International Journal of Cyber Criminology
Vol 12 Issue 1 January – June 2018

Young People, the Internet, and Emerging Pathways into Criminality: A Study of Australian Adolescents

Russell Brewer[1]
Flinders University, Australia

Jesse Cale[2]
University of New South Wales, Australia

Andrew Goldsmith[3]
Flinders University, Australia

Thomas Holt[4]
Michigan State University, United States of America

Abstract

This article explores the ways in which young people experience the Internet as a potentially criminogenic medium. To date, little research has explored the possible links between the mundane, ubiquitous use of digital communication technologies by young people and involvement in delinquency in online contexts. The current empirical study seeks to address this gap, by investigating how a young person's digital pursuits (i.e. relative access, technical competencies, and exposure to pertinent technologies, Internet sites and services), as well as various developmental considerations, are linked to delinquent online encounters – be they tentative engagements of a naïve or non-criminal kind or deliberate, more serious forms of technologically-mediated criminality. Drawing on data collected from a cohort of adolescents enrolled at a secondary school in a large Australian city, the results establish significant relationships between many of these concepts, but also flag that online delinquent encounters amongst young adolescents are unlikely to correspond with serious criminal involvements, with such activities being episodic and for the most part trifling. The results further highlight the need for a better understanding of the role of digital communication technologies on pathways into cybercrime.

Keywords: Adolescents, Cybercrime, Digital Drift, Matza, Pathways into Crime.

[1] Senior Lecturer, Centre for Crime Policy and Research, Flinders University, GPO Box 2100, Adelaide, SA, 5001, Australia. Email: russell.brewer@flinders.edu.au
[2] Senior Lecturer in Criminology, School of Social Sciences, University of New South Wales Sydney, NSW, 2052, Australia. Email: j.cale@unsw.edu.au
[3] Strategic Professor in Criminal Justice, Centre for Crime Policy and Research, Flinders University, GPO Box 2100, Adelaide, SA, 5001, Australia.
Email: andrew.goldsmith@flinders.edu.au
[4] Professor, School of Criminal Justice, Michigan State University, 655 Auditorium Road, East Lansing, MI, 48824, USA. Email: holtt@msu.edu

Introduction

Numerous seminal criminological studies of real-world offending suggest that young people are particularly vulnerable to this intensification of criminogenic opportunities and means (e.g. Cloward & Ohlin, 1960; Matza, 1964; amongst various other contemporary studies). What is less known is the extent to which these processes operate in online contexts, which in recent research, we frame as a process of 'digital drift' (Goldsmith & Brewer, 2015). This concept posited the idea that within the conditions of everyday computer and Internet use are both the technical and social affordances that may intensify and foster opportunities for online delinquency of various kinds. That is, while the Internet can provide users the technical means for committing both cyber-enabled crime and cybercrimes (e.g. through access to new tools; or making available a virtually limitless pool of targets), it also, offers these same users new ways of encountering others and forming social attachments that may, or may not lead to joint crime activities (see further, Diamond & Bachmann, 2015; Holt & