Guest Editorial

Beyond Cybercrime: New Perspectives on Crime, Harm and Digital Technologies

Faith Gordon
Australian National University, Australia
Alyce McGovern
UNSW, Australia
Chrissy Thompson
Australia
Mark A. Wood
Deakin University, Australia

Introduction

During the last decade, there has been an upsurge in scholarship taking an interdisciplinary approach to examining the nexus between crime, harm and digital technologies. Such scholarship encompasses and extends the remit of traditional ‘cyber’ and computer crime research and often moves beyond notions of cyberspace and online/offline dichotomies to account for the increasingly ‘onlife’ (Floridi 2013) way harms are perceived, perpetrated and responded to. This special issue extends criminological scholarship by similarly examining how digital technologies are conceptualised within research on crime and (in)justice. Each article in this special issue takes an interdisciplinary approach to examining intersections between crime, harm, (in)justice and digital technologies. The contributions bring criminology into conversation with fields such as critical algorithm studies, digital sociology, design studies, continental philosophy and critical data studies. The articles analyse a range of harms, including doxxing, domestic violence, the digital racialisation of crime, and gender-based violence. Through analysing these and other harms, the authors make theoretical contributions that broaden our understanding of the technology–harm nexus and provide criminologists with new ways of moving beyond cybercrime.
Why ‘Beyond Cybercrime’?

**Beyond Cybercrime**

One way of going ‘beyond cybercrime’ is to move beyond the ‘cyber’ prefix itself. The ‘cyber’ in ‘cybercrime’ has its origins in the notion of ‘cyberspace’, a term that is often attributed to science fiction author William Gibson. First used by Gibson (1987/1986) in the 1982 novelette, *Burning Chrome*, and later popularised by his influential 1984 debut novel, *Neuromancer* (Gibson 2016/1984), the concept of ‘cyberspace’ has been employed extensively within both popular culture and academic discourse. Cyberculture (Bell and Kennedy 2000), cyberpolitics (Hill and Hughes 1998; Jordan 2001) and cybercrime (Wall 2007; Yar and Steinmetz 2019) are but a few examples of terms incorporating the cyber prefix and, with it, the conceptualisation of cyberspace it presupposes. The concept of cyberspace has several implications. First, the term frames computational media through a spatial lens (Yar 2005). For proponents of the term, computational technologies generate a new navigable space for human interactions and communication. Indeed, as Dodge and Kitchin (2001: 1) explained:

> the term cyberspace literally means ‘navigable space’ and is derived from the Greek word kyber (to navigate). In William Gibson's 1984 novel *Neuromancer*, the original source of the term, cyberspace refers to a navigable, digital space of networked computers accessible from computer consoles; a visual, colourful, electronic, Cartesian datascape known as ‘The Matrix’ where companies and individuals interact with, and trade in, information. Since the publication of Neuromancer, the term cyberspace has been reappropriated, adapted and used in a variety of ways, by many different constituencies, all of which refer in some way to emerging computer-mediated communication and virtual reality technologies.

Second, the concept presents cyberspace as a separate space to terrestrial space—a separation that is echoed in the now more common distinction between online and offline spaces. Such a distinction between ‘cyberspace’ and ‘physical’—or offline—spaces has been central to some conceptualisations of cyber criminology. Jaishankar (2007: 1), for example, argued that cyber criminology as a field is dedicated to studying the causes of ‘crimes that occur in the cyberspace’ and examined their ‘impact in the physical space’.

