Article

European Journal of Criminology

European Journal of Criminology
1–20
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1477370819887305
journals.sagepub.com/home/euc
SAGE

The seductions of cybercrime: Adolescence and the thrills of digital transgression

Andrew Goldsmith
Flinders University, Australia

David S. Wall
University of Leeds, UK

Abstract

This article offers a socio-technical framework for better understanding youthful attraction to, and engagement in, online transgressions and delinquencies. Specifically, it takes the concept of 'seduction' from the work of Katz, as well as 'affordance theory' and insights from software and human–computer interaction studies, to analyse the affordances of the Internet that tempt and invite youthful transgressions such as digital piracy, viewing illegal pornography and hacking. We argue that Internet affordances not only enable transgressions to occur but can also precipitate them. The implications for youth crime policy are briefly addressed. Policy needs to reckon with the power of these factors in adolescent lives and thus minimize reliance on punitive responses. The article also contributes to the development of the concept of digital drift, by showing how Internet features and affordances foster drift into cyber delinquency.

Keywords

Affordance, cybercrime, digital drift, Katz, seduction

Introduction

The public Internet has been with us for just 25 years (Castells, 2001). Yet, in this time, it has intrigued, engaged and seduced more than half the planet's population. It is estimated that almost 4.5 billion people are Internet users as at 30 June 2019 (Internet World Stats, 2019). Young people (under the age of 30) are more likely than older persons to have

Corresponding author:
Andrew Goldsmith, Centre for Crime Policy and Research, College of Business, Government and Law, Flinders University, GPO Box 2100, Adelaide, SA 5001, Australia.
Email: andrew.goldsmith@flinders.edu.au

access to and to spend extended time on the Internet, conducting searches, playing games and using social media (Eurostat, 2017). Its empowering possibilities have been much commented upon, just as its attractions for entertainment, leisure and distraction have also become more apparent and commercially valuable. Given its relative novelty and generally positive global reception, it is perhaps not surprising that some of its downsides have only recently started to emerge in the public arena (for example, Keen, 2012; McNamee, 2019; Zittrain, 2008) and to receive scholarly analysis. The profound salience of the Internet in the lives of many children and adolescents has triggered concern about cyber safety, such as its use by adults to exploit children and by some children to bully other children, as well as the detrimental effects on youth wellbeing from extended participation in online gaming and social media (Valkenburg and Pietrowski, 2017).

In this article, rather than looking at young people as victims of crime or as problematic Internet users (see Valkenburg and Pietrowski, 2017), we shall explore the Internet's significance in terms of turning adolescents, those from 12 to 19 years of age, towards offending. The commission of cyber-related crimes by 'normal' youth, we propose, is 'easy to do' and 'almost accidental' (Goldsmith and Brewer, 2015; Matza, 1964). 'Digital drift' (Goldsmith and Brewer, 2015), we shall argue, needs to be understood partly in terms of the features and affordances ('possibilities for action') of the Internet that amount to persuasive *technologies* that can make a variety of user applications 'irresistible' (Alter, 2017; Schull, 2012). Such conditions, we shall argue, make drift more powerful, sustained and difficult to reverse. In this article, we are specifically interested in the elements (features, affordances) of the Internet that render it a 'seductive swamp' (Vaidhyanathan, 2011), especially for adolescents, enabling and provoking transgressions and what have been called 'cyborg crimes' (Van der Wagen and Pieters, 2015) – crimes produced through the combination of human and computer agency. The agency of the latter, however, is often not visible or predictable, exhibiting what can be called a 'technological unconscious' (Wood, 2018: 79). Consequently, in interactions between individuals and these platforms, human foresight of outcomes is limited by the unpredictable composition, structure and operation of the Internet's architecture (Van der Wagen and Pieters, 2015: 592–3).

A second aim of this article is to consider the implications of this adolescent 'digital drift' for the development of sound policy. Given the heavy engagement among young people with various Internet platforms (social media, gaming, web searches), we need to do more than sharpen our awareness of the criminogenic implications of this 'swamp'. This awareness also needs to inform the development of appropriate regulatory responses that better target the drivers of these behaviours and that limit the punitiveness often seen in such cases (Long and Hopkins Burke, 2015; Wall, 2017). For example, hackers are found to be disproportionately very young and male (Hutchings and Chua, 2016). This aspect of 'youth' causes very practical problems for law in terms of prosecution and prevention that will be outlined later (Wall, 2017; Yar, 2005). Such concern is also found in other transgressive areas such as the use of pornographic imagery; see, for example, Quadara et al. (2017), who found that exposure to it can shape unsafe sexual practices and progressively strengthen attitudes that are supportive of violence.

In developing our position in relation to youth seduction and the Internet, we will draw upon Jack Katz's (1988) work on youth shoplifters and graffiti artists because it offers us some useful analogies for thinking about the connection between young people's emotional drives and the commission of crimes. Katz's stress upon the importance of foreground factors (emotions, situational cues, etc.) in understanding youth crime pushes us to consider the emotional needs and rewards linked with particular Internet applications, and how the Internet itself facilitates and intensifies, in some cases, motivations to transgress. His notion of 'sneaky thrills' points to the emotional rewards young offenders often derive from covert and even brazen criminal acts. Pursuing his idea of crime as seductive, we propose to break down the features of Internet engagement that contribute to 'sneaky thrills' and progression to online offending. We argue that the seductive features and affordances of the Internet are of such a nature that 'normally' perceived boundaries can blur to cause 'normally' non-deviant people to become deviant.

The focus on adolescence requires a brief note on the developmental characteristics of this group. According to Valkenburg and Pietrowski (2017: 94–5), this group is charged with three socio-emotional tasks: 'developing an identity, learning about intimacy, and discovering their sexuality.' Seeking information and validation, particularly through communication with peers, is important and a prevalent part of adolescent behaviour. An interest in extreme and risky content is common across the age range, but, as they progress through this period, a growing interest in personal autonomy and adult interests can also be observed. The pervasive uptake of social media and other Internet activities has been observed to enhance the ability and time spent by members of this age group in communication and on other adolescent preoccupations. In terms of transgressive potential, it is widely accepted that adolescence is a phase, especially for males, of greater *sensation-seeking*, that is, 'the tendency to seek out novel, varied, and highly stimulating experiences, and the willingness to take risks in order to attain them' (Steinberg et al., 2008: 1765). For much of adolescence there is also considerable evident *impulsivity*, limiting the individual youth's capacity for self-control (Forrest et al., 2019: 27).

A note on affordances and features: In order to understand what makes the Internet particularly seductive for young people, we need to consider the linkages between young people's desires and needs and the machine elements of Internet platforms. The relevant characteristics may be technical *features* (for example, hypothetically, 'Friending' on Facebook) that *afford* particular action possibilities (connecting with others) that respond to individual *needs*, such as autonomy, competence and relatedness (Deterding, 2011; Karahanna et al., 2018). In terms of the affordance literature, we propose a relational view of Internet seduction, looking at the 'routine activities enacted through engaging with the materiality of a technological artefact' (Wood, 2018: 81). Without digressing too far into the relevant literature, a couple of points can usefully be made. The first is to acknowledge that some affordances and features contribute to making use 'helpful, fun or aesthetically pleasing'; affordances of this kind are known as 'reception affordances' (Nahl, 2007: 2039). Secondly, the affordance literature also refers to 'motivational affordances' and 'situated motivational affordances'; the latter has been defined as the 'opportunities to satisfy motivational needs provided by the relation between the features of an artifact [here, the Internet] and the abilities of a subject in a given situation' (Deterding, 2011: 3). Motivational needs referred to here are those mentioned earlier: competence, autonomy and relatedness. In the third section ('The Internet as a seductive setting'), we develop the idea of affordances of seduction in some detail, relating it to what we know about youth motivations and desires.

