's account further shows how the battle for control over the profitable business also led victims to emerge. Although, in an unanticipated manner initially (namely, the pimp who was exploiting his workers), it was the workers who held the least control while being financially and physically coerced. Consequently, Liam highlighted how, with the enterprise becoming mediated by surveillant technology, patterns of exploitation intensified. As 'lucrative investments', the workers were fought over by competing unscrupulous actors and Liam muscled out the former security provider, setting a fairer price for his services as the drone attacks stopped. Ironically, though, Liam was fired shortly after when deemed no longer necessary.

Deceiving/Distracting

When offenders are directly under state surveillance (e.g., EM), maintaining law-abiding appearances is vital to continue operations undetected. As another layer of security, criminals can employ misdirection so the police observe the wrong locations during investigations. The following section, '*deceiving/distracting'*, discusses how members of organised crime groups mislead watchers by acting compliant/diverting attention. It compares the case of Vince who is on EM for cloning cars and a career criminal called Teeth who distributes Class-A drugs:

Vince

Vince is in his early 30s and shortly released from prison with EM alongside probation requirements; he has convictions for handling stolen goods (cloned cars), credit card fraud and possession with intent to supply narcotics (cocaine and mephedrone). He was required to counter his surveillant restrictions by sneakily distributing narcotics into jail while complying with his parole conditions:

Vince: 'I mean I'm pretty much clean, only thing I got goin' is this little letter thing.'

> Carl: 'What's that?'
> Vince: 'Get this… basically I found a way using Sect. 39 solicitor correspondence to get spice into my mates… Sect. 39 is official case letters, the screws ain't allowed to open them. What I do, is I make up the letter, make it look real. Got

[6] Liam claimed that many clients were off-duty police officers, plausibly providing the enterprise with some protection from raids.

> my own emblem and made up the solicitor's name and address and everything (laughs), identical to the ones I got when I was in… Printed them off a computer, dipped them in synthetic liquid spice… then I send it… Last time I quadruple dipped and got half the wing hospitalised (laughs). My stuff is the dogs bollox. The screws don't have a fucking clue… I get seven hundred notes of one and it costs me less than a tenner to make.'

Vince was surveilled through several well-connected criminal justice agencies and on a tight regime of EM, which carried a strong chance of prison recall if he violated his curfew.[7] Although his temporal-spatial behaviour was visible, Vince deceived his observers by switching offence type, demonstrating how state surveillance has significant limitations despite its pervasiveness. By appearing compliant with his parole conditions, Vince's testimony highlights how mainly relying on EM location data to manage offending is easily exploitable. Coordinating with contacts still behind bars, Vince expressed acute awareness of these weaknesses as he invisibilised his nefarious activities. Indeed, he innocently played along, knowing that his watchers were simply looking in the wrong places: '*Mate you just gotta know how to play it*, *show them what they want and they'll back off from ya'*.

Vince's story also reveals how indigent circumstances prompted his counter-surveillance. Indeed, due to his strict curfew requirements and impoverished situation, criminogenic factors that necessitated minimal temporal-spatial movement had arisen; even minor breaches could see him jailed, which was likely if he became gainfully employed in his qualified trade or mobile for street-level narcotic distribution (like Idris). Furthermore, unlike other participants in this article -who had flashy apartments, clothes, cars and cash- Vince was desperate to attain basic items but left prison with nothing and had poor relations with his family. Thus, aware of the reliability of the EM equipment to detect violations and that the monitoring company maintained good communication with Probation, Vince deceived his observers by innovating new crimes committed from his mother's basement that reduced risk and avoided visibility. Vince's account also illustrates how worse harm occurred as his offending was displaced to spice distribution, wreaking havoc in his previous jail. The remainder of the section examines Teeth; a highly-intelligent criminal with a brutal reputation:

Teeth

Teeth is a hardened career criminal in his mid-40s and sells heroin and crack cocaine but started as a professional car thief in his youth. He has been involved in various crimes over many years, from professional theft to credit card fraud, interspersed with remorseless violence. Eventually caught for distributing narcotics, he served a lengthy prison sentence but has continued cautiously since.[8]

[7] The threshold for violating electronic monitoring as early release is much lower than a community sentence.

[8] Teeth also got early release from custody with EM parole for this.

Nearing midnight, Teeth takes me and his drug runner to give insights into his work. We stop at a pool-club in the city-centre and find a secluded spot; he sends 'Hector' to get drinks while we talk about technology:

Mark: 'Can you tell me a bit about the tech, I remember seeing you using the police scanner before, how'd you get the radio frequency?'