This conceptualisation of cyberspace as a separate domain to ‘physical’ space has, however, attracted significant criticisms (Powell, Stratton and Cameron 2018; Salter 2016), with contemporary research demonstrating a ‘blurring of the boundaries’ between online and offline spaces (Gordon 2021). Jurgenson (2011, 2012) argued that distinctions between cyberspace and terrestrial/physical space often instate a form of ‘digital dualism’. Digital dualism, as Jurgenson (2011: 84) explained, is a ‘conceptual position … that views the digital and physical as separate spheres’. Critics of digital dualism have argued that the notions of cyberspace and being online are unable to capture the full range of ways that digital technologies can shape human experiences and practices, either unbeknown to them or in ways that do not involve users engaging with graphical user interfaces (Floridi 2013). To employ the postphenomenological vocabulary of Don Ihde (1990: 99), the notions of cyberspace and being online are unable to adequately capture *background relations* with digital technologies: relations in which technologies are not directly experienced but, nonetheless, structure human experiences as a ‘present absence’ (see Verbeek 2005). Here, we can take Kitchin and Dodge’s (2011) notion of ‘code-spaces’ as well as the Internet of Things (Milivojevic and Radulski 2020) to think anew about digital technologies and whether many of the assumptions underlying the cybercrime research of the early 2000s still hold today. For these and other reasons, several fields have turned away from the term. Cyber anthropology and cyber sociology have been supplanted by digital anthropology (Horst and Miller 2020) and digital sociology (Lupton 2015; Marres 2017), and scholars in security studies have argued that it is time to retire the cyber prefix from their disciplines (Branch 2021; Futter 2018). In this special issue, we similarly contemplate the utility of the cyber prefix for criminologists as we reflect on its place in our contemporary technoscape.
Beyond Cybercrime

In addition to going beyond the 'cyber' in cybercrime, we might also go beyond the 'crime' in cyber crime and instead take harm, rather than crime, as the central point of reference for examining the effects of digital technologies. To paraphrase Hillyard and Tombs (2007), by switching our point of reference from (cyber)crime to (techno-)social harm, we take up a broadly zemiological, rather than criminological, approach to digital technologies. Indeed, the very name of this special issue evokes Hillyard et al.'s (2004) Beyond Criminology: Taking Harm Seriously, a collection calling for a move from criminology to zemiology: a discipline dedicated to the study of social harms (Canning and Tombs 2021).

Thus, a second way of moving ‘beyond cybercrime’ is to consider a range of harms that fall beyond the parameters of traditional cybercrime scholarship. Due to its object of research—computer-facilitated crimes—cyber criminology focuses on a very specific subset of harms implicating digital technologies. Namely, the cybercrime approach focuses overwhelmingly on digital harms entailing ‘instrumental harm relations’: instances where technology is used in a manner that harms (see Wood 2021). This is not to say that cybercrime research necessarily treats technology as a neutral tool; cybercrime researchers have examined how the affordances and effects of digital technologies may contribute to computer-facilitated crimes (see Goldsmith and Wall 2019). However, cybercrime research has been primarily concerned with explaining why individuals use digital technologies to harm others and how such harms might be prevented. This is, of course, an important subset of technology-related harms that criminologists and zemiologists must examine. However, it is a subset that far from exhausts the forms of harm that technologies are implicated in creating (see Wood 2021). Criminologists and zemiologists might, for example, readily consider how the ‘engineered sociality’ (Van Dijck 2012: 161-162) of social media platforms contribute to the formation of communities, affinity groups and publics that promote harms that are not enacted through digital technologies (Wood 2017). While, in these cases, technologies have contributed to harms, these harms fall outside the umbrella of cybercrime. To go ‘beyond cybercrime’ is to acknowledge the plethora of ways in which digital technologies can contribute to social harms—ways that go well beyond using digital technology as the means to harm another.

This Special Issue

This special issue comprises 10 journal articles and one book review. Collectively, the contributions broaden our theoretical and conceptual understandings of the technology–harm nexus and provide criminologists with new ways of moving beyond cybercrime. The issue consists of two parts. The first part of the issue, entitled ‘Digital (in)Justices’, contains five manuscripts, each examining a particular intersection between digital technology and criminal justice agencies.