We will then examine two forms of problematic online engagement. The first considers the link between involvement in Internet searches and participation in the world of online pornography. It examines how unanticipated or innocent encounters online with material of a legal pornographic nature can progress or 'drift' into consumption or even production of illegal pornography. The second looks at the motivations expressed by young participants engaged in hacking. It takes the lens of seduction to explore how features of the Internet exert an appeal to some young people to proceed from gaming and other online activities to hacking. In both cases, we focus on how the affordances invite as well as facilitate movement from unexceptionable, or at least unremarkable, online behaviour to cyber delinquency. Lastly, we discuss the implications of acknowledging the sensuality of youth cybercrime before revisiting the concept of digital drift and considering some implications for policy.

Seduction into crime

Seduction is linked to the power of particular *situations* to shape decisions and behaviour. Well before the advent of the Internet, Briar and Piliavin proposed the idea of 'situational inducements' that 'can evoke motives to deviate' (1965: 38). Within environmental criminology, Clarke observes that '[i]ndividuals without pre-existing dispositions [for crime] can be drawn into criminal behaviour by a proliferation of criminal opportunities' (2008: 179). Similarly, Wortley urges the need to acknowledge the 'precipitating role of immediate environments' in causing persons to commit crimes that '*they otherwise would not have contemplated at that time*' (2008: 64; emphasis added). As these comments indicate, situations can shape motivations through suggestion and intensification of feelings as well as provide opportunities for crime. These motivational influences, we will demonstrate, exist in online as well as offline environments.

This focus is shared in Katz's work on the seductions of crime. Although seduction as a concept is invoked in order to explore offline delinquency, Katz encourages researchers to pay attention to the individual's journey between the sense of the self as subject and as object, between 'being in and out of control, between directing and being directed by the dynamics of the situation' (1988: 8). Almost presciently in light of the coming of the Internet era, he observed that, through an experiential immersion in certain settings, 'an individual can genuinely experience a new or different world' (Katz, 1988: 8). The emotional pull of particular settings has to be acknowledged as raising the prospects for transgression, he suggests. In the cyber realm, deep immersion in online activities such as gaming and social media is widely noted as commonplace (Presdee, 2000; Wall, 2007) and sometimes problematic (Schaffer and Fang, 2018).

Seduction in offline youth offending

The Oxford Dictionary tells us that seduction is the act of tempting or enticing another into an act of wrongdoing, or at least of leading another person astray (Oxford Dictionary, 2017).[1] It imports concepts of attraction, vulnerability, submission and transgression.

There is a strong sexual as well as romantic connotation in many uses of the term. It also suggests enchantment, of being ‘both caught up and carried away’ by a person or experience (Bennett, 2001: 5). Within his broader account of crime as seductive, the concept of ‘sneaky thrills’ is used by Katz to explain some of the key motivational influences in youth participation in shoplifting and vandalism. This term refers to the thrilling sense of anticipation of committing a crime such as shop theft, the surge of sometimes conflicting emotions during the criminal act, and the exhilaration felt afterwards from successfully executing these crimes. Katz describes the movement towards committing the criminal act in terms of ‘flirtation’, in which the individual finds him- or herself in ‘magical environments’ or an ‘enchanted land’. These settings are experienced in part as invitational, suggesting to the individual knowledge of what the individual needs or wants to do (Katz, 1988: 56). In some cases, the physical settings can elicit hidden or previously unknown desires in the participants, encouraging transgression; in other words, they exercise seductive effects (also see Wortley, 2008).

A number of situational characteristics supported examples of seduction in Katz’s study. Material abundance within easy reach was one. Some of Katz’s young respondents indicated that, while browsing in stores, they realized ‘it would be so easy’ to take an item and, perhaps even, to leave the store without detection. Katz observes that in such settings they can explore their ‘secret, inner desire to be deviant’ while facing only a small chance of being detected (1988: 58). For adolescents involved in shoplifting or vandalism, Katz proposes, the distinctive allure of property crimes can be located in the ‘dialectic of being privately deviant in public places’ (1988: 77).

The opportunity presented by certain situations to demonstrate personal competence can be very appealing for young people. For Katz, the euphoria often reported by young people after committing such crimes could be linked to their ‘abilities to obscure areas of routine personal incompetence’ (1988: 77). The sense of mastery they experience means that these crimes are more often ‘emotionally compelling’ than ‘materially necessary’ (Katz, 1988: 78). This sense, we shall see, is also highly valued among young computer hackers (Steinmetz, 2016; Turgeman-Goldschmidt, 2005). Positive feelings from accomplishment tend to reinforce those new behaviours: ‘If nothing succeeds like success, nothing also entraps like success’ (Hans Jonas, quoted in Simanowski, 2016: 29).

Katz reminds us therefore that the features of some offline settings can both interest and propel youth in the commission of crime. The affective domain is often more important in shaping these decisions than the cognitive, ‘rational’ domain. The ability to act undiscovered and to ‘get away with things’, the so-called ‘sneaky thrills’, is a strong motivator for many young people. By implication, Katz directs us to look at the Internet settings in terms of how they can meet similar emotional needs and how they can shape desires to transgress. The young offender’s ‘sensual concentration on the boundary between the self as known from within and as seen from without’ (Katz, 1988: 58) points us to consider the identity-shaping drives and affordances to be found and exploited on the Internet.

The Internet as a seductive setting

Memorably, as noted earlier, the Internet has been described as a ‘seductive swamp’ (Vaidhyanathan, 2011: 55). This description evokes images of an environment very attractive to enter, yet also reluctant to release those who enter it. Some at least of the seductive features of new technologies have already been featured in popular culture. The 2013 Spike Jonze film *Her* portrays the course of a romantic relationship between an actual person (a man, Theodore) and an 'intelligent assistant' by the name of Samantha (a kind of futuristic Google Siri). In addition to showing a deepening intimacy between a man and a machine, the film vividly captures the 'invitational' nature of such devices, as well as the growing emotional dependency of the former upon the latter (see Finn, 2017: 77–85). Also of a seductive character, there is something deeply confessional and intimate in the way many people relate to the Google search engine (the gateway to the Internet for many users). As Stephens-Davidowitz notes, 'people sometimes don't so much query Google as confide in it . . . people tell the giant search engine things that they may not tell anyone else' (Stephens-Davidowitz, 2017: 4–5).

For many young people, it has been suggested the Internet offers them a 'second life' (Wall, 2007: 22; Presdee, 2000), a place where they can leave their 'first lives' for a while in order to have fun and transgress social norms. The Internet has become a '"safe site" of the second life of the people' 'where we can enjoy in private immoral acts and emotions' (Presdee, 2000: 64). Transgression is enabled in the idea of the 'ambivalent Internet' (Phillips and Milner, 2017). On this account, the Internet 'collapses and complicates binaries' and 'call[s] attention to socially constructed distinctions between "normal" and "aberrant"' (Phillips and Milner, 2017: 12–13). By drawing attention to boundaries, and inviting participants to test, even breach, them, the Internet can be said to operate in a seductive fashion.

Technologies of digital seduction

In this section, we attempt to set out some distinct affordances and other technical features of the Internet that contribute to its seductive influence upon many young people. As proposed earlier, the 'possibilities for action' (affordances) need also to bring into view the technical features and emotional needs of users that also help to show the Internet's seductive side. The literature has already begun to identify relevant affordances in the context of cyber deviance and cybercrime. In relation to cybersex addiction, Cooper (2000) proposed three as particularly significant: its *accessibility*, its *affordability*, and its *anonymity.* As he comments:

> [These features] combine to turbo-charge (i.e., accelerate and intensify) online sexual interactions. Flirtation and innuendo, long the staples of leisurely seduction, rapidly escalate into frank sexual discussions and proposals on the Internet. This abrupt and norm-changing shift evokes intense reactions. The speed, magnitude, and endless possibilities, as well as the attendant effects, are without precedent. (Cooper, 2000: 2)

These features undoubtedly also apply in making sense of the seductive elements of other online activities that appeal to young people and encourage transgression and experimentation. We propose to add to this list, suggesting four more: *abundance, ambivalence, arousal* and *asymmetry*. Each will be considered now in terms of their seductive features and relevance to youth cyber-related transgressions.

Accessibility. Three aspects need to be distinguished here: ease of use, sense of competence or mastery, and speed of access. As a potential site for online deviance, the Internet offers almost unparalleled opportunity by virtue of the fact that online access is widely available to and used routinely by young people. In one recent study of young Australians under the age of 18, 90 percent regularly used Google search alone (ACMA, 2016). Access is easy because online presence is woven already into the daily life of young people in so many ways, facilitated by expanded Internet coverage and the availability of mobile computing, in particular 'smart phones'. The ability to connect to other people through social media and email, as well as to web pages all over the world, constitutes a powerful communication and information enabler for any number of different purposes. As criminologists, we know that routine activities in many young lives provide the opportunity and prompts for many forms of deviation (Felson and Eckert, 2018: 75). In terms of cyber delinquency, Internet-based activities (gaming, browsing, etc.) provide virtual 'convergence settings' in which to experience tentative forms of delinquency.

A second aspect of accessibility, as noted, is that ease of use enables many persons to develop a sense of technical mastery that can prompt further investment in online skill acquisition. The sense of 'I can do this' is often missing in other spheres of young persons' lives, as Katz has noted. Technical ease of use and ready skill-building to a threshold level of participation online is widely experienced as rewarding by gamers and hackers, as discussed further below. The affordances that facilitate mastery in turn promote repeat involvements, even habituation; 'what is technologically feasible becomes all but universally irresistible' (Simanowski, 2016: xiv). The large amount of time young people spend on sites such as Google suggests a level of competency, even ease, of operation and explains the tendency for many people to 'stick' there for long periods.

Speed itself contributes to the intensification of experiences as well as to their exhilarating effects, as Cooper (2000) has noted in relation to the Internet. Studies of offline leisure activities have noted the importance attached to feelings of exhilaration in various kinds of edgework such as motorcycle racing and other extreme sports (for example, Copes, 2003). However, speed is also a machine feature of Internet operation (Dieter and Gauthier, 2019; Wacjman, 2015). This feature accords very closely with the appeal among many adolescents of activities that are fast-paced and even extreme (Valkenburg and Pietrowski, 2017: 94–5). It can contribute to *deindividuation*; as well as being sensual and liberating, it often encourages 'indifference' towards one's usual surroundings (Virilio, 1991: 111), disinhibition (Suler, 2004), and thus risk-taking. The rapid, almost machine gun like exposure to new and challenging material that, for instance, web browsing or gaming can generate has also been linked to disorientation and digital 'vertigo' (Keen, 2012; Kurek, 2018).

Anonymity. The prevalence of cyber trolling, for example, has been attributed to the anonymous feature of the Internet (Goldsmith and Brewer, 2015; Gorman, 2019). People can go online under assumed identities using avatars or indeed without the need to signal their presence online. This capability has been expressly linked to the emergence of disinhibited behaviours online (Suler, 2004), behaviours that adolescents would otherwise find impossible or much harder to contemplate in face-to-face interactions (Valkenburg and Peter, 2009: 4). The user all too often presumes a certain privacy or intimacy for the interactions or transactions taking place online, leading to a reduction in self-awareness and self-regulation. These reactions accentuate the likelihood of responses based upon their current emotional state with little regard for longer-term or even immediate consequences (Kurek, 2018). Under conditions of presumed anonymity, young people feel more able to search for, and examine, material on personal matters related to issues such as identity and sexuality in the absence of any external scrutiny. Online offers an environment for 'safe edgework' (Shay, 2017) where intentional self-testing can occur and emotional rewards can be obtained, outside the gaze of peers, parents and other guardians.

Affordability. Once a person has access to the Internet, many of its functions and contents are freely available at little or no cost. Personal information can be derived from sites such as Facebook without charge as well as anonymously. Written, aural and visual material, including pornography, can be downloaded or accessed without the need to send money or pay using a credit card. The way in which Internet-based material is treated by online participants may in fact reflect the fact that the material is free. Similar to the position of the *tragedy of the commons*, the absence of a charge for use often encourages promiscuous and even careless use of such material. Here, the ability to download illegally and free from the Internet in large measure explains the high incidence of online copyright piracy among young people.

Abundance. This feature is closely connected to the affordances of accessibility and affordability. What it signifies is that the affordable and accessible nature of the Internet opens up the online participant to a veritable and seemingly limitless cornucopia of material and experiences of various kinds that is searchable and findable (Manovich, 2013: 114–15; also see Wood, 2018). The pleasures of idle curiosity and the opportunities for immersion appear endless in this world. With nearly 2 billion websites and nearly 4 billion Google searches each day,[2] one can just begin to appreciate the scope for novelty and exploration of curiosity presented by the Internet. As we note below, one of the characteristics of web searches on the Internet is to present users with unanticipated material, sometimes of an extreme and disturbing nature. Such stimulation can simultaneously deny orientational knowledge to users, reducing their agency (Simanowski, 2016: 76). It may induce in some a level of existential vertigo (Coyne, 2016; Keen, 2012). The range of tempting choices encountered by Katz's shoplifting respondents in the department stores they visited pales by comparison with what is on offer via the Internet.

Ambivalence. The polysemous nature of the Internet's holdings as well as the diversity of the participating Internet audiences invite contact with novelty, variety and the unanticipated. It also encourages a feeling that nothing is forbidden or indeed unknown to human experience. The contingency of behavioural norms and the fallibility of traditional sources of authority (for example, parents, teachers) are rendered apparent amidst the cacophony of online voices (Phillips and Milner, 2017: 12). Williams (2018) refers to the distraction potential of the Internet that reduces our capacity for careful reflection. What results, he suggests, is a state of wantonness, in which 'reflected upon, intentional reasons for action' are removed, 'leaving only impulsive reasons in its own wake' (Williams, 2018: 68). Previous taboos melt away or at least are opened up to sceptical examination. From a criminogenic perspective, this affordance contributes to a loosening of personal standards and a reduction in self-regulatory capacity that can lead to deviant behaviours. Another feature of ambivalence is the sense of unreality often mentioned by hardened Internet users, which can reduce the perceived harm as well as the risk from crossing boundaries in these environments (Rimer, 2017). The ability to attach, then detach, often very quickly in online encounters and under the cover of anonymity also contributes to a sense of normlessness (anomie) and to explaining the character of digital drift (Goldsmith and Brewer, 2015).

Arousal. In addition to the thrill derived from speed, another part of the Internet's seductive quality lies in the stimulation it provides for curiosity, for the exploration of difference (Coyne, 2016), and for what, in relation to pornography, has been termed 'carnal resonance' (Paasonen, 2011). Exposure to new, attractive and transgressive images and possibilities can provoke and arouse both physiologically and intellectually. Internet technologies can strike the 'right neurological notes' to render the technologies irresistible to some users (Alter, 2017: 5). Similarly, Whitty and Carr refer to 'psychic keys' that 'appear to enable past unconscious experiences to be released to inform present behaviour' (2003: 881). Although arousal in part benefits from other affordances such as accessibility and abundance, it has its own precipitative weight and force for many adolescents, especially young men (Valkenburg and Pietrowski, 2017: 171). Whatever dispositional or developmental individual variations may exist in terms of self-regulation and impulse control, arousal from digital devices represents a separate, additional variable in the matrix of factors that we need to take account of in making sense of youth cybercrimes. The rewards and reinforcement from the accessibility and abundance of arousing material online set the scene for habituation as well as for further risk-taking. As Prichard et al. note (2011: 594), 'sexual arousal is associated with increased risk-taking behaviours and lower perceptions of negative consequences'. In young people already predisposed to risk-taking, the arousal is likely often to be particularly strong and relatively poorly self-regulated (Valkenburg and Pietrowski, 2017: 171).

Asymmetry. This feature points to elements of the technical environment that preclude, degrade or otherwise diminish the capability for conscious, rational engagement by users with cyber systems. Such elements create a 'treadmill of incompetence', rendering online participants never so fully in control that they 'can prevent the technologies from operating on them in unexpected or undesirable ways' (Williams, 2018: 23). This aspect involves not just tempting and overwhelming instincts through the provision of accessible, arousing abundance, etc., but also works to obscure the motives and logics underpinning particular online experiences. The ability to surprise, for example, is a feature of what Zittrain termed the Internet's *generativity*, its 'capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences' (2008: 70). The role of algorithms, relatively speaking a hidden yet highly influential feature in Internet settings, is significant here, being invisible and/or incomprehensible even to seasoned Internet users (Finn, 2017). These mediating features have also been called 'non-conscious infrastructures' (Dieter and Gauthier, 2019: 21; see also Wood, 2017), pointing to the agentic qualities possessed by computing technologies. The notion of ‘addiction by design’ (Schull, 2012), referring to the technical features of gambling machines that provide variable rewards and entrench compulsive participation by some gamblers, is an example of such infrastructure.

Equally, the overlapping, interconnected, dispersed nature of the Internet itself (a network of networks) makes its outputs and products to some extent unpredictable in content, timing and presentation (Dieter and Gauthier, 2019). Terms such as ‘assemblage’ and ‘constellation’ (Suler, 2004) are used by some scholars to capture the loosely coupled nature of Internet structure and effectivity because, although individuals may appear to ‘work together as a functional entity across the network, they may not necessarily have any other unity’ (Wall, 2007: 167). One important consequence of these features is that they contribute to what Hansen (2012: 33–4) has called ‘operational blindness’ among user populations (see Dieter and Gauthier, 2019: 17).

In summary, what we have described is a set of affordances and related features that can seduce and prompt young people in particular into transgressive behaviours through a variety of appeals to pleasure, availability and convenience. We have also noted their self-reinforcing capacities through providing ready gratification. Drift is rewarded and transgression is reinforced. We now turn to two examples that illustrate, we believe, the ‘seductive swamp’ of the Internet in action in encouraging and precipitating transgressions and criminal acts.

Seductions of cybercrime: Two explorations

The first exploration here relates to youthful online participation on sites that offer illegal and legal pornographic material – colloquially known as pornography. The ‘arousal by design’ nature of this material, as well as the fact that it can take legal as well as illegal forms, provides the opportunity to explore the idea that young people can be seduced by watching online materials into deeper and more problematic engagements online and offline. The second example addresses a form of cybercrime committed by young people (as well as older persons) – hacking (computer misuse) – which can excite public and official interest by virtue of its perceived threat to personal privacy, to the integrity of information systems and databases, and, in some instances, to national security itself. Again, the premise for this exploration is the idea that Internet affordances play an important part in not only encouraging this kind of cybercrime but also seducing adolescent participants into deeper levels of offending.

Pathways through porn

The starting point here is the wider context of the sheer abundance and accessibility of online pornography. The Internet has rendered ‘sneaky thrills’ of sexual voyeurism available on an unprecedented scale. For adolescents, not just adults, it is there to be accessed, which it seems many in fact do (Attwood et al., 2018). According to Stephens-Davidowitz (2017), US online searchers of all ages are more likely to search for porn than for the weather forecast. In another example, in a ‘sting’ experiment conducted in the United Kingdom, an apparently ‘legal’ website, which, once entered, offered the opportunity to connect to websites harbouring hard-core pornography, was observed over 88 days.

During that time, it had 803 visitors, almost all entering in the belief the site was purely legal in character. Of those visitors, 457 proceeded to click on the hard-core sites promising access to pornographic material, leading the researchers to conclude, ‘Worryingly . . . a majority of Internet users will not resist temptation’ (Demetriou and Silke, 2003: 220). The study was unable to differentiate the age of the users in question (adolescent vs. adult), but the results suggest that accessibility online to such material is particularly seductive generally.

Search engines such as Google make Internet pornography not only highly accessible and affordable but also anonymous (Steel, 2015). Viewers can ‘delight in [the] transgressive behaviour’ of others with little or no risk of detection (Penfold-Mounce, 2009: 6). Its sheer abundance is also readily searchable and findable. Typing the search term ‘free porn’ into Google on one occasion generated 92,800,000 results. The architecture of the Internet itself leads the user very quickly from apparently innocent to much deeper exposure (Prichard et al., 2011: 594). The abundance on offer is readily disclosed to even the relatively inexperienced online searcher of any age. One of the first sites to be found, Pornhub,[3] opens to a gallery of sexual images covering provocative themes such as ‘mom and son sleep together’, ‘face-sitting lesbians’ and ‘tanned teens get spanked in the ass’. In addition, a side menu offers an alphabetical list of many dozens of ‘categories’ of pornography, ranging from ‘amateur’ and ‘anal’ to ‘vintage’ and ‘webcam’, which can be explored by a further click of the mouse. As noted above, the linkages between sites themselves contribute to accessibility and abundance. The role of ‘pop-up’ websites, sites that appear unsolicited by the user, is clear in terms of accelerating and elevating exposure to this material (Lewis et al., 2018; Winder et al., 2015).

