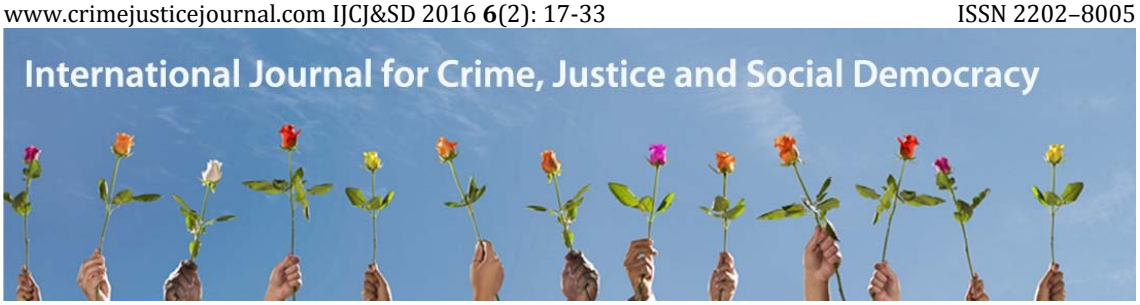
www.crimejusticejournal.com IJCJ&SD 2016 **6**(2): 17-33 ISSN 2202–8005



Crime and Justice in Digital Society: Towards a 'Digital Criminology'?[1]

Greg Stratton, Anastasia Powell, Robin Cameron
RMIT, Australia

Abstract

The opportunities afforded through digital and communications technologies, in particular social media, have inspired a diverse range of interdisciplinary perspectives exploring how such advancements influence the way we live. Rather than positioning technology as existing in a separate space to society more broadly, the 'digital society' is a concept that recognises such technologies as an embedded part of the larger social entity and acknowledges the incorporation of digital technologies, media, and networks in our everyday lives (Lupton 2014), including in crime perpetration, victimisation and justice. In this article, we explore potential for an interdisciplinary concept of digital society to expand and inspire innovative crime and justice scholarship within an emerging field of 'digital criminology'.

Keywords

Cybercrime; cyber; virtual; digital society; digital criminology.

Please cite this article as:
Stratton G, Powell A and Cameron R (2017) Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy* 6(2): 17-33. DOI: 10.5204/ijcjsd.v6i2.355.

Introduction

The transformative effect of digital and communications technologies, in particular social media, has been a well-documented focus of interdisciplinary study. Since the introduction of personal computer workstations in the early 1980s, and following the launch of the 'world wide web' in 1991, the criminological study of computer and cyber crimes has likewise rapidly expanded. Charting this scholarship alongside developments in computing, communications and other digital technologies reveals the influence of key technological shifts in the focus of criminological theory and research. Yet in this article, we suggest that recent and ongoing developments in technology, such as the social web, big data and the Internet of things, have been inadequately considered by criminologies of computing and cyber crime. Much research in the field continues to focus foremost on policing and investigations, legislative frameworks, and the motivations of cyber criminals, often in the context of individualised and 'rational offender' theories that seek to explain technology as merely a tool in the commission of otherwise familiar crimes. Moreover, the topics addressed by much computer and cyber crime research have remained relatively consistent over the last decade and predominantly include hacking; financial theft and identity fraud; illicit online markets and networks; child sexual exploitation; cyberbullying; and, more recently, information privacy and digital surveillance.

The conventional scope of computer and cyber criminologies has arguably developed to the comparative neglect of a wider range of ways in which computers and digital networks enable social harm. These include the role of technologies in a wider range of offending and victimisation, and recognise the increasingly embedded nature of online/offline experiences in crime and justice, the online victimisation of marginalised communities (such as on the basis of race, gender and sexuality), and broader issues of persistent social and digital inequalities as they relate to crime and justice. Rapidly emerging issues such as online justice movements, digital vigilantism, and so-called 'open-source' policing or social network surveillance, provide further examples under-examined within criminology. One possible explanation for what might be described as a 'siloed' cyber criminological focus lies in critiques of the discipline more broadly; namely, that criminology itself has become increasingly insular and self-referential, losing some of its fundamental and dynamic origins as the *multi*disciplinary study of crime, deviance and justice (see Garland 2011 for a detailed discussion). In light of this, we suggest that computer and cyber criminologies could benefit from an expansion and revitalisation that might be inspired by reference to developments in social, critical and technological theory from outside the discipline itself. Indeed, it is our intention to re-invigorate an ongoing conversation within the discipline that might expand the scope of conventional frameworks of cyber crime towards a broader exploration of crime and justice in the digital age.

In this article we offer the concept of the 'digital society' and its associated theoretical antecedents as one such framework to inform, expand and inspire innovative crime and justice scholarship within an emerging field of 'digital criminology'. To do so, we first provide a brief history of key developments in Internet and mobile technologies and their associated trends in crime and criminological research, as well as some limitations of this scholarship to date. Secondly, we consider recent criminological engagements with theories of *technosociality*, which have sought to expand the discipline beyond a conventional 'cyber' or 'virtual' approach to online crime and criminality. Third, informed by interdisciplinary social and technology theory, we define what we mean by the digital society and explore how this concept may further push the boundaries of 'cyber' criminologies and fruitfully expand theoretical frameworks and empirical examinations of crime and justice in the digital age.

A brief history of computer and cyber criminologies

The Internet has long-reaching origins, from advances in computing in the 1950s, to the first messages sent via the US military funded 'Advanced Research Projects Agency Network' (ARPANET) in 1969, to the earliest electronic mail (and spam) in the 1970s, to online

communications within private closed networks in the 1980s, to the global web in the 1990s (Leiner et al. 2009). Indeed, technological developments and their associated implications for crime and criminology can be charted across three broad periods. The 'pre-web' era of the 1980s to early 1990s, the 'global web' era of the 1990s to early 2000s, and the 'social web' era from the mid-2000s to the present day. Such a historical account is not intended to suggest that the challenges and opportunities for both crime and criminological scholarship presented by each era were (or are being) replaced or discontinued with the next but, rather, that each period brings with it unique advances in technology that have particular impacts for crime and can be broadly linked with associated shifts in criminological thinking and research.

It was not until the 1980s that personal computers[2] were widely adopted in workplaces and public institutions (see Ceruzzi 2003). From the 1980s onwards, however, the information and activities of governments, education institutions and corporations were rapidly computerised and associated with greater electronic data storage, as well as increased connectivity within closed internal and private networks (Ceruzzi 2003; Williams 1997). Criminology in this pre-web era (1980s to 1991) recognised that such widespread computer availability and electronic data storage, combined with internally networked workstations and dial-in connections, had opened-up governments, corporations and educational institutions to new forms of crime through technology misuse. Computer-related economic crimes (including financial data theft and identity fraud), 'eavesdropping' and the interception of confidential communications, software piracy (via illegal disk-based copies), and the security and privacy of confidential information systems were among the predominant concerns of the time (see, for example, Clough and Mungo 1992; Sieber 1986). Given the predominance of computer technology in public and corporate organisations, these emerging harms were in turn largely associated with white-collar crime (Croall 1992; Kling, 1980; Montgomery 1986).