Pamela Ugwudike, in ‘Predictive Algorithms in Justice Systems and the Limits of Tech-Reformism’, examines how recidivism prediction algorithms used within the criminal justice system can perpetuate racial biases. Drawing together insights from critical algorithm studies and digital sociology (van Dijk 2005), Ugwudike details not only how these algorithmic biases can work to reproduce structural inequalities but how they are symptomatic of structural inequities. Such biases, Ugwudike argues, speak to the issue of who has the ‘digital capital’ to shape the design of algorithms. In doing so, they also speak to tensions between approaches that advocate a form of tech-reformism and approaches that address—and seek to change—the structural conditions that lead to algorithmic biases. Tech-reformist strategies, Ugwudike details, exhibit a technocratic and often ‘techno-chauvinist’ mindset, adopting a ‘soft determinism’ (Benjamin 2019) that searches for technical fixes for algorithmic biases. Moreover, they fail to address the structural antecedents of algorithmic injustice, such as the exclusion of affected groups from the design process. To explain and address these antecedents, Ugwudike develops a framework for understanding and mitigating algorithmic biases that accounts for the structural contexts in which algorithms are created and trained.
In 'The Carceral Automaton: Digital Prisons and Technologies of Detention', Carolyn McKay argues that prisons are on the cusp of technological transformation because the twenty-first century has brought with it a digital connectivity that permeates both prison design and the management of prisoners. The article provides a critical overview of the digital technologies that have emerged and are present in 'smart prisons'. McKay presents two distinct limbs that are emerging: (1) technologies that benefit the authorities and are embedded into the infrastructure of prisons to provide heightened security; and (2) technologies that have the potential to benefit prisoners in accessing justice, maintaining family relationships and facilitating programs that assist with optimising post-release circumstances and rehabilitation. Through the lens of the COVID-19 pandemic, McKay draws on recent Australian case law that demonstrates several of the harms that can ensue when human contact is replaced with 'smart' prison technologies. As McKay details, 'smart' prison technologies can produce environments that intensify mental health issues and feelings of social isolation among prisoners. These harms prompt a variety of ethical questions about the rise of 'smart prisons' and the processes of datafication, surveillance and automation that lie at the heart of these environments.

Michelle Lyttle Storrod, in 'Ecological Ruptures and Strain: Girls, Juvenile Justice and Phone Removal', details the harms of court-imposed phone removal orders on girls involved with the juvenile justice system. Integrating Bronfenbrenner's (1992) ecological systems theory, Agnew's (1992) general strain theory and feminist criminology (Belknap 2020), Storrod examines the digital ecologies inhabited by young people and how court-imposed phone and internet access bans can exacerbate the strains faced by young women who have entered the juvenile justice system. Drawing on interviews with 42 court-involved girls and 22 juvenile justice practitioners, Storrod details the numerous roles mobile phones can play in sustaining justice-involved girls' support systems. Justice-involved girls' digital ecologies, Storrod argues, can be central to obtaining support, creating feelings of safety and coping with the challenging micro-, meso- and exo-systems they inhabit. Consequently, phone removal orders can generate significant 'ecological ruptures'; ruptures that, in turn, create the very strains that can contribute to further involvement in the juvenile justice system.

In their piece, ‘“You Can't Actually Escape It”: Policing the Use of Technology in Domestic Violence in Rural Australia’, Bridget Harris and Delanie Woodlock examine digital coercive control in rural contexts. Juxtaposed against the 'spaceless' nature of digital forms of abuse, they explore the ways in which victims of domestic violence have to navigate issues of ‘space’ and ‘place’ when seeking assistance from criminal justice authorities. As Harris and Woodlock demonstrate through interviews and focus groups with rural, regional and remote victims/survivors of violence, many find it difficult to both seek assistance and navigate leaving relationships due to the complex combination of ‘spacelessness’, which leaves individuals at risk of harm at any place and time, place, which can mean geographic isolation from assistance for individuals living in rural areas, and space, which accounts for the particular social, cultural and practical features of an area that might make seeking assistance challenging. While some of the women interviewed had positive experiences with authorities, a number reported not being taken seriously by police, who either minimised their experiences or discouraged them from taking further action. As Harris and Woodlock argue, the mixed experiences of rural, regional and remote women seeking assistance from criminal justice agencies speak to the need for more specialised training and support in these areas, particularly given the enormous barriers victims/survivors already face in coming forward and seeking help.

In 'Good Tech, Bad Tech: Policing Sex Trafficking with Big Data', Richard Kjellgren considers efforts to police sex trafficking using big data, unpacking the complex nexus between sex trafficking, exploitation and technology. Drawing on feminist perspectives and critical data studies, Kjellgren examines the ways in which technology is positioned as both the problem and the solution when it comes to sex trafficking. As Kjellgren argues, while big data analytics and anti-trafficking software are hailed as potential saviours in the fight against sexual exploitation and trafficking, such claims suffer from two limitations. First, we are yet to fully understand the extent to which the internet and communications technologies have
facilitated sex trafficking and, therefore, cannot yet fully appreciate the benefits and risks of deploying the same technologies to address these concerns. Second, the belief in the capabilities of algorithms and data analytics to respond to sex trafficking often fails to take an adequately nuanced approach to the continuum of experiences of sexual labour. As Kjellgren explains, the uncritical uptake of big data analytics obscures this continuum of exploitation, leading to atheoretical and stereotypical understandings of sex trafficking and victimhood. Further, the social context of exploitation is neglected in favour of focusing on technology as a primary driver of sex trafficking. For Kjellgren, any efforts to explore the nexus between sexual exploitation and technology must account for these broader social contexts and understandings.

The second part of the special issue—‘Rethinking the Technology–Harm Nexus’—includes five manuscripts that engage with a range of techno-social harms. The authors provide novel theoretical contributions that explore how the intersection of technology and harm can be problematised and reconceptualised.

In their article ‘A Post-Capitalocentric Critique of Digital Technology and Environmental Harm: New Directions at the Intersection of Digital and Green Criminology’, Laura Bedford, Marcus Foth, Monique Mann and Reece Walters urge us to pay greater attention to the wider impacts of society’s engagement with digital technologies. First, they highlight how technological solutions to environmental problems bring with them their own environmental harms. Second, using three examples to demonstrate the environmental harms of technology—deep-sea mining for minerals used in the creation of technology, inbuilt obsolescence of devices and the disposal of e-waste—they highlight the enormous environmental impacts of digital technologies at the manufacturing stage, during the life of the product and the end-of-life phase. Drawing on design research, which has taken a reflective approach to considering how the discipline might be complicit in perpetuating social and environmental harms, Bedford et al. similarly invite digital and green criminologists in particular to imagine a post-capitalocentric, more-than-human way of challenging the growth of solutions to the environmental harms of technology that merely recreate such harms.

In ‘Dynamics of Social Harms in an Algorithmic Context’, Hanna Malik, Mika Viljanen, Nea Lepinkäinen and Anne Alvesalo-Kuusi synthesise the insights of zemiology (Pemberton 2015) and critical algorithm studies (Tufekci 2015) to explore how algorithmic systems can shape the nature and extent of mass harms. They do so by examining three cases of mass harms implicating algorithmic systems: (1) the Michigan Integrated Data Automated System, which caused significant financial, emotional and autonomy harms when the automated system generated widespread false positive fraud findings in unemployment and insurance claims; (2) the 2010 flash crash, in which algorithms accelerated the sudden price collapse in the United States stock markets; and (3) the 2018 discovery that political consulting company Cambridge Analytica had created psychometric profiles of Facebook users, drawing on data harvested without their explicit consent, for the purpose of voter microtargeting. To understand the dynamics of these harms, Malik et al. argue, scholars of social harm must reorient their focus from the socio-economic to the ‘socio-econo-technological’ by examining the technological layer of harm production.