There seems little doubt that, in at least some cases of serious sexual offending involving online grooming of minors, the earlier use of the Internet is implicated by offenders themselves, not only in encouraging but also in initiating their interest in child pornography: ‘If it wasn’t for the Internet I would have never known. I think as the Internet grows, more people will find out their sexual desires just as I did’ (message posted on child pornography board by ‘Dad’; quoted in Russell and Purcell, 2001: 59).

It is well established that first exposure to online pornography takes place increasingly during adolescence or even childhood (for example, Attwood et al., 2018; Lewis et al., 2018). Initial exposure is often inadvertent or unsolicited, because of the capability (asymmetry) of the Internet to ‘surprise’ (Lewis et al., 2018; Nash et al., 2015; Prichard et al., 2011). The fact that young people spend often long periods on the Internet makes the probability of such coincidental exposure to sneaky sexual episodes greater than for those less tied to the Internet. Drift in this sense is often unintentional. In turn, whether initially the exposure was inadvertent or not, ready access to material of a sexually explicit nature ‘can catapult adolescents’ interest in sex beyond their natural sexual curiosity’ (Donevan and Mattebo, 2017: 82; Dines, 2010). This unexpected exposure among younger people can be disturbing as well as sexually arousing, and almost certainly informs the mental landscapes of young people already uncertain and curious about their sexual nature and future sexual selves (Mulholland, 2013; Valkenburg and Pietrowski, 2017). The Internet intensifies youth exploration and reflection on these themes by offering ‘the illusion of availability’ and, by virtue of affordances in play, ‘the non-consequence of consumption’ (Welsh, 2002: 450). Online, as well as offline, sneaky thrills can sometimes have negative consequences. This situationally induced online curiosity has been linked, as we saw earlier, to some cases of later sexual transgression (Wortley and Smallbone, 2014).

Highways to hacking

Hacking, the unauthorized accessing and interference with computer networks and databases (computer misuse), is not a particularly prevalent form of youth cybercrime, compared with, say, copyright piracy or online bullying (Brewer et al., 2018). In terms of adolescent participation, there are those who 'drift' into minor forms of cyber vandalism (so-called 'script kiddies') through to those called 'crackers', engaged in deliberate serious online criminal activity (Long and Hopkins Burke, 2015). Such variations in motivation and skill competence still need to be understood in terms of the development of the computer-related skills as well as the accompanying attitudes that encourage involvement in serious forms of hacking, which can often have devastating consequences. The necessary skills and sensibilities are typically honed over time during childhood and adolescence, often involving socialization through participation in activities such as online gaming. Gaming is clearly a form of play that also commonly is associated with the use of 'cheats' (cheating), which are widely condoned by players yet against the rules of the game (for example, Wu and Chen, 2018). As we will see, the rewards and satisfaction from achieving mastery in video gaming (Schaffer and Fang, 2018) are immediately recognizable in terms of the pleasures from hacking identified through interviews with hackers.

Wall (2017) analysed a range of hacker testimonies and found a four-stage model of activity shift in which offenders were gradually 'seduced' more deeply into cybercrime: firstly, from playing video games fairly, to using cheats to win games; secondly, from exploiting gaming cheats to engaging in chat/gaming/hacking forums to learn how to disable 'friends'' computers to win games; thirdly, from disabling 'friends'' computers to learning about stronger hacking tactics (such as Distributed Denial of Service); fourthly, from practising minor forms of offending to more serious offending such as exploiting large DDoS attacks, committing data breaches, ransomware (Wall, 2017: 1091; also see Porcedda and Wall, 2019). This progression is confirmed by a law enforcement official with extensive experience of investigating young people suspected of committing cybercrimes, interviewed by Hutchings:

> If you have teenage kids these days, especially boys, you see a lot of them play online games . . . they're teaching each other. It starts with fun and games online . . . tricking people to give up their identities or to give you property within the game and run away with it . . . And then you find a friend who's, [says] guess what I did the other night, so they start talking about it, and then gee, that sounds great, and how did you do that? So . . . . . . as they get older they realize well, what I was doing here, why can't I use this out here and make a bit of coin out of it. (Hutchings, 2013: 150)

Although gaming is rarely if ever intrinsically dangerous, Harvey, one of the hackers interviewed by Steinmetz, observed that it is an important common link for the small number who progress from transgression to more mainstream cybercrime: 'I think video games got us, a lot of us, into it because that was how you started learning to write your own code and how to de-protect it' (Steinmetz, 2016: 62).

For the hacker, the vast scale of the Internet (abundance) and its relative accessibility mean that there is no shortage of targets or opportunities to develop and refine one's hacking skills. The field of hacking is also built upon a structural dichotomy between 'white' and 'black' hats, and indeed some shades of grey in between (Coleman, 2013; Steinmetz, 2016). However, it is widely acknowledged that these identities are not fixed, and there is movement between the two categories. The shared focus among hackers on the skills required to undertake more serious kinds of hacking reminds us of the important role of peer influence in not just encouraging transgression but also neutralizing any negative connotations. Thus, among hackers, what is done, if not strictly legal, is viewed at least as *positive deviance* (Turgeman-Goldschmidt, 2005).

Hacking is pleasurable for many, and this reward encourages further involvement. In the following example (PBS, 2001a), a hacker explains the appeal:

> Well, it's power at your fingertips. You can control all these computers from the government, from the military, from large corporations. And if you know what you're doing, you can travel through the internet at your will, with no restrictions. That's power; it's a power trip. . . . everybody likes to feel in control.

The 'sneaky thrill' is present: 'certainly there was a great rush, so to speak. You do get a rush from doing it – definitely. There is a lot of adrenaline, if nothing else' (PBS, 2001b). 'Getting away with it' is exciting (Steinmetz, 2016: 102), particularly when one is violating another's private space. A female hacker interviewed by Turgeman-Goldschmidt also confirms this attraction: 'The thing about hacking is the excitement, the adrenaline, the fun of doing something illegal' (2011: 45). Another interviewee expressly invoked seduction to explain how he feels: 'It's so juicy. It's so seductive . . . It's stimulating, and it overtakes you. You just can't have a little bit of it. You have to know as much as possible, as fast as possible' (Turgeman-Goldschmidt, 2005: 13).

The motivation from a sense of 'idle curiosity' is commonly expressed in hacker accounts. As one said, 'the best definition I heard of a hacker was just someone who . . . if they saw something closed and it was doing something, they just wanted to open it up to see how it was working, and then how to maybe play with it a little bit to make it work a little better' (PBS, 2001c). Curiosity can also verge on voyeurism; the affordances that make these intrusions possible are blind of course to any moral distinction. One interviewee, asked why he spent so many hours engaged in hacking, replied:

> I think, obviously, I'm just a very nosy person. I'm like your nosey neighbor on steroids, basically. [W]hen you see into someone's computer, it gives you an idea of how they work, who they speak to, what they're interested in, whether they actually do any work, what their job is. You can see a lot of someone's life just from the contents of their PC. (PBS, 2001b)

Another linked his voyeurism to his lack of respect for privacy and confidentiality:

> If I can enter [someone else's computer], it's not private . . . I'm very nosy. When I was younger . . . I'd peep into people's windows with binoculars. It happens that I get turned on by a target and break in out of curiosity. (Turgeman-Goldschmidt, 2005: 37)

The lifeworld of hackers therefore points to a frequent, if not near-constant, negotiation of boundaries between the licit and the illicit. The affordances and other features related to online presence can facilitate and even encourage drift between white hat and black hat activities. In addition to providing opportunities for the development of skill or craft, the technological environments with which they engage offer and tempt *craftiness*, the highly sensual and all-consuming exploration of both the unauthorized possibilities as well as the limits of computing technologies (Coleman, 2013: 100).

These observations are acutely reflected in recent court cases involving the hackers Hutchins (BBC, 2019), Qaiser (Dearden, 2019), West, Kelley and others (Porcedda and Wall, 2019). The evidence from each of the above cases and also from other similar types of cyber-dependent cases across a range of jurisdictions is that they began experimenting and then offending when aged in their early to mid-teens. They quickly developed their coding skills from 'wannabes' to 'script kiddies', then to skilled hackers, but were in their mid to late teens (two–four years later) before they became persons of interest to law enforcement agencies. In each case the defendant demonstrated rapid progression into more serious forms of cybercrime offending, in a manner very similar to the four stages of drift outlined earlier (Wall, 2017). As we will argue below, the seductive processes can quickly lead to more serious outcomes unless more timely, targeted interventions can disrupt and divert these processes so as to mitigate escalating risk from unchecked cyber activity (see Porcedda and Wall, 2019).

Responding to the sensuality of youth cybercrime

It follows from our argument that good policy in youth cybercrime must accept the proposition that 'however powerful and well trained the surface will is, it is not a match for circumstances' (Aldous Huxley, quoted in Williams, 2018: 23). Without ignoring class, peer influence, family background, race, poverty (Katz's 'background factors') or indeed addiction, there needs to be a deeper understanding of the persuasive technologies at work in the lives of young people. Consequently, it must be recognized that not all motivations for transgression are indicative of deep criminal pathology or criminal career commitment.

Policy should consist of interventions that take account of the relative lack of worldly experience of many young offenders. Online persuasive technologies render the challenge of weighing up potential risks and harms from particular actions even harder in many instances. A propensity for thrill-seeking common especially among young males encouraged by the Internet can induce a form of non-malicious myopia towards possible or likely consequences. Punitive responses therefore need to be sparingly applied. Reversing the drift into criminal online activities in part depends upon provision of pro-social supports that acknowledge the desire for human connection as well as the assertion of identity and the pursuit of pleasurable, rewarding activities. The PREVENT principles adopted in the UK and elsewhere stress the importance of preventive measures and the minimal use of deterrent and punitive measures in order to deal effectively and efficiently with offending that may be widespread yet not entrenched in individual cases. Early interventions (such as offender workshops) and alternative forms of resolution (such as Cease and Desist orders and restorative justice) are being proposed and developed to prevent cybercrime offenders progressing into more serious forms of offending (see NCA, 2017). Reconnecting young people to education and work opportunities is fundamental. The role of restorative justice in dealing especially with the younger, more recently ‘drifted’ transgressors is worthy of exploration (Brewer et al., forthcoming). Those responsible for diversions will need to form relationships with education providers and potential employers in order to assist young offenders to develop a sense of an alternative, legitimate identity in which cyber interests can be incorporated and celebrated, rather than repressed or shunned.

Giordano, Cernovich and Rudolph (2002: 1001) refer to the need for desistance processes generally to enable the envisioning by offenders of ‘an appealing and conventional “replacement self”’. In the case of many young cyber-offenders, the quest for a more conventionally endorsed and appealing alternative self will often be less difficult than it will be for more entrenched, offline offenders with histories of violence or dishonesty. Reversing the drift in such cases will often require a reorientation of focus rather than the abandonment of old skills and habits. In the case of a ‘black hat’ hacker, for example, a turn towards ‘white hat’ hacking activities would ensure a high level of continuity with previously acquired skills and previously rewarding experiences from developing and applying new skills. For those adolescents less entrenched in the world of hackers, it should be even easier to reverse the online drift through education in the risks and harms that nonetheless emerge from their naive or tentative engagements with the Internet.

Another way to ‘brighten the lines’ between acceptable and unacceptable online behaviours is to make those behind the technologies involved more responsive to and responsible for what takes place on their platforms (Williams, 2004). Whatever measures are taken ultimately, policy makers need to avoid provoking needless defiance (Holt et al., 2018) among those they seek to regulate by considering wherever possible the affective and emotional needs of young people. Not all by any means will find meaningful legitimate work in the computer industry in the future. The challenge then is to explore and support ‘different conformities’ (Bottoms et al., 2004: 384), that is, ways in which young people can act pro-socially without abandoning completely the allures of cyberspace.

Conclusion

For many young people, and particularly adolescents, the Internet is indeed a seductive swamp, rich in attractive offerings. For those already prone developmentally to curiosity and sensation-seeking, it can be difficult not to yield to its charms. As well as offering an abundance of ‘sneaky thrills’, it contributes to ‘the expanded possibilities of the self’. We have seen how it opens up ‘ways of being that previously seemed inaccessible’ (Katz, 1988: 73). Significantly in criminological terms, in various ways it encourages and precipitates cyber-related transgressions in otherwise unremarkable young people. Online as well as offline deviance can be ‘delightful’ (Katz, 1988: 312). From a regulatory perspective, however, these features serve to degrade young people’s finite resources of self-regulation and impulse control (Forrest et al., 2019). Digital drift for many young people therefore becomes *extremely* easy to do (Goldsmith and Brewer, 2015).

Beyond drawing attention to the precipitative consequences of the Internet’s seductive features, we have also pointed to the need for closer consideration of the Internet’s generativity (Zittrain, 2008). If, indeed, the Internet can produce ‘operational blindness’ (Hansen, 2012), how this is done through the specific features and affordances of the Internet needs better understanding. The concept of seduction needs further explication in terms of the particular affordances and features of the full range of Internet technologies, including social media and online gambling sites. Drift may well be precipitated or encouraged differently in different online environments. Deeper engagement with the field of human–computer interaction offers promising prospects for interested criminologists. For example, concepts such as ‘situated motivational affordances’, affordances that link the socio-emotional needs of young people to the experiential rewards and outcomes arising from particular elements of the Internet infrastructure, lend themselves to closer study in terms of coming to terms with the thrills as well as the other satisfactions derived from different online transgressions (see Karahanna et al., 2018). As noted, effective regulatory responses must reflect the socio-technical differentiation that exists between platforms and various online activities. They must also respond to the range of meanings and motivations young people bring to, and find in, their online behaviours, not least of all in order to bring young people along in any regulatory initiatives (Holt et al., 2018).

Acknowledgements

We would like to thank Rod Watson, Jane Turner Goldsmith and Peter Grabosky, as well as the two anonymous reviewers, for closely reading, and encouraging improvement upon, earlier drafts of this article. Flinders student Paige Fletcher assisted with editing the final copy.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was part supported by an Australian Research Council Grant DP170103538 and UK Engineering and Physical Sciences Council awards (EMPHASIS EP/P011721/1 and CRITiCal EP/M020576/1).