This pre-web period also marked the initial legislative leaps to address computer-enabled crime. For example, one of the earliest laws that defined computer crime was passed in Florida in the United States in 1978 in response to the fraudulent printing of winning tickets at a dog-racing track using a computer (Hollinger and Lanza-Kaduce 1988). This law was notable as it defined all unauthorised access to a computer as an offence regardless of whether or not there was malicious intent (Casey 2011: 35). By 1983 another 20 states had introduced computer crime legislation. The *Computer Fraud and Abuse Act* of 1984 criminalised various forms of unauthorised computer accessing of information. Viewing information relating to defence or foreign relations matters was regarded as a felony offence, whereas intrusions designed to access or alter all other non-classified forms of information were regarded as misdemeanours (Griffith 1990: 460). Similar computer crime laws were subsequently introduced elsewhere. In Australia, for instance, a 1989 amendment to the *Crimes Act* outlined three categories of computer 'hacking' crimes: mere access without seeking out or altering specific information; access without initial intent but seeking or altering information; and access with intent to seek or alter specific information. In England, meanwhile, it was 1990 before the first criminal statute to tackle the misuse of computers was passed (Wasik 1991). Consistent with many legislative frameworks the very act of using a computer to breach a network or database was highlighted as an offence regardless of specific intent (Greenleaf 1990: 21). Indeed, a tension running throughout these initial legal reforms was the question of whether the act of computer misuse or unauthorised access itself should be specifically criminalised, in addition to the equivalent terrestrial or analogue crimes that may result.

The modern 'World Wide Web' went live to a global public on 6 August 1991 (Leiner et al. 2009). While understanding and legislating computer crime typified criminological research of the 1980s and early 1990s, with the 'global web' era (1990s to 2000s) came an associated shift towards Internet and 'cyber crime' research. The increased accessibility of online information sharing and communications that the global web brought for everyday users was widely recognised as creating new and massively expanded opportunities for crime because 'the

perpetrators who attacked machines through machines ... started attacking *real humans* through the machines [emphasis added]' (Jaishankar 2011: 26). Thus, while financial fraud, data theft, information privacy and identity crime became (and remain now) persistent themes in criminological research, the attention of 'cyber crime' scholars broadened to include interpersonal harms such as online child sexual exploitation and 'child pornography' (see, for example, Armagh 2001; Esposito 1998; Mitchell et al. 2010) with both crimes having become the focus of much public and policy concern.

The scope and focus of cyber crime scholarship in the global web era is well captured by David Wall's (2001) original and highly influential typology which comprises four categories of cyber crime:

1) *cyber-trespass*, incorporating unauthorised access to a computer system, network or data source, such as through on-site system hacking, online attacks, and/or malicious software ('malware');
2) *cyber-deception/theft*, including financial and data thefts, intellectual property thefts and electronic piracy. Such crimes may be facilitated through fraudulent scams, identity fraud and malware;
3) *cyber-porn and obscenity*, referring to the online trading of 'sexually expressive material' and including sexually deviant and fetish subcultures, sex work, sex trafficking and sex tourism, as well as child sexual grooming and exploitation material; and
4) *cyber-violence*, referring to the various ways that individuals can cause interpersonal harms to others. Such harms include cyberstalking, cyberbullying, harassment and communications that support prospective acts of terror (for example, including 'bomb talk' or the circulation of instructions for making explosives and other weaponry).

These in turn can be understood according to a common categorisation in cyber crime research whereby the first category represents 'computer focused' acts (that is, directed at the machine), while the latter three are more readily described as 'computer assisted' acts (see, for example, Jewkes and Yar 2010; Smith, Grabosky and Urbas 2004). Wall's (2001) early work identified that the Internet had influenced crime across these categories in at least three broad ways. First, it provided a platform for communications that may enable and sustain existing harmful and criminal activities, such as drug trafficking, hate-speech, stalking and sharing information on how to offend. Second, it enabled participation in a transnational environment that provides new opportunities and expanded reach for criminal activities that would be subject to existing law in sovereign states. Third, the distanciation of time and space creates potentially new, unbounded, contestable and private harms, such as the misappropriation of imagery and intellectual property. In particular, he suggested that the shrinking role of the state and the relative ungovernability of cyberspace presented particular challenges both for policing this 'virtual community' and for the discipline of criminology more broadly (Wall 1997). Wall argued that, while the new 'cyberspace' offered enormous democratising potential, 'there are also many opportunities for new types of offending' and that the Internet posed a 'considerable threat to traditional forms of governance and ... to traditional understandings of order' (Wall 1997: 208).

Despite the plethora of studies on cyber crimes, cyber criminality and cyber law enforcement that emerged over this period, comparatively fewer studies have sought to apply or adapt criminological *theory* to such research (Holt and Bossler 2014, 2015). The works that have undertaken such conceptual development have drawn predominantly on a handful of 'rational choice', deviant lifestyle and subcultural theories of crime (for reviews, see Diamond and Bachman 2015; Holt and Bossler 2014). In particular, Routine Activity Theory (RAT) (Cohen and Felson 1979) features so repeatedly in cyber crime theorising that it might be described as the prevailing orthodoxy in such research (Holt and Bossler 2008; Hutchings and Hayes 2008;

Pyrooz, Decker and Moule 2015; Reyns, Henson and Fisher 2011; Yar 2005). As Grabosky (2001: 248) explains: '[o]ne of the basic tenets of criminology holds that crime can be explained by three factors: motivation, opportunity, and the absence of a capable guardian ... [and although] derived initially to explain conventional "street" crime, it is equally applicable to crime in cyberspace'. While not all criminologists agree as to the applicability of the theory to cyber crimes (see Jaishankar 2008; Yar 2005), its dominance is arguably highly influential in framing the focus of much research with regards to identifying the motivations of individual cyber offenders, 'target hardening' and identifying 'risky' online victim behaviours. Moreover, identifying the challenges of law enforcement (as a form of guardianship) across a global network is a trend that has continued in computer and cyber criminologies. Indeed, in recent a review of the current state of cyber crime scholarship, Holt and Bossler (2014: 21) describe the preceding twenty years of criminological research as predominantly focused on the study of the 'impact of technology on the practices of *offenders*, factors affecting the *risk of victimization*, and the applicability of *traditional theories* of crime to *virtual offences* [emphasis added]'.

With the millennium came web 2.0 and the 'social web' (2000s to present), as online communications became increasingly collaborative with expanded capacity for user-generated content development and sharing, as well as online social networking. Between 2002 to 2010, there was an explosion of social networks and image-sharing platforms including Friendster, Myspace, Facebook, YouTube, Twitter, Tumblr and Instagram. Research into cyberbullying, cyberstalking and online harassment rapidly expanded over this period as the relative ease, anonymity and reach of online communications were associated with (continuing) concerns regarding invasive and threatening communications (Pittaro 2007; Reyns, Henson and Fisher 2011; Spitzberg and Hoobler 2002), particularly in relation to vulnerable groups such as children and young adults.

As the social web expanded, so too did the 'dark web' or 'deep web', a shorthand for the content on the Internet that is not indexed (and thus not searchable) by standard search engines and/or protected by layers of encryption and other security mechanisms (see Bergman 2001). Not *all* content on the dark web is necessarily or by definition illicit. Nonetheless, the concealment of such underground networks provides the ideal environment for illicit content (including child exploitation material), criminal organising (such as by terrorist or organised crime networks), and black markets (such as trading in malware and illicit drugs) (Martin 2014; Weimann 2016; Yip, Webber and Shadbolt 2013). A growing focus of cyber crime research has thus sought to identify and understand the nature and patterns of such online criminal social networks (Décary-Hétu and Dupont 2012; Holt 2013; Westlake and Bouchard 2016).

A further feature of the social web era is the increasingly 'mobile web', with smartphones and wearable technology becoming ever-more ubiquitous and simultaneously collecting expansive 'big data' about ourselves, our identities and our everyday lives. Criminological research has also sought to engage with these increasingly automated, algorithmic and computational capacities as they relate to crime data analytics, law enforcement and justice system practices (Berk 2008; Birks, Townsley and Stewart 2012; Brantingham 2011). There is to date, however, a comparative dearth of criminological research that has begun to empirically and critically explore the range of challenges and opportunities presented by 'big data' analytics. More recently, Janet Chan and Lyria Bennett Moses (2016: 25) have noted criminologists' relatively small engagement with big data research has tended to lie in two main areas: social media data analysis; and an increasing uptake of computer modelling/algorithms as a predictive tool in police and criminal justice decision making. They suggest that criminologists and, indeed, social scientists more broadly must increasingly 'share the podium' and collaborate with technical experts to further progress this field.

Breaking through the online/offline and real/virtual binaries

As the preceding discussion implies we suggest that there are notable gaps in the current field of cyber crime research (see also Hayward 2012; Holt and Bossler 2014). Despite the passing of more than ten years since the rise of the social web, much criminological scholarship arguably remains focused on computing and Internet technologies either as the *targets* of crime, or as mere *tools* in the commission of otherwise familiar and recognisable crimes. The topics and foci of much cyber crime research is likewise limited in scope. An overview of both seminal and contemporary works including books, edited collections and journal special issues over the past twenty years yielded recurring topics. These have included hacking, data theft, online fraud and scams, digital piracy, child 'pornography', online sex work, cyberbullying and cyberstalking, and cyberterrorism and online extremism, as well as the challenges for cyber legislation and law enforcement (Grabosky and Smith 1998; Holt 2011; Jaishankar 2011; Wall 1997). A limited amount of cyber crime research has been directed towards information privacy and data surveillance (Thomas and Loader 2000; Yar 2012). Moreover, minimal cyber crime scholarship has engaged with persistent social inequalities—the digital divide—as it relates to crime (see Halford and Savage 2010) and, as such, few studies have explored the unequal nature, impacts and responses towards cyber crimes and other digital harms with respect to gender, gender-identity, race and/or sexuality (notable exceptions include Halder and Jaishankar 2012; Powell and Henry 2016; Mann, Sutton and Tuffin 2003; Sutton 2002). Indeed in their recent review of cyber crime scholarship, Holt and Bossler (2014) make no mention of technology-enabled and online violence against women (despite discussing studies on harassment, stalking and bullying, which they overtly associate foremost with juvenile victims/offenders), or of Internet hate such as racially motivated hate speech or harassment focused on sexuality and/or gender-identity. This apparent oversight reflects a general dearth of cyber crime research that has engaged with forms of violence against marginalised and/or minority communities.

Arguably, there remains an inherent dualism whereby cyber crimes continue to be framed as a mirror or the online double of their terrestrial counterparts, differing perhaps by medium and reach, but not by nature; trespass becomes *cyber*-trespass, theft becomes *cyber*-theft, bullying becomes *cyber*-bullying; terrorism becomes *cyber*-terrorism. The foremost focus on the cyber, itself a direct reference to Internet and 'virtual' technologies, also obscures the diverse and embedded nature of digital data and communications in contemporary societies. Jaishankar (2007: 2) for instance, describes the field of cyber criminology itself as studies of '*cyber* crime, *cyber* criminal behaviour, *cyber* victims, *cyber* laws and *cyber* investigations [emphasis added]', as if these categories were all readily or neatly distinguishable from a 'non-cyber' equivalent.

Yet, in a ground-breaking article featured in *Theoretical Criminology*, Sheila Brown (2006a: 227) challenges such computer and cyber criminology to look outside of its conventional disciplinary frameworks and look instead 'towards theories of the *technosocial* [emphasis added]'. Analyses of cyber crime, she suggests, are likewise caught up in false distinctions between 'virtual' and 'embodied' crime; seeking to develop and translate 'old' legal and theoretical frameworks to understanding the 'new' crimes in cyberspace. Brown argues that, within criminology, 'nowhere is captured the vision of the crucial nature of the world as a human/technical hybrid ...' (Brown 2006a: 227), in which all crime occurs in networks, which vary only in degrees of virtuality/embodiment. Drawing variously on social and technology theorists such as Latour (1993), Lash (2002), Haraway (1985, 1991) and Castells (1996, 2001), Brown suggests a need for criminologists to understand crime and criminality at the increasingly blurred intersections of biology/technology, nature/society, object/agent and artificial/human. Computing and information theories, she argues, 'will increasingly infuse both domains of Law and Criminology' (Brown 2006a: 236) as social theory is not in itself sufficient to analyse and understand crime in contemporary societies.

Ten years after Brown's (2006a) challenge, and despite a burgeoning literature on computer and Internet-enabled crime, few criminologists have embraced this important conceptual undertaking. A notable exception lies in the emerging work of cultural criminologists who have sought to explore how the social web may be changing the culturally constructed nature, and socially constituted practices, of crime and deviance (see Jewkes 2007; Jewkes and Yar 2010, 2013; Surette 2015). For example, criminologist Majid Yar (2012) makes a persuasive case for considering the impact of communications technologies and new media as itself a *motivator* of criminality. In discussing the practice of 'happy slapping',[3] Yar (2012: 252) argues that 'crucial to understanding this phenomenon is the role played by participants' desire to be seen, and esteemed or celebrated, by others for their criminal activities'. He argues that this 'will-to-represent' one's transgressive self is linked to broader trends both of a self-creating subjectivity associated with processes of de-traditionalisation (Beck and Beck-Gernsheim 2002; Giddens 1991), and the ready availability of new media platforms for such self-creation (Yar 2012: 251). A further pertinent example lies in Keith Hayward's (2012) article in which he similarly notes the narrow scope of conventional cyber crime scholarship, and calls for further criminological engagement with spatial and socio-technical theory. Rather than a cyber crime focus on technology as a tool of diffusion which has increased criminal opportunities and networks, he suggests 'a better way of thinking about digital/online (criminal) activities is as a *process*, namely as phenomena in constant dialogue and transformation with other phenomena/technologies' (Hayward 2012: 455, emphasis in original). Hayward (2012: 456), drawing on Actor-Network Theory (Latour 1993, 2005) and Castell's (1996) networked 'space of flows', among others, notes the potential for communication technologies 'to alter the way we experience the sense of *being* in an environment [emphasis in original]'.

The core of Brown's (2006a) and, indeed, others' (such as Aas 2007; Hayward 2012; Wood 2016) related arguments, that criminological theory is enhanced by a hybridised concept of the human/technology nexus and a reconfigured concept of the agency exercised by human/technological hybrid 'actants', is not, however, without criticism. For example, Owen and Owen (2015: 17) take issue with Brown's central thesis 'that it is increasingly difficult to distinguish "human agency and culpability"' from "non-human objects and technology"'. Rather, they argue that, regardless of environmental conditions (of which technology is infused) 'reflexive agents possess the agency to choose not to engage in criminal activities where they believe that their actions will harm others …' (Owen 2014: 3). With the dominance of rational actor theories in conventional cyber crime scholarship, Latour's concept of agency as expressed in Actor-Network Theory represents a substantial ontological leap. Indeed perhaps this ontological dissonance in part explains why Brown's (2006a) criminology of hybrids—or, as elsewhere described, *virtual criminology* (Brown 2006b)—does not appear to have been widely adopted as a term in the international scholarship or, indeed, as a disciplinary sub-field. Furthermore, as Brown (2006b: 486) defines virtual criminology as one which 'places simulated and disembodied relations centre stage', we suggest the term itself and its definition invokes, even re-institutes, the very binary frame of real versus virtual that it seeks to disrupt. Nonetheless we take the sentiment of Brown's (2006a) challenge to criminology as a platform from which to launch into a broader exploration of how our conceptualisations of crime and justice in an increasingly 'digital society' might be further advanced by an associated and broadly cast field of *digital criminological* scholarship. The conventional scope of computer and cyber criminologies has arguably developed to the comparative neglect of a range of influences. These include the role of technologies in a widening range of offending and victimisation; recognising the increasingly embedded nature of online/offline experiences in crime and justice; the online victimisation of marginalised communities (such as on the basis of race, gender, and sexuality); broader issues of persistent social and digital inequalities as they relate to crime and justice; and rapidly emerging topics including online justice movements, digital vigilantism, and so-called 'open-source' policing or social network surveillance. Conversely, we suggest that these are appropriate issues of empirical analysis and theorisation for criminology and, as such, there is much to be gained by moving beyond a relatively siloed cyber-oriented criminology towards an exploration of the

broader implications of digital technologies as embedded in emerging *technosocial practices* that are shaping crime, deviance, criminalisation, and justice and community responses to crime in various ways.

Digital society and its implications for criminology

Criminology has not been alone in its desire to better understand the influence of diverse contemporary technosocial practices. A diverse range of explanations has been offered through interdisciplinary concepts such as the network society (Castells 1996), information society (Webster 1995), cyberculture (Levy 2001) and cybersociety (Jones 1994). Similar to the issues present in 'computer' and 'cyber crime' scholarship, many of these explanations have focused on a particular element of a technosocial shift to highlight or explain the causation of the change. Despite some limitations, a recurring theme amongst theories of technological advancement rests in establishing technologies as enabling (and disabling) rather than determining (Silverstone 1999: 21).

One way that criminology can account for the enabling and disabling effects of technologies is to conceptualise crime, deviance and justice as increasingly *technosocial practices* within a *digital society*. Gere (2002: 12) advocates the utility of digital as a 'marker of culture' that 'encompasses both the artefact and the systems of signification and communication that most clearly demarcate our contemporary way of life from others'. Key to the digital society then, is the recognition of a shift in structures, socio-cultural practices and lived experience that does not distinguish between the online and offline world. By focusing on the digital, Deuze (2006) contends that researchers can explore the impact of technologies that shape cultural artifacts, arrangements and activities, both online and offline. Extending the disintegration of the boundary between online and offline realities, Baym (2015: 1) notes that the distinguishing features of digital technologies are the manner in which they have transformed *how people engage* with one another. This enmeshment of the digital and social has also been referred to as the digitalisation of society in which 'technology is society, and society cannot be understood or represented without its technological tools' (Castells 1996: 5). By focusing on *digital* society, over other prefixes such as cyber or virtual, criminologists are prompted to move beyond framing 'computer', 'cyber' or 'virtual' crime and justice as fundamentally distinct from or, indeed, oppositional to 'non-technological' forms of crime and justice. At the same time, encouraging research under the more pervasive concept of digital *society* draws the criminological imagination towards an exploration of the relational, cultural, affective, political and socio-structural dimensions of crime and justice that are reproduced, reinstitutionalised and potentially resisted, in both familiar and unfamiliar ways. Indeed, part of our motivation for using digital 'society', over other similar and popular suffixes such as 'age' or 'era', is to deliberately invoke analyses of social inequalities, socio-cultural practices and socio-political factors that underpin crime and justice more broadly, and that arguably persist as our lives become increasingly digital. We propose that such a conceptual focus on *digital society* also opens up several new and rapidly emerging foci for criminological theory and research. Although far from being a comprehensive list, we identify seven avenues for the study of crime, deviance and justice in a digital society, drawing on examples from interdisciplinary research across sociology, cultural and media studies, journalism, policing and surveillance studies, as well as law and criminology.

Digital spectatorship

Just as traditional media and crime scholarship have highlighted tendencies for crime media consumers to be more punitive in their attitudes towards crime and justice, there is also potential for technological advancements to increase the immersion of crime news in our daily lives to be associated with an amplification of 'penal populism' (see Quilter 2012). The potential for increased spectatorship is itself facilitated in large part by the Internet of things and social media as well as our 'perpetual contact' via wearable technologies that provide live access to crime and justice news as events unfold. The capacity to follow 'crime in real time' has further implications

with respect to intensifying misperceptions and fear of crime, as well as calling on everyday citizens to more actively participate in crime news as eye-witnesses and citizen journalists (see Allan 2013).

Digital engagement

Expanding beyond cultural criminology and media-crime scholarship, the portability, ubiquity and perpetual contact of digital technologies allow the public to adopt new 'gatewatching' roles (Bruns 2003, 2005). In accessing a diverse variety of media content available to them, publics are now able to (re)consume, (re)produce, and (re)publish through digital technologies that offer new opportunities for criminologists to explore (Bruns 2003, 2005). These opportunities lie across a variety of platforms such as social media (Facebook, Twitter, Instagram), traditional media source (television, radio, print), and online media sources (news websites, blogs, Reddit). One example can be found in Milivojevic and McGovern's (2014) analysis of Facebook users' responses to Melbourne woman Jill Meagher's assault and murder in which they identify disruptive narratives from the public that shifted the traditional media's all-too familiar and predictable victim-blaming tropes to provide a counter-frame that re-focused the emphasis towards men's violence against women.