> Teeth: 'It was different back then. This was when the police were using analogue radios. Now it's all digital so you can't do it. We used CB radios, you'd leave 'em on scan and they'd find the police frequency. Police would change the frequencies all the time, so this was the only way to do it. But scanners didn't play a big part in the drugs… we used them mainly for stealing cars. So, when we were doing a job, we'd leave 'em scanning and when the police come into the area, we pick 'em up. I'd have someone on lookout and if he heard any reports for cars coming to the address we was at, we'd know about it. The police didn't know we had scanners, so… we'd get on the phone and tell 'em we've seen this big black bloke beating the shit out of this poor white lady a few blocks up. Make it sound really bad. Soon as they heard, they get diverted and it gives us time to finish the job…'.

Discussing his previous exploits in car theft, Teeth's testimony illuminates how device-systems relied on by law enforcement can be exploited to distract their users. Specifically, Teeth detailed how he became invisible as he monitored his observers' radio communications, intercepting them and throwing officers off the trail by diverting emergency services to concocted offences. He also highlighted how his knowledge of police work allowed successful counter-surveillance strategies; he predicted how the prioritisation of resources alongside racial and gendered prejudices would inform their responses. The observation below demonstrates how Teeth continued to anticipate police monitoring and stay undetected while moving into drug distribution.

We get into to Teeth's car. Inside, he pulls out a small device and waves it around the interior. Later he explains his actions:

Mark: 'So, what were you doing with that thing you used?'

> Teeth: 'Oh that? I've just got a little RF [radio frequency] scanner I sweep over it. These listening devices let off a radio signal and you can tune into 'em. It don't always work… These days they use a little memory chip. They stick it in your car leave it recording an' take it out another time and listen through it.'

We drive out of the city centre toward the suburbs, Teeth's drug runner looks out and continually watches the environment for police activity. Although the two make a game of it, Hector is expected to perform and there is a clear chain of command. From earlier conversations, I get the impression that Teeth is keen to show his criminal proficiency and arranges several drug deals in my presence. I steer the conversation towards mobile phones; he informs me of a contact who can change their IMEI numbers, so they can't be tracked:

Teeth: 'You gotta change the sim-card but keep the phone, police fucking hate that. Can't track you with these mobile webs they got (StingRay device) (*points out to the road as if there is a device somewhere picking up phone signals*). Right this guy Jack we're gonna meet, he's a real nutter, weird one he is. Had to take one of his Teeth once… keep him in check.'

The above anecdote indicates intricate levels of counter-surveillance as Teeth scanned the interior of his vehicle using specialised radio-frequency equipment to detect police bugs. He further highlighted how he avoided becoming visible through passive-monitoring device-systems, like police webs, that monitor mobile phones by recruiting contacts who could switch their IMEI numbers. Teeth, nevertheless, sometimes showed a preference for less-hi-tech solutions, using first-generation 'burner phones' for sales whose sim he regularly replaced.

The sophistication and depth of Teeth's actions further highlight how knowledge about securitisation has become commonplace in the early 21st century, with organised criminal operations requiring safeguarding to deter unwanted eyes and remain profitable. Furthermore, Teeth deceived the police by keeping his smartphone on at home to create a digital alibi and rigged the location with CCTV linked to another Smartphone to see the location on the move, allowing him to respond to potential raids. Teeth further invisibilised his operations through the highly exploitative practice of debt bondage: commandeering customers' bank cards and spending their money untraced (Berry et al., 2023). By observing several drug deals that were arranged during the fieldwork, the researcher was also temporarily drawn into this network. Again, Teeth's account shows how worse harm arose as he moved into the illicit drug market, trading heroin and crack cocaine while responding with callous cruelty to those who crossed him.

Disappearing/Blocking

Information Communications Technologies are central to how contemporary society is governed. However, criminal actors can step outside this surveillant web by avoiding technologies that harvest data or by repurposing technologies to block information flows. The following section, '*disappearing/blocking'*, discusses how targets of observational systems disappear or use technologies to hide their activities. It examines the case of Shane who physically removed his tag during his bail order and Charley who used encrypted messaging to shield his communications while selling steroids.

Shane

Shane, in his early 20s, is a notorious former prisoner in the region who has convictions for assault, commercial burglary and selling narcotics and was awaiting trial for an alleged assault on a Prison Officer committed a week before release from his last jail stint. Previously on EM bail on a 4 p.m. to 8 a.m. curfew that also required daily sign-ins at a police station, Shane opted to remove his tag and go on the run due to the delay of his trial several times while facing a reasonable chance of reconviction.

I exit my ride to walk the remaining distance to my work as nightclub security. The venue is located directly next to a notorious alleyway, infamous for the distribution of crack cocaine and heroin in the city. Moving past the revellers, nitrous-oxide vendors and beggars, I recognise a large figure standing with his back to a boarded shop covered in graffit. It's Shane, the first person I interviewed who disappeared shortly after; he cautiously watches people and momentarily tenses as I approach but relaxes when he recognises me. Someone yells: 'NOS-BALOON, MATE?!' into my face, which I decline and Shane offers his fist to bump. As I suspected, he was on the run: he'd cut his tag off and vacated his sister's home. Unable to work or claim benefits, he'd returned to whatever means available while sleeping on a friend's floor.

After work, I receive a message from an unknown number cryptically declaring: 'whisky brandy'. Confused, I text back and the reply states: 'white or brown' and is signed: 'bandit'. I realise that it's from Shane's new phone –we'd swapped details and this was his street alias- the message was code for crack or heroin referring to the colour of the substances; he'd sent out blanket messages to boost demand.

Shane's previous EM and bail regime had allowed the rigorous control of his whereabouts while he awaited his trial; nevertheless, he disappeared using rather low-tech means (a bread knife) after seven months spent inside this matrix of observation. Besides showing that monitoring systems can become vulnerable to basic strategies, Shane's case indicates how particularly tight controls with unclear procedural justice outcomes may promote recidivist-organised offending. Indeed, Shane discussed how his EM bail order -which had a 16-hour a-day curfew and required daily trips to a police station- was initially scheduled for three months; however, it was extended over seven after several reschedules and with no end in sight, worsening anxiety led him to prefer the risk of prison.

Shane's life on the run also highlights how 'dropping off the grid' sometimes displaces crime into more harmful offending; after becoming invisible, Shane subsisted on the margins of society, also moving into the high-harm trade of crack cocaine and heroin. Shane chanced eventual discovery despite taking precautions to shield his identity; regardless, his current danger appeared preferable to his previous circumstances, creating a form of *penal limbo.* To help stay undetected after the police issued a warrant for his arrest, Shane used older cell phones for communication/sales and avoided social media, deploying acrostics to minimise the creation of phone data implicating him in new offences.

Shane's circumstances as an outlaw eventually became unsustainable. Having spent most of his young life behind bars and now under the constant threat of arrest, he eventually handed himself into police custody. Speaking a year later, he discussed how intense state surveillance also created worries about being a financial burden on his sister and young niece, eventually leading him to want a total reset: '*When I get out of prison… I can't be goin' around with nuffin'… I can't be walking the streets with nuffin', I can't be going out with my friends and him be buyin' me drinks. Like, I'm the kind a guy who wants to be offerin' you the drinks, d'you know what I mean?' It's just shit'.* To add insult to injury, the initial case against Shane was dropped due to a lack of evidence but he was re-sentenced to six months in prison for the bail order violation. The remainder of the section examines the case of Charley who distributes image and performance-enhancing drugs:

Charley

Charley is an online steroid supplier in his late 30s and distributes internationally. In his youth, he supplied cannabis and ecstasy pills to friends in small amounts. He hosted a website on the clear-net but increasingly uses social media for local sales; however, due to an inter-jurisdictional police sting, he temporarily closed his enterprise after this interview. The discussion highlights his previous attempts to block surveillance:

Charley: 'I never use my sim for calls or anything like that, Facebook's got encryption. I don't have to worry about the police listening in or anything. I mean… not that they're gonna bother for a bit of gear, but you never know…'.

Currently unknown to the authorities, Charley discussed commonplace communications platforms that block state surveillance through in-built features to sell restricted pharmaceuticals. Charley's testimony shows that smartphone apps, like Facebook or Whatsapp, with end-to-end encryption are often preferred device-systems for criminals to conduct local business; he believed the technology diminished the risk of leaking information due to messages bypassing phone service providers. This strategy of distributing black-market prescription medications through digital platforms locally to trusted customers and internationally (online) through postal services, earned Charley and associates around a million pounds per year.