ORCID iDs

Andrew Goldsmith https://orcid.org/0000-0002-2791-9119
David S Wall https://orcid.org/0000-0002-6003-1592

Notes

1. *Oxford Dictionary Online*, URL (accessed 25 August 2017): https://en.oxforddictionaries.com/definition/seduction.
2. Internet Live Stats. URL (accessed 5 March 2019): http://www.internetlivestats.com/.
3. Pornhub is a file-sharing website launched in 2010 that shares videos of sexual materials. It was and still is reputedly the largest pornography site on the Internet.

References

ACMA (2016) Snapshot: Aussie teens and kids online. Australian Communications and Media Authority. URL (accessed 11 November 2019): https://www.acma.gov.au/publications/2016-02/report/snapshot-aussie-teens-and-kids-online.

Alter A (2017) *Irresistible: Why We Can't Stop Checking, Scrolling, Clicking and Watching*. London: Bodley Head.

Attwood F, Smith C and Barker M (2018) 'I'm just curious and still exploring myself': Young people and pornography. *New Media & Society* 20(1): 3738–3759.

BBC (2019) Marcus Hutchins spared US jail sentence over malware charges. *BBC News*, 26 July 2019. URL (accessed 11 November 2019): https://www.bbc.com/news/technology-49127569.

Bennett J (2001) *The Enchantment of Modern Life*. Princeton, NJ: Princeton University Press.

Bottoms A, Shapland J, Costello A, Holmes D and Muir G (2004) Towards desistance: Theoretical underpinnings for an empirical study. *Howard Journal of Criminal Justice* 43(4): 368–389.

Brewer R, Cale J, Goldsmith A and Holt T (2018) Young people, the Internet, and emerging pathways into criminality: A study of Australian adolescents. *International Journal of Cyber Criminology* 12(1): 115–132.

Brewer R, de Vel-Palumbo M, Hutchings A, Holt T, Goldsmith A and Maimon D (forthcoming) *Cybercrime Prevention: Theory and Applications*. London: Palgrave.

Briar S and Piliavin I (1965) Delinquency, situational inducements, and commitment to conformity. *Social Problems* 13(1): 35–45.

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

Clarke R (2008) Situational crime prevention. In: Wortley R and Mazerolle L (eds) *Environmental Criminology and Crime Analysis*. Cullompton: Willan Publishing, 178–194.

Coleman E (2013) *Coding for Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.

Cooper A (2000) Cybersex and sexual compulsivity: The dark side of the force. *Sexual Addiction & Compulsivity* 7: 1–3.

Copes H (2003) Streetlife and the rewards of auto theft. *Deviant Behavior* 24(4): 309–322.

Coyne R (2016) *Mood and Mobility: Navigating the Emotional Spaces of Digital Social Networks*. Cambridge, MA: MIT Press.

Dearden L (2019) Hacker who blackmailed porn users into handing him money after they clicked on his pop-up adverts jailed. *Independent*, 9 April. URL (accessed 11 November 2019): https://www.independent.co.uk/news/uk/crime/porn-hacker-blackmail-zain-qaiser-trial-prison-sentence-a8861236.html.

Demetriou C and Silke A (2003) A criminology internet sting: Experimental evidence of illegal and deviant visits to a website trap. *British Journal of Criminology* 43: 213–222.

Deterding S (2011) Situated motivational affordances of game elements: A conceptual model. Paper presented to CHI 2011 workshop: 'Gamification: Using Game Design Elements in Non-gaming Contexts'. Vancouver, Canada, 7–12 May.

Dieter M and Gauthier D (2019) On the politics of chrono-design: Capture, time and the interface. *Theory Culture & Society* 36(2): 61–87.

Dines G (2010) *Pornland: How Porn Has Hijacked Our Sexuality*. Boston: Beacon Press.

Donevan M and Mattebo M (2017) The relationship between frequent pornography consumption, behaviours, and sexual preoccupancy among male adolescents in Sweden. *Sexual and Reproductive Healthcare* 12: 82–87.

Eurostat (2017) Being young in Europe today – digital world. URL (accessed 11 November 2019): https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Being_young_in_Europe_today_-_digital_world.

Felson M and Eckert M (2018) *Introductory Criminology: The Study of Risky Situations*. New York: Routledge.

Finn E (2017) *What Algorithms Want: Imagination in the Age of Computing*. Cambridge, MA: MIT Press.

Forrest W, Hay C, Widdowson AO and Rocque M (2019) Development of impulsivity and risk-seeking: Implications for the dimensionality and stability of self-control. *Criminology* 57(3): 512–543.

Giordano P, Cernovich S and Rudolph J (2002) Gender, crime and desistance: Towards a theory of cognitive transformation. *American Journal of Sociology* 107(4): 990–1064.

Goldsmith A and Brewer R (2015) Digital drift and the criminal interaction order. *Theoretical Criminology* 19(1): 112–130.

Gorman G (2019) *Troll Hunting: Inside the World of Online Hate and Its Human Fallout*. London: Hardie Grant Books.

Hansen M (2012) Engineering pre-individual potentiality: Technics, transindividuation and 21st century media. *Substance* 41(3): 32–59.

Holt T, Brewer R and Goldsmith A (2018) Digital drift and the 'sense of injustice': Counter-productive policing of youth cybercrime. *Deviant Behavior* 40(9): 1144–1156.

Hutchings A (2013) Hacking and fraud: Qualitative analysis of online offending and victimization. In: Jaishankar K and Ronel N (eds) *Global Criminology: Crime and Victimization in the Globalized Era*. Boca Raton, FL: CRC Press, 93–114.

Hutchings A and Chua Y (2016) Gendering cybercrime. In: Holt TJ (ed.) *Cybercrime through an Interdisciplinary Lens*. Abingdon: Routledge, 167–188.

Internet World Stats (2019) Usage and population statistics. Internet usage and world population statistics estimates for June 30, 2019, as of Sept 20, 2019. URL (accessed 11 November 2019): https://internetworldstats.com/stats.htm.

Karahanna E, Xu S, Xu Y and Zhang N (2018) The needs–affordance–features perspective for the use of social media. *MIS Quarterly* 42(3): 737–756.

Katz J (1988) *The Seductions of Crime*. New York: Basic Books.

Keen A (2012) *Digital Vertigo*. New York: Griffin.

Kurek A (2018) Understanding online disinhibition: An investigation of the relationship between information and communication technology and adolescent personality, identity and behavior. PhD thesis, Victoria University of Wellington, New Zealand.

Lewis L, Mooney-Somers J, Guy R, Watchirs-Smith L and Skinner R (2018) I see it everywhere: Young Australians' unintended exposure to sexual content online. *Sexual Health* 15(4): 335–341.

Long M and Hopkins Burke R (2015) Vandalism and cyberspace. In: Long M and Hopkins Burke R (eds) *Vandalism and Anti-social Behaviour*. New York: Springer, 171–189.

McNamee R (2019) *Zucked: Waking up to the Facebook Catastrophe*. London: HarperCollins.

Manovich L (2013) *Software Takes Command*. New York: Bloomsbury Press.