Briony Anderson and Mark Wood, in ‘Harm Imbrication and Virtualised Violence: Reconceptualising the Harms of Doxxing’, develop concepts for understanding the harms of doxxing—publishing ‘personally identifying information’ about someone else on the internet. Drawing on Gross’s (1979) distinction between first-order and second-order harms, Anderson and Wood argue that doxxing produces both first-order harms to a victim’s interests and bodily integrity and second-order harms to a victim’s security interests. Understanding the relationship between these harms requires an ontology that can not only recognise how harms can be nested in, and emerge from, other harms but can also recognise how violence can be inscribed into (digital) objects that can carry the potential to harm. Anderson and Wood suggest that bringing Bhaskar’s (2008) critical realist ontology into conversation with Deleuzian (Bryant 2011;
Deleuze 1991; Lévy 1998) conceptualisations of the virtual can offer such an ontology. Further, they develop two concepts—the virtualisation of violence and harm imbrication—that synthesise Bhaskarian/Deleuzian theories to account for these characteristics of doxxing’s first- and second-order harms.

In ‘Swallowing the Black Pill: Involuntary Celibates’ (Incels) Anti Feminism within Digital Society,’ Angus Lindsay explores a harmful component of the ‘manosphere’ in his research into the involuntarily celibate (incel) worldview: the ‘black pill’. Through analysing online discussion forums frequented by incels, Lindsay demonstrates how the ‘black pill’ philosophy produces a mythology of victimisation founded on a belief that society is ordered around a hierarchy of attractiveness. It is through this hierarchy—and the series of biologically deterministic beliefs that underpin it—that incels justify their sexlessness. Further, the black pill philosophy, which is propagated on digital counter-publics, serves to normalise acts of violence against women and other out-groups, such as alpha-male ‘chads’. As Lindsay argues, the black pill represents a form of stochastic terrorism that has inspired incels to enact a range of harms, from gender-based hate-speech to terrorist violence.

In ‘Crime in the Age of the Smart Machine: A Zuboffian Approach to Computers and Crime’, Kevin Steinmetz introduces Shoshana Zuboff’s work on computer technologies to existing criminological research on crime and technology. Taking two key concepts from Zuboff’s (1988) writing in The Age of the Smart Machine: The Future of Work and Power, Steinmetz examines how Zuboff’s ‘informating’ and ‘intellective skills’ can just as readily be applied to illegitimate forms of labour as legitimate. Steinmetz argues that analysing cybercrimes through the lens of informating enables us to reshape our understanding of computer crime. Further, applying Zuboff’s concept of intellective skills—that is, the interpretation of data through a ‘symbolic medium’ such as a computer—can assist criminologists in understanding their role in the commission of computerised crimes. Steinmetz suggests that the utility of a Zuboffian approach, which frames cybercrimes as informed criminal labour, lies in its ability to connect the individual to both the situational and the structural.

Finally, the special issue finishes with Hannah Klose’s review of ‘The Pixelated Prisoner: Prison Video Links, Court ‘Appearance’ and the Justice Matrix’ by Carolyn McKay (Abingdon, Routledge, 2018, 242 pp). Klose argues that McKay’s (2018) inclusion of the typically marginalised voices of prisoners significantly adds to the limited body of existing international research on prisoners’ experiential accounts and perspectives of emerging technologies within the criminal justice system.

Correspondence: Dr Mark A. Wood, Lecturer in Criminology, Deakin University, Victoria, Australia
mark.wood@deakin.edu.au

---

Please cite this Guest Editorial as:

Except where otherwise noted, content in this journal is licensed under a [Creative Commons Attribution 4.0 International Licence](https://creativecommons.org/licenses/by/4.0). As an open access journal, articles are free to use with proper attribution.

ISSN: 2202-8005