Further talking about how he deployed social-media platforms to prevent his data from becoming visible, Charley discussed how their difficulties wiretapping; accessing data from servers and devices meant that these platforms had been highly successful for him in blocking contemporary forms of digital regulation -until that point. Indeed, it had been a tip-off from a contact trafficking the contraband through Europe that informed Interpol of the network, leading them to close their website. Nevertheless, Charley also highlighted how he occasionally took unnecessary risks as he sometimes used Fakebook's non-encrypted messaging service for sales. Whether this was complacency or a lack of knowledge around the safety of these platforms was not discussed; however, a plausible explanation relates to his criminal market: distributing steroids to bodybuilders who typically communicated through smartphones with standard non-encrypted Facebook messenger, he became locked into trading formats with buyer consensus.

Charley's account, again, highlights how dynamic circumstances influence counter-surveillance. A comparison of how Charley masked his digital footprint to Teeth in their respective enterprises illustrates this further. Charley, being around 10 years younger was *already familiar* with smartphones when he entered the drug trade and knew how to block potential observation using inbuilt features; contrastingly, Teeth was incarcerated during their mass proliferation and preferred the perceived safety of his older tools. Teeth believed that by generating more data, smartphones presented a greater risk for communication, so avoided them for business. That said, both dealers also traded substances with vastly different penalties and enforcement priorities.

For Charlie, selling steroids was less risky, though, significant harms still sometimes occurred as his products were untested, sometimes wrongly dosed and mislabelled.[9]

Discussion

This paper addresses the following research questions through analysing the above data: (1) How do organised crime groups avoid visibility from state surveillance? (2) How is organised crime displaced by surveillance? (3) What harm arises as organised crime is displaced/invisibilised?

Here, *'manipulation/redeployment'* are useful frameworks for considering counter-surveillant strategies within organised crime groups, such as Idris', who exploit limitations within surveillant systems to keep their operations invisible. Writings on surveillance discuss how recent technologies (from mobile phones to EM tags) increase the control capabilities of governing institutions by making behaviour visible and manageable (Haggerty & Ericson, 2000). ANT, instead, emphasises that socio-technical systems are 'fluid', which can lead to varying outcomes (De Laet & Mol, 2000). By acknowledging that interactions between objects and humans are undetermined, the approach has value in understanding how Idris manipulated the surveillant regime of EM as he shifted his narcotics distribution around his curfew. Certainly, research suggests that crime is temporally displaced by EM when users switch offending times (Hucklesby, 2013); Idris, similarly, worked around the penal technology, even deftly using his restrictions to get himself off the hook in a new investigation.

Closer readings of Deleuze acknowledge his commitment toward 'fragmentation', which asserts that governing agendas are often incomplete and prone to fracturing (Haggerty & Ericson, 2000). Although this understanding of governance may be valuable to reflect on Idris, he also outlined how his regime became undoubtedly coercive in other ways; being electronically monitored prevented him from visiting family and significantly worsened his mental health. ANT asserts that objects may not only be viewed differently depending upon the perceiver but can lead entirely 'different realities' to be constructed around them (Law, 2000). Idris' performances within different research settings may illuminate this claim as he downplayed his criminal exploits, hiding his ankle tag after proudly exhibiting them beforehand. According to Ekblom (2017), technological adaptations purely serve the purpose of controlling and preventing crime. Idris' testimony challenges this whilst developing EM research that shows how stigma or pride may be felt by different users (Nellis, 2013); he, perplexingly, appeared to feel both yet became increasingly violent during his sentence, causing significant harm when disciplining treacherous associates.

The frameworks '*manipulation/redeployment'* also have value when reflecting upon how criminals co-opt observational technologies to provide high demand/low supply 'protection services' where state control is absent (Gundur, 2022). Liam detailed how illicit enterprises are particularly at risk from predators as observational

[9] Charley claimed that steroid use is reasonably common amongst police officers, also plausibly providing another layer of protection.

technologies allow money to be extorted from targets. For Haggerty and Ericson, the emergence of mass surveillance is tied to the idea of 'risk management', whereby new monitoring systems provide the state with the capacity to predict and control future behaviour (2000: 611). Conversely, Liam's anecdote indicates the re-deployable nature of observational tools, like drones, which may be used to *increase risk*. ANT work on governance helps to understand this dichotomy, arguing that social-spatial territories must be continuously established through surveillant devices in various locations, making them fluid (Woolgar & Neyland, 2013). Liam's account perhaps evidences this by showing how 'ecologies of risk' were constructed from the bottom-up, becoming contestable by criminal groups.

Criminological research shows how technology allows older forms of crime to be committed in new ways, including smuggling drugs via drones into prison (Ralphs et al., 2017). With the drone flown to instil fear, Liam's account highlights more creative forms of repurposing. Writings on the abuses of state surveillance have highlighted victims of unwanted or intrusive monitoring (Gilliom, 2007); similarly, Liam's anecdote shows how the battle for control across the criminal network led multiple victims to emerge (particularly the workers). ANT's network approach considers how collateral impacts can arise from unwanted observation, with research advancing the idea of 'hybrid victimisation' to describe how cybercrime disperses harm while blurring boundaries between networked victims and offenders (Van Der Wagen & Pieters, 2018). The idea can be considered through Liam's testimony, which showed how the technological connectivity enabled by surveillant technologies blurs boundaries between criminals and targets, leading one faction in the prostitution network to gain an advantage. In a related vein, writings on online sex-work question 'who its real victims are', whilst continued offline prohibition is claimed to harm workers (Denney & Tewksbury, 2017). Liam's evidence highlights problems created by this crime control approach: the operation's activity could be easily displaced by changing its business patterns, whilst the workers became more vulnerable to exploitation as the security was tightened.

In the case of Vince and Teeth, the typologies '*deceiving/distracting'* are valuable in thinking about how criminals use knowledge about what their watchers can see to appear compliant or divert attention away from illicit activities. In his testimony, Vince discussed changing his offence type to spice distribution to appear reformed while resolving being financially penalised by his EM parole conditions. Schuilenburg (2015) discusses how finer control is today possible using Deleuze's (1992) idea of 'rhizomes', which explains how the observation and governance of behaviour has become increasingly decentralised yet all-pervasive. This can be applied when pondering the multiple well-connected agencies that closely monitored Vince. Nevertheless, he cunningly worked around them while under near-constant surveillance and set up a spice smuggling ring, using contacts in jail to run narcotics undetected.

ANT research has used the idea of 'discretion' to show how actors can influence decision-making processes by concealing their intentions or design-scripts, allowing desired outcomes to be subverted (Law, 2004). Vince's activities illuminate this claim; he subverted his arrangements and invisibilised his nefarious activities, even using their 'de-centeredness' to his advantage due to their reliance on coercive -yet optically narrow- surveillant technologies. His account provides further detail on

findings that show crime is displaced as some EM users switch offences to avoid detection while appearing compliant (Hucklesby, 2013).

Ekbom's (2017) concept of a criminal 'technological arms race' rests on rational choice theory; devices may prevent crime but are malleable enough to be defeated. Despite appearing instructive in Vince's case, similar ideas are challenged for underestimating how technologies create and change associations (Ihde, 2003). Certainly, Vince's circumstances had become especially criminogenic due to being unable to work without serious risk of violating his curfew and his family's increasing irritation with his dependence upon them. However, again, reducing his deception to a simple cost-benefit analysis ignores important ecological factors that contribute to criminal decision-making: he believed that his parole regime set him up to fail, leaving him with little choice but to draw upon his criminal associates to get by. Vince provides details on concepts like 'partial compliance', which are advanced in EM literature concerning how some users offend while complying and others vice versa (Nellis, 2013); moreover, it demonstrates how worse harm occurred as his offending was displaced into the, sometimes, lethal spice trade.

In the case of Teeth, this framework is also useful when considering how organised crime groups can anticipate and divert law enforcement, such as through bogus phone calls and digital alibis. The idea of 'target hardening' is borrowed by Ekblom to describe how technological advances in security make offences, e.g., vehicular crime, increasingly difficult (2017). However, his approach is further challenged for implicitly concentrating on the perspective of authorities over criminals (Berry, 2018). Indeed, when thinking about how Teeth foiled his observers to steal cars and sell narcotics, 'target weakening' seems accurate. Work on policing also discusses how prioritising resources typically determines officers' responses (Bacon, 2017). Teeth highlighted how this knowledge helped him to provide disinformation about bogus offences while monitoring police conversations. Research on the digitisation of information highlights how 'fake news' and propaganda have become normalised in our current era (Zuboff, 2019); Teeth's example demonstrates that criminals can also employ these tactics, expertly distorting knowledge through communication systems to distract observers.

Lending the idea of 'deterritorialisation', Haggerty and Ericson (2000: 606) explain how abstracting individual identities from physical space as discrete data flows allows their granular control in digital space. Nevertheless, as observed, Teeth avoided his 'data double' being visibilised by minimising Smartphone use. A key claim in ANT that can assist in understanding how he continued his organised drug distribution network undetected, is that expert knowledge *increasingly becomes common knowledge* as lay actors are integrated into systems. Indeed, research on EM surveillance reports that controversies about securitisation often inform how the sanction operates for users (Berry, 2019). The complexity and extent of Teeth's operations perhaps illuminate this argument further; despite new listening and wiretapping devices being used by the police and mobile phones generating location data through GPS\ cell site connectivity (Bennett, 2012), he successfully distracted potential watchers. Furthermore, his account indicates how worse harm can arise from attempts to avoid becoming visible to state surveillance as he progressed into the lower-risk/higher-

profit hard drug trade, inflicting intimidation and violence upon those who failed to pay their debts.

In the case of Shane who went outside the gaze of EM by removing his tag, the frameworks, '*disappearing/blocking'*, were useful in demonstrating how criminals disappear from surveillance/use technologies to hide their activities. Deleuze has asserted that governance no longer works at the level of individual identities but by managing sub-individual data through more dictatorial processes of 'modulation' (Hui, 2014). Although very applicable for understanding how EM uses discrete data to control whereabouts, further thought is required for how it fails. Indeed, it was precisely because of how coercive this digital modulation had become that Shane disappeared from observation. His account supports research on EM bail, which shows it does not always decrease the ill effects of remand or maintain public protection when suspects cannot live or make plans (Barry et al., 2007). Indeed, standalone EM use is criticised as a 'cheap form of incapacitation' that provides little longer-term value (Nellis, 2013); Shane's testimony further highlights how organised offending can be displaced into high-harm markets as offenders avoid visibility when surviving entirely outside civil society; indeed, putting himself in harm's way by vending in notoriously dangerous locations.

ANT work on governmentality examines how governing activity becomes 'insecure' when relied-upon actors behave unexpectedly or confounding variables are encountered, which necessitates repairs to fix them (Woolgar & Neyland, 2013). Shane's account illuminates this argument: as a key stakeholder whose goodwill was relied upon for the continued digitised management of his behaviour, uncertainty around his future and worsening circumstances led him to disappear. For contemplating the relatively low-tech nature of Shane's invisibilisation strategy, the recent concept of the 'digital divide' might also be instructive (Berry, 2021). Used to explain new forms of inequality led by increasing digitalisation, Shane's life history (where he spent most of his life in prison and extreme material poverty) perhaps illustrates how members of organised crime groups with less technological proficiency struggle to offend undetected within tight observational regimes. That said, Shane showed that simple strategies can still challenge technologically mediated forms of investigation, using simple text message codes and avoiding smartphones while on the run.

With Charley exploiting features within social media platforms to shield his operations, the framework of 'disappearing/blocking' also has utility in examining how criminals avoid becoming visible to law enforcement. Indeed, research shows that, despite being less secure than they assume, smartphone apps with end-to-end encryption are often used by offenders in illicit enterprises (Moyle et al., 2019). Nonetheless, Charley and associates successfully deployed these tools to acquire a near fortune from the organised distribution of black-market pharmaceuticals, minimising risk (notwithstanding his occasional complacency). Haggerty and Ericson (2000) deploy the idea of the 'data double' to explain how social control is enabled in virtual space by 'reassembling digitised footprints'. Although it has value in examining contemporary forms of digital regulation, it lacks when reflecting on how Charley managed to avoid the data created through his steroid sales being intercepted, even when blasé about not encrypting messages.

The ANT concept of 'black-boxing' -which describes how technologies become closed-off to prevent scripts from changing, unwanted information leaking or when users do not see alternative usage modes- can provide an alternative explanation for Charley's inconsistent invisibility ploys. The proposition is illuminated through the way he redeployed his favoured social media platform to sell steroids through riskier methods for financial gain, either placing trust in his presumed lower priority for enforcement agencies or unwillingness to decline non-encrypted custom. Certainly, research shows that distributing drugs online creates risks of surveillance through the additional monitoring of data (Berry, 2018); regardless, Charley and associates even risked being visible on the clear-net for international sales to increase profit from foreign markets.

As discussed, Ekblom (2017) sees criminal justice equipment purely as instrumental; however, Charley's account shows that techniques to avoid observation cannot be taken for granted as organised criminals sometimes deploy device-systems inexplicably. Claims that expanding observation regimes mostly impact 'non-criminals' have merit (Zedner, 2007).[10] Charley's account highlights how organised offending is often displaced by attempts at visibilisation, existing as occupational hazards that committed criminals knowledgeably work around; indeed, his transition to steroids reduced his legal precedence whilst jeopardising his customers' health with home-made anabolic recipes. Approaches towards surveillance based on crime control rather than harm reduction, risk worsening this.

Conclusion

This article examined data from two ethnographies of active offenders operating under regimes of surveillance and considered how they avoided visibility while continuing illicit enterprises: counter-surveillance. It showed that despite the penal sanction of EM and investigatory technologies of law enforcement, organised crime is often displaced by state surveillance, sometimes leading to more harmful criminal activities. Contemporary top-down interpretations of Deleuze and theories of surveillance, like Ekblom's, that see innovations as move-countermove were shown to be lacking when applied to real offenders; subsequently, the ethnographic approach of actor-network theory was deployed to illuminate the various strategies deployed within organised crime groups. Analysing several cases, these differing strategies resulted from the inherent re-deployability of contemporary surveillance tools, which made avoiding, manipulating and re-purposing them possible. Consequently, the article shows weaknesses in attempts at controlling crime this way: driven by the high financial rewards of illicit enterprises and barriers toward legitimate economic activity. With some participants using serious violence, coercion and intimidation; others trading in highly damaging substances or operating in exploitative ventures, critical re-consideration of prohibition-based policy is raised. As non-criminals are also more likely to be controlled and monitored as surveillance intensifies and collateral victims remain, this provokes serious questions about state responses to crime in the 21st century.

[10] Though must not be overestimated: many offenders on EM report its benefits (Hucklesby, 2013: p.236).

Finally, the article provides a detailed analysis of an emerging issue. It gestures to a rapidly evolving criminological area that will change due to AI developments and smart infrastructure, which organised crime groups must negotiate and re-purpose to remain profitable and hidden. Therefore, this ethnographic snapshot will likely require revision in the coming years to understand how traditional street offences related to organised crime continue becoming mediated by surveillance technology, besides how displacement and harm arise.

Acknowledgements This article is dedicated to the memory of 'Idris' -rest in peace brother. Although troubled, you were generous, honest and unwaveringly loyal to your friends and family.

Data availability The data analysed in the current study are unavailable due to the confidentiality agreement between the researcher and the participants. This clause was also part of the ethics application that was approved.

Declarations

Ethical approval The respective University's Ethics Boards approved these projects.

Informed consent Each participant read and agreed to the Letter of Information, outlining the research goals and objectives. The letter also informed the participant that the ethics board approved the research and contact information for ourselves and the ethics board was provided.

Statement regarding research involving human participants and/or animals This research was completed with the participation of offenders subject to electronic monitoring and organised criminal offenders. Participation was voluntary and interviews/observations were only conducted with those that consented.

Competing interests We have no conflicts of interest to disclose and received no personal financial compensation for this research.

References

Bacon, M. (2017). *Taking care of business: Police detectives, drug law enforcement and proactive investigation*. Oxford University Press.

Barry, M., Malloch, M., Moodie, K., Nellis, M., Knapp, M., Romeo, R., & Dhansiri, S. (2007). *An evaluation of the use of electronic monitoring as a condition of bail in Scotland*. (Report) Scottish Executive. https://strathprints.strath.ac.uk/18649/6/strathprints018649.pdf

Bennett, D. (2012). The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. *Information Security Journal: A Global Perspective*, *21*(3), 159–168.