Digital investigation and evidence

Digital technologies offer opportunities for a range of actors to explore and investigate criminal behaviour in both online and offline settings. Data that have been stored or transmitted on digital devices are increasingly and readily used to explore theories of how offences occurred or to assist in developing other elements of offences such as providing an alibi or proving intent (Casey 2011: 7). Emergent in the discussion of digital evidence is the utility of technologies other than the personal computers such as mobile, personal and wearable devices that expand the repertoire of investigators and traditional law enforcement agencies (Chaikin 2006). For example, wearable fitness technologies have been introduced as evidence in criminal trials to identify the location of key figures at the time of the crime (Rutkin 2015; Gottehrer 2015). Importantly, digital evidence is collected and used in different ways that require a greater understanding of the investigation process. Digital investigations raise new and important questions about how evidence is collected, retained and regulated in relation to privacy and individual liberties (Kerr 2005: 280). For example, where online platforms such as Facebook provide government agencies with new opportunities for investigation, the monitoring and policing of them can represent a form of surveillance creep (Trottier 2014: 79). This was evident during the 2011 Vancouver riot, where police and Facebook users drew on posted content and collaborated to identify suspected rioters (Trottier 2014).

Digital justice and 'digilantism'

The democratisation effect of digital technologies has enabled state agencies to engage with the public in ways that were previously unavailable. The use of social media by police (Goldsmith 2015; McGovern and Lee 2012) and the courts (Johnston and McGovern 2013; McGovern 2011) both encourage access and engagement with the justice system, whilst also causing problematic and potential disruptive effects on traditional justice process such as the involvement of juries in the court system (Aaronson and Patterson 2012; Browning 2014). At the same time, the digital society has also encouraged 'informal' justice practices and community responses in relation to crime. For example, Corien Prins (2011) has advocated for a sub-field of *e-victimology* exploring how digital participation facilitates new practices for self-help and self-activism, as well as the increased potential for threats to victims' well-being and privacy. Similarly, Anastasia Powell (2014, 2015) and Bianca Fileborn (2014) have examined emerging 'informal justice' practices of victim-survivors and their advocates in response to sexual violence and street harassment operating in civil society. Meanwhile, some scholars have also raised concerns surrounding informal justice processes embracing the use of technologies, highlighting the potential for a digital media 'pillory' (see Hess and Waller 2014), and 'digilantism' (see Van Laer and Van Aelst

2013) whereby digital vigilantism can result in injustices, harassment and violence towards alleged offenders. Also labelled 'viral justice' (Aikins 2013; Antoniades 2012; Thompson, Wood and Rose 2016), such analyses suggest a need to further examine the nature and impacts of citizen-led justice practices that are enabled by digital participation.

Digital surveillance

Digital technologies enhance opportunities for state-sanctioned surveillance to occur. From this has emerged increasing sociological and criminological critiques of the powers that are enabled by such technologies (Bauman and Lyon 2012; Lyon 2003; Graham and Wood 2003). Governments caught by judicial bodies in activities that have identified serious breaches of privacy, due process and individual liberties have further intensifying the critique of these programs (Bauman et al. 2014; Margulies 2013). As the opportunities for criminologists to explore digital technologies and surveillance expand, so too has the pervasive nature of counter-surveillances through a digital evolution developed whereby agents of power within criminal justice systems are increasingly tracked, documented and held accountable for their actions and responsibilities (Bradshaw 2013; Marx 2003; McGrath 2004). In addition to surveillance of the powerful, the digital society allows for peer-to-peer or lateral digital surveillance which monitors crime from collectives rather than from positions of privilege (Smyth 2012; Trottier 2012). For example, 'crowdsourced surveillance' represents a 'socio-technical assemblage' of citizens, policing and private institutions that allows for criminological investigation in the relationship to between these technologies and responses to and prevention of crime (Trottier 2014: 81).

Digital space and embodied harms

A growing body of literature is exploring issues of spatiality and embodiment as they relate specifically to the harms of gendered and sexual violence (see Henry and Powell 2015), as well as racial, sexuality and/or gender-identity based hate (Awan and Zempi 2016; Citron 2014; Mann, Sutton and Tuffin 2003). The harassment, forms of violence and hate speech experienced by such groups take place not only via digital communications but also in a specific context of broader patterns of violence and abuse that persist and are perpetuated by cultures and structures of inequality, marginalisation and exclusion. 'Cyber' versus 'real' harassment, violence and hate speech typologies can serve to minimise harms enabled by communications and online technologies. Nevertheless, understanding these harms situated in digital society arguably better captures the lived experiences of marginalised communities and the operation of power, inequalities and violence across every aspect of their daily lives.

Digital social inequalities

Threaded throughout each of the above potential foci of criminological research are persistent themes of social inequalities such as the intersections of race, class, gender and sexuality. While sociological, political and technology studies have continued to theorise the nature of 'digital social inequality' (see Gilbert 2010; Halford and Savage 2010; Orton-Johnson and Prior 2013), such examinations are arguably under-developed in criminology. Yet both equity of access and equity of participation are increasingly important issues not only in society more broadly, but also with implications for crime and justice. While unequal technosocial relations may be facilitating new practices and cultures of particularly racial and gender-based harms (Mann, Sutton and Tuffin 2003; Powell and Henry 2016), importantly, the capacity of and nature of resistance to these harms and to broader racial and gender inequalities have arguably been changed by digital communications in significant ways. The ability for marginalised communities to 'watch the watchers', to share video evidence of private abuses and police brutality, to organise via both tweets and streets protests against continued racial and gender inequalities are not merely technological shifts but, rather, have enabled invigoration of social justice movements in a broader political context of disenchantment. Understanding the nature, impacts and justice movements of digital-social inequalities is thus a further crucial research topic within a digital criminology.

Conclusion: Towards a scholarship of 'digital criminology'

In an edited collected titled *What is Criminology?* (Bosworth and Hoyle 2011), David Garland argues that, to the detriment of our discipline, criminology is losing its dialogic nature of cross-disciplinary engagement and needs to be regularly infused with empirical and theoretical innovation from the outside. In large part, our argument in this article is that criminological engagement with computer and cyber crime has, to date, been likewise largely insular; and lacking in a critical and interdisciplinary engagement with disciplines such as sociology, computer science, politics, journalism, and media and cultural studies. This, we suggest, is particularly detrimental to advancing a new generation of scholarship concerning technology, crime, deviance and justice in our digital age.

The avenues for digital criminological research presented here are intended both to encompass and to expand substantially the traditional focus of computer and cyber crime scholarship. At the same time, they represent an enticement and a provocation for continued development of the field. While there are many social and technological theoretical frameworks and disciplinary influences that may invigorate criminological research, what underlies many of them is a fundamental recognition that the influences of technology on contemporary crime and justice cannot be understood either as mere tools or as operating in a separate sphere of our experience. Rather, here we have deployed the concept of 'digital society' to emphasise the embedded nature of technology in our lived experiences of criminality, victimisation and justice; the emergence of new technosocial practices of both crime and justice; and the continued relevance of social, cultural and critical theories of society in understanding and responding to crime in a digital age. As such, 'digital criminology' refers to the rapidly developing field of scholarship that applies criminological, social, cultural and technical theory and methods to the study of crime, deviance and justice in a digital society. Rather than necessarily a sub-discipline *per se*, we advocate that digital criminology may provide a fruitful platform from which to expand the boundaries of contemporary criminological theory and research. Our intention is to foster a broader and ongoing conversation within the discipline that cuts across technology, sociality, crime, deviance and justice; and to inspire new conceptual and empirical directions.