Matza D (1964) *Delinquency and Drift*. New York: Wiley.

Mulholland M (2013) *Young People and Pornography: Negotiating Pornification*. New York: Palgrave.

Nahl D (2007) Social-biological technology: An integrated conceptual framework. *Journal of the American Society for Information Science and Technology* 58(13): 2012–2046.

Nash V, Adler J, Horvath M, Livingstone S, Marston C, Owen G and Wright J (2015) Identifying the routes by which children view pornography online: Implications for future policy-makers seeking to limit viewing. Report of Expert Panel for DCMS. London: Department for Culture, Media and Sport. URL (accessed 11 November 2019): http://eprints.lse.ac.uk/65450/.

NCA (National Crime Agency) (2017) Pathways into cyber crime. *Report, National Cyber Crime Unit / Prevent Team*, January. URL (accessed 11 November 2019): https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1.

Paasonen S (2011) *Carnal Resonance: Affect and Online Pornography*. Cambridge, MA: MIT Press.

PBS (2001a) Interview: Anonymous. *PBS Frontline*. URL (accessed 11 November 2019): http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/anon.html.

PBS (2001b) Interview: Raphael Gray a.k.a. Curador. *PBS Frontline*. URL (accessed 11 November 2019): https://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/curador.html.

PBS (2001c) Interview: Reid & Count Zero. *PBS Frontline*. URL (accessed 11 November 2019): https://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/reidcount.html.

Penfold-Mounce R (2009) *Celebrity Culture and Crime: The Joy of Transgression*. New York: Palgrave.

Phillips W and Milner RM (2017) *The Ambivalent Internet*. Malden, MA: Polity Press.

Porcedda MG and Wall DS (2019) Cascade and chain effects in big data cybercrime: Lessons from the TalkTalk hack. In: *Proceedings of WACCO 2019: 1st Workshop on Attackers and Cyber-Crime Operations (IEEE EuroS&P 2019)*, Stockholm, Sweden, 20 June.

Presdee M (2000) *Cultural Criminology and the Carnival of Crime*. London: Routledge.

Prichard J, Watters P and Spirovanovic C (2011) Internet subcultures and pathways to the use of child pornography. *Computer Law & Security* 27: 585–600.

Quadara A, El-Murr A and Latham J (2017) *The Effects of Pornography on Children and Young People: An Evidence Scan*. Research Report. Melbourne: Australian Institute of Family Studies. URL (accessed 11 November 2019): https://aifs.gov.au/publications/effects-pornography-children-and-young-people.

Rimer J (2017) Internet sexual offending from an anthropological perspective: Analysing offender perceptions of online spaces. *Journal of Sexual Aggression* 23(1): 33–45.

Russell D and Purcell N (2001) Exposure to pornography as a cause of child sexual victimization. In: Dowd N, Singer D and Wilson R (eds) *Handbook of Children, Culture, and Violence*. Thousand Oaks, CA: SAGE, 59–83.

Schaffer O and Fang X (2018) What makes games fun? Card sort reveals 34 sources of computer game enjoyment. In: *24th Americas Conference on Information Systems (AMCIS 2018): New Orleans, Louisiana, USA, 16–18 August 2018*. Vol. 1. Atlanta, GA: Association for Information Systems: 1392–1401.

Shay H (2017) Virtual edgework: Negotiating risk in role-playing gaming. *Journal of Contemporary Ethnography* 46(2): 203–229.

Schull M (2012) *Addiction by Design: Machine Gambling in Las Vegas*. Princeton, NJ: Princeton University Press.

Simanowski R (2016) *Data Love: The Seduction and Betrayal of Digital Technologies*. New York: Columbia University Press.

Steel C (2015) Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child Abuse & Neglect* 44: 150–158.

Steinberg L, Albert D, Cauffman E, Banich M, Graham S and Woolard J (2008) Age differences in sensation seeking and impulsivity as indexed by behaviour and self-report: Evidence for a dual systems model. *Developmental Psychology* 44(6): 1764–1778.

Steinmetz K (2016) *Hacked: A Radical Approach to Hacker Culture and Crime*. New York: New York University Press.

Stephens-Davidowitz S (2017) *Everyone Lies: What the Internet Can Tell Us about Who We Really Are*. New York: Bloomsbury Press.

Suler J (2004) The online disinhibition effect. *CyberPsychology and Behaviour* 7(3): 321–326.

Turgeman-Goldschmidt O (2005) Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review* 23: 8–23.

Turgeman-Goldschmidt O (2011) Identity construction among hackers. In: Jaishankar K (ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, FL: CRC Press, 31–51.

Vaidhyanathan S (2011) *The Googlization of Everything*. Berkeley, CA: University of California Press.

Valkenburg P and Peter J (2009) Social consequences of the Internet for adolescents. *Current Directions in Psychological Science* 18(1): 1–5.

Valkenburg P and Pietrowski J (2017) *Plugged In: How Media Attract and Affect Youth*. New Haven, CT: Yale University Press.

Van der Wagen W and Pieters W (2015) From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology* 55: 578–595.

Virilio P (1991) *The Aesthetics of Disappearance*. Cambridge, MA: MIT Press.

Wacjman J (2015) *Pressed for Time: The Acceleration of Life in Digital Capitalism*. Chicago: University of Chicago Press.

Wall D (2007) *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity.

Wall D (2017) Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing. In: Brownsword R, Scotford E and Yeung K (eds) *The Oxford Handbook on the Law and Regulation of Technology*. Oxford: Oxford University Press, 1075–1096.

Welsh I (2002) *Porno*. London: Vintage.

Whitty M and Carr A (2003) Cyberspace as potential space: Considering the web as a playground to cyber-flirt. *Human Relations* 56(7): 869–889.

Williams M (2004) Understanding King Punisher and his order: Vandalism in an online community – Motives, meanings and possible solutions. *Internet Journal of Criminology* 1–40.

Williams J (2018) *Stand Out of the Light: Freedom and Resistance in the Attention Economy*. Cambridge: Cambridge University Press.

Winder B, Gough B and Seymour-Smith S (2015) Stumbling into sexual crime: The passive perpetrator in accounts by male internet sex offenders. *Archives of Sexual Behavior* 44(1): 167–180.

Wood M (2017) Anti-social media and algorithmic deviancy amplification: Analysing the id of Facebook's technological unconscious. *Theoretical Criminology* 20(7): 168–185.

Wood MA (2018) *Antisocial Media: Crime-watching in the Internet Age*. Cham: Palgrave Macmillan.

Wortley R (2008) Situational precipitators of crime. In: Wortley R and Mazerolle L (eds) *Environmental Criminology and Crime Analysis*. Cullompton: Willan Publishing, 48–69.

Wortley R and Smallbone S (2014) A criminal career typology of child sexual abusers. *Sexual Abuse: A Journal of Research and Treatment* 26(6): 569–585.

Wu Y and Chen V (2018) Understanding online game cheating: Unpacking the ethical dimension. *International Journal of Human-Computer Interaction* 34(8): 786–797.

Yar M (2005) Computer hacking: Just another case of juvenile delinquency? *Howard Journal of Criminal Justice* 44(4): 387–399.

Zittrain J (2008) *The Future of the Internet*. New Haven, CT: Yale University Press.