Berry, M. A. (2018). Technology and organised crime in the smart city: An ethnographic study of the illicit drug trade. *City Territory and Architecture*, *5*(16), 2–11.
Berry, C. R. (2019). Under surveillance: An actor network theory ethnography of users' experiences of electronically monitored punishment. *European Journal of Criminology*, 1–20.
Berry, C. R. (2021). Life on tag: An actor network theory ethnography of users' experiences of electronically monitored punishment. [Doctoral dissertation, University of Bristol]. Student theses. https://research-information.bris.ac.uk/en/studentTheses/life-on-tag
Berry, M. A., Salinas, M., & Gundur, R. V. (2023). Financial risk management strategies of small to medium illicit drug enterprises: Considering low-level money laundering. *Trends in Organized Crime*,1–23.
Braun, V., & Clarke, V. (2014). Thematic analysis. *Qual Res Clin Health Psychology*, *24*, 95–114.
De Laet, M., & Mol, A. (2000). The Zimbabwe bush pump: Mechanics of a fluid technology. *Social Studies of Science*, *30*(2), 225–263.
Deleuze, G. (1992). Post-script on the societies of control. *Jstor*, *59*(3), 1–7.
Denney, A. S., & Tewksbury, R. (2017). ICT's and sexuality. In M. R. McGuire, & T. J. Holt (Eds.), *The Routledge handbook of technology, crime, and justice* (pp. 113–133). Routledge.
Ekblom, P. (2017). Crime, situational prevention and technology. The nature of opportunity and How it evolves. McGuire, M. R., & Holt, T. J. (Eds.). *The Routledge handbook of technology, crime, and justice*. (pp.353–374) Routledge.
Gacek, J. (2022). *Portable presence: Electronic monitoring and the creation of carceral territory*. McGill, Queens University Press.
Gilliom, J. (2007). Struggling with surveillance: Resistance consciousness and identity. In K. D. Haggerty, & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 111–129). University of Toronto.
Guerette, R. T. (2009). *Analyzing crime displacement and diffusion*. (Report). US Department of Justice, Office of Community Oriented Policing Services. https://popcenter.asu.edu/sites/default/files/tools/pdfs/displacement.pdf
Gundur, R. V. (2022). *Trying to make it*. Cornell University Press.
Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622.
Hucklesby, A. (2013). Insiders views: Offenders' and staff's experiences of electronically monitored curfews. In M. Nellis, K. Beyens, & D. Kaminski (Eds.), *Electronically monitored punishment: Critical and international perspectives* (pp. 228–247). Routledge.
Hui, Y. (2014). Modulation after control. *New Formations*, *84*(85), 74–92.
Ihde, D. (2003). Beyond the skin-bag: The brain extends its reach outside the body, so are we all cyborgs? *Nature*, *424*, 615.
Latour, B. (2005). *Reassembling the social: An introduction to actor network theory*. Oxford University Press.
Law, J. (2004). *After method: Mess in social science research*. Routledge.
Layder, D. (1998). *Sociological practice: Linking theory and social research*. Sage Publications Ltd.
Lianos, M., & Douglas, M. (2000). Dangerization and the end of deviance: The institutional environment. *The British Journal of Criminology*, *40*, 261–268.
Lyon, D. (2007). Synopticon and Scopholia: Watching and being watched. In K. D. Haggerty, & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 36–54). University of Toronto.
Marx, G. T. (1988). *Undercover: Police surveillance in America*. University of California Press.
Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *A Journal of the Society for the Psychological Study of Social Issues*, *59*(2), 369–390.
McGuire, M. R. (2012). *Technology, crime, and justice*. Routledge.
Moyle, L., Childs, A., Coomber, R., & Barrat, M. J. (2019). #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy*, *63*, 101–110.
Nellis, M. (2013). Surveillance based compliance using electronic monitoring. In P. Ugwudike, & P. Raynor (Eds.), *What works in offender compliance* (pp. 143–164). Palgrave Macmillan.
Nellis, M. (2019, February 4). *Clean and dirty electronic monitoring*. Justice Trends Magazine. Retrieved March, 7, 2023, from https://justice-trends.press/shaping-lives-the-use-of-electronic-monitoring/
Ralphs, R., Williams, A., Askew, R., & Norton, A. (2017). Adding spice to the porridge: The development of a synthetic cannabinoid market in an English prison. *International Journal of Drug Policy*, *40*, 57–69.

Rao, M. B., Jongerdon, J., Lemmens, P., & Ruivenkamp, G. (2015). Technological mediation and power: Postphenomenology, critical theory, and autonomist Marxism. *Philos Technol*, *28*, 44–474.
Schuilenburg, M. (2015). *The securitization of society*. New York University.
Tombs, S. (2018). For pragmatism and politics: Crime, social harm and zemiology. In A. Bouklia, & J. Kotze (Eds.), *Zemiology: Reconnecting crime and social harm*. Palgrave Macmillan.
Van Der Wagen, W., & Pieters, W. (2018). The hybrid victim: Reconceptualising high-tech cyber victimization through actor-network theory *European Journal of Criminology*, 1–18.
Vandenberghe, F. (2002). Reconstructing humants: A humanist critique of actant-network theory. *Theory Culture and Society*, *19*(5), 51–67.
Woolgar, S., & Neyland, D. (2013). *Mundane governance: Ontology and accountability*. University of Oxford.
Young, J. (2011). *The criminological imagination*. Polity.
Zedner, L. (2007). Pre-crime and post-criminology. *Theoretical Criminology*, *11*(2), 261–281.
Zuboff, S. (2019). *The age of surveillance capitalism*. Wiley.