Correspondence: Dr Greg Stratton, Lecturer, Justice and Legal, School of Global, Urban and Social Studies, 411 Swanston Street, Melbourne VIC 3000, Australia.
Email: gregory.stratton@rmit.edu.au

[1] This research was funded by the Australian Government through an Australian Research Council, Discovery Early Career Researcher Award (DE160100044) awarded to Dr Anastasia Powell. The views expressed herein are those of the authors and are not necessarily those of the Australian Government or Australian Research Council.

[2] Personal computing workstations, such as the Xerox Alto in 1973, the Sun 1 in 1982, and the Apple Macintosh 128k in 1984, can be differentiated from the centralised, stationary and ponderous early computers (see Goldberg 1988). These personal computing workstations were also among the first to use a graphical user interface, which did not require specific knowledge of command-line programming, and thus radically opened up computing to individual users both through portability and ease of use (Goldberg 1988).

[3] 'Happy slapping' refers to a meme originating in the UK as early as 2004 whereby an individual or group of teens or young adults would film what were typically minor assaults (such as slapping or hitting a victim), and then post the recordings online. The assaults range from a literal slap, to sexual assault, and even murder (see Ching et al. 2012; Saunders, 2005).

References

Aaronson DE and Patterson SM (2012) Modernizing jury instructions in the age of social media. *Criminal Justice* 27(4): 26-35. Available at

http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1233&context=facsch_lawrev (accessed 10 May 2017).

Aas KF (2007) Beyond the desert of the real: Crime control in a virtual(ised) reality. In Jewkes Y (ed.) *Crime Online*: 160-177. Portland, Oregon: Willan Publishing.

Aikins M (2013) Viral justice. *The New York Times,* 28 June. Available at http://latitude.blogs.nytimes.com/2013/06/28/viral-justice/ (accessed 19 March 2017).

Allan S (2013) *Citizen Witnessing: Revisioning Journalism in Times of Crisis. Key Concepts in Journalism*. Cambridge, England: Polity.

Antoniades A (2012) Viral justice: Domestic abuse victim calls out attacker on Facebook. *Takepart,* 14 September. Available at http://www.takepart.com/article/2012/12/14/viral-justice-domestic-abuse-victim-calls-out-attacker-facebook (accessed 14 December 2017).

Armagh DS (2001) Virtual child pornography: Criminal conduct or protected speech. *Cardozo Law Review* 23(6): 1993-2010.

Awan I and Zempi I (2016) The affinity between online and offline anti-Muslim hate crime: dynamics and impacts. *Aggression and Violent Behavior* 27(March-April): 1-8. DOI: 10.1016/j.avb.2016.02.001.

Bauman Z and Lyon D (2012) *Liquid Surveillance: A Conversation*. Cambridge, England: Polity.

Bauman Z, Bigo D, Esteves P, Guild E, Jabri V, Lyon D and Walker RB (2014) After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8(2): 121-144. DOI: 10.1111/ips.12048.

Baym NK (2015) *Personal Connections in the Digital Age*. Cambridge, England: Polity.

Beck U and Beck-Gernsheim E (2002) *Individualization: Institutionalized Individualism and its Social and Political Consequences*. London: Sage. Available at http://ebookcentral.proquest.com.ezp01.library.qut.edu.au/lib/qut/detail.action?docID=254692 (accessed 19 March 2017).

Bergman MK (2001) White paper—The deep web: Surfacing hidden value. *Journal of Electronic Publishing* 7(1). DOI: 10.3998/3336451.0007.104.

Berk R (2008) How you can tell if the simulations in computational criminology are any good. *Journal of Experimental Criminology* 4(3): 289-308. DOI: 10.1007/s11292-008-9053-5.

Birks D, Townsley M and Stewart A (2012) Generative explanations of crime: Using simulation to test criminological theory. *Criminology* 50(1): 221-254. DOI: 10.1111/j.1745-9125.2011.00258.x.

Bradshaw EA (2013) This is what a police state looks like: Sousveillance, direct action and the anti-corporate globalization movement. *Critical Criminology* 21(4): 447-461. DOI: 10.1007/s10612-013-9205-4.

Brantingham PL (2011) Computational criminology. Keynote address to the *European Intelligence and Security Informatics Conference*, 12-14 September. Athens, Greece: IEEE Computer Society.

Brown S (2006a) The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology* 10(2): 223-244. DOI: 10.1177/1362480606063140.

Brown S (2006b) Virtual criminology. In McLaughlin E and Muncie J (eds) *The Sage Dictionary of Criminology*: 224-258. London: Sage.

Browning JG (2014) Should voir dire become voir Google? Ethical implications of researching jurors on social media. *SMU Science and Technology Law Review* 17(4): 603-629.

Bruns A (2003) Gatewatching, not gatekeeping: Collaborative online news. *Media International Australia Incorporating Culture and Policy* 107(1) 31-44. DOI: 10.1177/1329878X0310700106.

Bruns A (2005) *Gatewatching: Collaborative Online News Production*. New York: Peter Lang.

Bosworth M and Hoyle C (2011) *What is Criminology?* Oxford, England: Oxford University Press.

Casey E (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Cambridge, England: Academic Press.

Castells M (1996) *The Rise of the Network Society*. Oxford, England: Blackwell.

Castells M (2001) *The Internet Galaxy*. Oxford, England: Oxford University Press.

Ceruzzi PE (2003) *A History of Modern Computing*. Cambridge, Massachusetts: MIT Press.

Chaikin D (2006) Network investigations of cyber attacks: The limits of digital evidence. *Crime, Law and Social Change* 46(4-5): 239-256. DOI: 10.1007/s10611-007-9058-4.

Chan J and Bennett Moses L (2016) Is big data challenging criminology? *Theoretical Criminology* 20(1): 21-39. DOI: 10.1177/1362480615586614.

Ching H, Daffern M and Thomas S (2012) Appetitive violence: A new phenomenon? *Psychiatry, Psychology and Law* 19(5): 745-763. DOI: 10.1080/13218719.2011.623338.

Citron DK (2014). *Hate Crimes in Cyberspace*. Cambridge, Massachusetts. Harvard University Press.

Clough B and Mungo P (1992) *Approaching Zero: Data Crime and the Computer Underworld*. London: Faber & Faber.

Cohen LE and Felson M (1979) Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44(4): 588-608.

Croall H (1992) *White Collar Crime: Criminal Justice and Criminology*. Bristol, England: Open University Press.

Décary-Hétu D and Dupont B (2012) The social network of hackers. *Global Crime* 13(3): 160-175. DOI: 10.1080/17440572.2012.702523.

Deuze M (2006) Participation, remediation, bricolage: Considering principal components of a digital culture. *The Information Society* 22(2): 63-75. DOI: 10.1080/01972240600567170.

Diamond B and Bachmann M (2015) Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology* 9(1): 24-34. DOI: 10.5281/zenodo.22196.

Esposito LC (1998) Regulating the Internet: The new battle against child pornography. *Case Western Reserve Journal of International Law* 30(2/3): 541-564.

Fileborn B (2014) Online activism and street harassment: Digital justice or shouting into the ether? *Griffith Journal of Law & Human Dignity* 2(1): 32-51.

Garland D (2011) Criminology's place in the academic field. In Bosworth M and Hoyle C (eds) *What is Criminology?*: 298-317. Oxford, England: Oxford University Press.

Gere C (2002) *Digital Culture*. London: Reaktion Books.

Giddens A (1991) *Modernity and Self-identity: Self and Society in the Late Modern Age*. Stanford, California: Stanford University Press.

Gilbert M (2010) Theorizing digital and urban inequalities: Critical geographies of 'race', gender and technological capital. *Information, Communication & Society* 13(7): 1000-1018. DOI: 10.1080/1369118X.2010.499954.

Goldberg A (ed.) (1988) *A History of Personal Workstations*. New York: ACM Press.

Goldsmith A (2015) Disgracebook policing: Social media and the rise of police indiscretion. *Policing and Society* 25(3): 249-267. DOI: 10.1080/10439463.2013.864653.

Gottehrer G (2015) Connected discovery: What the ubiquity of digital evidence means for lawyers and litigation. *Richmond Journal of Law & Technology* 22(3): 1-27. Available at http://jolt.richmond.edu/2016/04/01/connected-discovery-what-the-ubiquity-of-digital-evidence-means-for-lawyers-and-litigation/ (accessed 10 May 2017).

Grabosky PN (2001) Virtual criminality: Old wine in new bottles? *Social & Legal Studies* 10(2): 243-249.

Grabosky PN and Smith RG (1998) *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities.* Sydney, New South Wales: Federation Press.

Graham S and Wood D (2003) Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy* 23(2): 227-248. DOI: 10.1177/0261018303023002006.

Greenleaf G (1990) Computers and crime-the hacker's new rules. *Computer Law & Security Review* 6(2): 21-22.

Griffith DS (1990) The Computer Fraud and Abuse Act of 1986: A measured response to a growing problem. *Vanderbilt Law Review* 43(2): 453-490.

Halder D and Jaishankar K (2012) *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations*. Hershey, Pennsylvania: IGI Global.

Halford S and Savage M (2010) Reconceptualizing digital social inequality. *Information, Communication & Society* 13(7): 937-955. DOI: 10.1080/1369118X.2010.499956.

Haraway D (1985) A manifesto for cyborgs: Science, technology and socialist feminism in the 1980s. *Socialist Review* 15(2): 65–107. DOI: 10.1080/08164649.1987.9961538.

Haraway D (1991) *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.

Hayward KJ (2012) Five spaces of cultural criminology. *British Journal of Criminology* 52(3): 441-462. DOI: 10.1093/bjc/azs008.

Henry N and Powell A (2015) Embodied harms gender, shame, and technology-facilitated sexual violence. *Violence Against Women* 21(6): 758-779. DOI: 10.1177/1077801215576581.

Hess K and Waller L (2014) The digital pillory: Media shaming of 'ordinary' people for minor crimes. *Continuum* 28(1): 101-111. DOI: 10.1080/10304312.2013.854868.

Hollinger RC and Lanza-Kaduce L (1988) The process of criminalization: The case of computer crime laws. *Criminology* 26(1): 101-126. DOI: 10.1111/j.1745-9125.1988.tb00834.x.

Holt TJ (ed.) (2011) *Crime On-line: Causes, Correlates and Context*. Durham, England: Carolina Academic Press.

Holt TJ (2013) Examining the forces shaping cybercrime markets online. *Social Science Computer Review* 31(2): 165-177. DOI: 10.1177/0894439312452998.

Holt TJ and Bossler AM (2008) Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior* 30(1): 1-25. DOI: 10.1080/01639620701876577.

Holt TJ and Bossler AM (2014) An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35(1): 20-40. DOI: 10.1080/01639625.2013.822209.

Holt TJ and Bossler AM (2015) *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses*. New York: Routledge.

Hutchings A and Hayes H (2008) Routine activity theory and phishing victimisation: Who gets caught in the 'net'? *Current Issues in Criminal Justice* 20(3): 433-452. Available at https://www.cl.cam.ac.uk/~ah793/papers/2009Routineactivitytheoryandphishingvictimisation.pdf (accessed 10 May 2017).

Jaishankar K (2008) Space transition theory of cyber crimes. In Schmallager F and Pittaro M (eds) *Crimes of the Internet*: 283-301. New Jersey: Prentice Hall.

Jaishankar K (ed.) (2011) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, Florida: CRC Press.

Jewkes Y (ed.) (2007) *Crime Online*. Cullompton, England: Willan.

Jewkes Y and Yar M (2010) The Internet, cybercrime and the challenges of the twenty-first century. In Jewkes Y and Yar M (eds) *Handbook of Internet Crime*: 1-8. Devon, England: Willan Publishing.

Jewkes Y and Yar M (eds) (2013) *Handbook of Internet Crime* (2nd edn). London: Routledge.

Johnston J and McGovern A (2013) Communicating justice: A comparison of courts and police use of contemporary media. *International Journal of Communication* 7: 1667–1687. Available at http://ijoc.org/index.php/ijoc/article/view/2029 (accessed 10 May 2017).

Jones S (1994) *Cybersociety: Computer-mediated Communication and Community*. Thousand Oaks, California: Sage.

Kerr OS (2005) Digital evidence and the new criminal procedure. *Columbia Law Review* 105(1): 279-318.

Kling R (1980) Computer abuse and computer crime as organizational activities. *Computer Law Journal* 2(1): 403-427. Available at http://repository.jmls.edu/cgi/viewcontent.cgi?article=1608&context=jitpl (accessed 10 May 2017).

Lash S (2002) *Critique of Information*. London: Sage.

Latour B (1993) *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.

Latour B (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press.

Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, Lynch DC, Postel J, Roberts LG, and Wolff S (2009) A brief history of the Internet. *ACM SIGCOMM Computer Communication Review* 39(5): 22-31. Available at http://www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf (accessed 10 May 2017).

Lévy P (2001) *Cyberculture*. Minneapolis, Minnesota: University of Minnesota Press.

Lupton D (2014) *Digital Sociology*. London: Routledge.

Lyon D (2003) Surveillance as social sorting: Computer codes and mobile bodies. In Lyon D (ed.) *Surveillance as Social Sorting*: *Privacy, Risk and Digital Discrimination*: 13-30. London and New York: Routledge.

Mann D, Sutton M and Tuffin R (2003) The evolution of hate. Social dynamics in white racist newsgroups. *Internet Journal of Criminology* 1: 1-32. Available at http://irep.ntu.ac.uk/id/eprint/10080/ (accessed 10 May 2017).

Margulies P (2013) NSA in global perspective: Surveillance, human rights, and international counterterrorism. *The Fordham Law Review* 82(5): 2137-2167. Available at http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4980&context=flr (accessed 10 May 2017).

Martin J (2014) Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice* 14(3): 351-367. DOI: 10.1177/1748895813505234.

Marx GT (2003) A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues* 59(2): 369-390. DOI: 10.1111/1540-4560.00069.

McGrath JE (2004) *Loving Big Brother: Performance, Privacy and Surveillance Space*. Abingdon, England: Psychology Press.

McGovern A (2011) Tweeting the news: Criminal justice agencies and their use of social networking sites. *The Australian and New Zealand Critical Criminology Conference Proceedings 2010*: 1-6. Sydney, New South Wales: University of Sydney, Institute of Criminology. Available at https://ses.library.usyd.edu.au/handle/2123/7378 (accessed 10 May 2017).

McGovern A and Lee M (2012) Police communications in the social media age. In Keyzer P, Johnston J and Pearson M (eds) *The Courts and the Media: Challenges in the Era of Digital and Social Media*: 160-174. Ultimo: Halstead Press.

Milivojevic S and McGovern A (2014) The death of Jill Meagher: Crime and punishment on social media. *International Journal for Crime, Justice and Social Democracy* 3(3): 22-39. DOI: 10.5204/ijcjsd.v3i2.144.

Mitchell KJ, Finkelhor D, Jones LM and Wolak J (2010) Growth and change in undercover online child exploitation investigations, 2000–2006. *Policing & Society* 20(4): 416-431. DOI: 10.1080/10439463.2010.523113.

Montgomery J (1986) Computer crime. *American Criminal Law Review* 24(3): 429-438.

Orton-Johnson K and Prior N (eds) (2013) *Digital Sociology: Critical Perspectives*. Hampshire, England: Springer.

Owen T (2014) *Criminological Theory: A Genetic-social Approach*. London: Palgrave.

Owen T and Owen J (2015) Virtual criminology: Insights from genetic-social science and Heidegger. *Journal of Theoretical and Philosophical Criminology* 7(1):17-31.

Pittaro ML (2007) Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology* 1(2): 180-197. Available at http://www.cybercrimejournal.com/pittaroijccvol1is2.htm (accessed 10 May 2017).

Powell A (2014) Pursuing justice online: Citizen participation in justice via social media. In West B (ed.) *Refereed Proceedings of The Australian Sociological Association Conference: Challenging Identities, Institutions and Communities*, 24-27 November. Adelaide, South Australia: University of South Australia.

Powell A (2015) Seeking rape justice: Formal and informal responses to sexual violence through technosocial counter-publics. *Theoretical Criminology* 19(4): 571-588. DOI: 10.1177/1362480615576271.

Powell A and Henry N (2016) Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives. *Policing and Society*: Epub ahead of print 8 March. DOI: 10.1080/10439463.2016.1154964.

Prins C (2011) Digital tools: Risks and opportunities for victims: Explorations in e-victimology. In Letschert R and Van Dijk J (eds) *The New Faces of Victimhood. Globalization, Transnational Crimes and Victim Rights*: 215-230. Netherlands: Springer.

Pyrooz DC, Decker SH and Moule Jr RK (2015) Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly* 32(3): 471-499. DOI: 10.1080/07418825.2013.778326.

Quilter J (2012) Responses to the death of Thomas Kelly: Taking populism seriously. *Current Issues in Criminal Justice* 24(3): 439-448. Available at http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1412&context=lhapapers (accessed 10 May 2017).

Reyns BW, Henson B and Fisher BS (2011) Being pursued online applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior* 38(11): 1149-1169. DOI: 10.1177/0093854811421448.

Rutkin A (2015) It's a Fitbit, Your Honour. *New Scientist* 225(3002): 17. DOI: 10.1016/S0262-4079(15)60024-0.

Saunders R (2005) Happy slapping: Transatlantic contagion or home-grown, mass-mediated nihilism? *Static* 1: 1–11. Available at http://www.observatorioperu.com/2012/mayo/web-saunders_happyslapping.pdf (accessed 10 May 2017).

Sieber U (1986) *The International Handbook on Computer Crime*. Chichester, England: Wiley.

Silverstone R (1999) *Why Study the Media*? London: Sage.

Smith R, Grabosky P and Urbas G (2004) *Cyber Criminals on Trial.* Cambridge, England: Cambridge University Press.

Smyth SM (2012) The new social media paradox: A symbol of self-determination or a boon for big brother? *International Journal of Cyber Criminology.* 6(1): 924–950. DOI: 10.2139/ssrn.2122939.

Spitzberg BH and Hoobler G (2002) Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society* 4(1): 71-92. DOI: 10.1177/14614440222226271.

Surette R (2015) Performance crime and justice. *Current Issues in Criminal Justice* 27(2): 195-216. Available at http://www.austlii.edu.au/au/journals/CICrimJust/2015/21.html (accessed 10 May 2017).

Sutton M (2002) Race hatred and the far right on the Internet. *Criminal Justice Matters* 48(1): 26-27. DOI: 10.1080/09627250208553450.

Thomas D and Loader B (eds) (2000) *Cyber Crime: Law Enforcement, Security and Surveillance in the Information Age.* London: Routledge.

Thompson C, Wood M and Rose E (2016) Viral justice: Survivor selfies, Internet virality and justice for victims of intimate partner violence. Paper presented at *British Society of Criminology 2016 Conference: Inequalities in a Diverse World,* 6- 8 July 2016. Nottingham, England: British Society of Criminology.

Trottier D (2012) *Social Media As Surveillance: Rethinking Visibility in a Converging World*. Surrey, England: Ashgate.

Trottier D (2014) Police and user-led investigations on social media. *Journal of Law, Information & Science* 23(1): 75-96. Available at http://www.austlii.edu.au/au/journals/JlLawInfoSci/2014/4.html (accessed 10 May 2017).

Van Laer J and Van Aelst P (2009) Cyber-protest and civil society: The Internet and action repertoires of social movements. In Jewkes Y and Yar M (eds) *Handbook of Internet Crime*: 230-254. Portland, Oregon: Willan Publishing.

Wall D (1997) Policing the virtual community: The Internet, cyberspace and cyber-crime. In Francis P, Davies P and Jupp V (eds) *Policing Futures*: 208-236. Hampshire, England: Palgrave.

Wall D (2001) Cybercrimes and the Internet. In Wall D (ed.) *Crime and the Internet*: 1-17. New York: Routledge.

Wasik M (1991) *Crime and the Computer.* Oxford, England: Clarendon Press.

Webster F (1995) *Theories of the Information Society*. London: Routledge.

Weimann G (2016) Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism* 39(3), 195-206. DOI: 10.1080/1057610X.2015.1119546.

Westlake BG and Bouchard M (2016) Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social Science Research* 59 (September): 23-36. DOI: 10.1016/j.ssresearch.2016.04.010.

Williams MR (1997) *A History of Computing Technology*. Los Alamitos, California: IEEE Computer Society Press.

Wood MA (2016) Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's technological unconscious. *Theoretical Criminology* 21(2): 1-18. DOI: 10.1177/1362480616643382.

Yar M (2005) The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology 2*(4): 407-427. DOI: 10.1177/147737080556056.

Yar M (2012) Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture* 8(3): 245-260. DOI: 10.1177/1741659012443227.

Yip M, Webber C and Shadbolt N (2013) Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society* 23(4): 516-539. DOI: 10.1080/10439463.2013.780227.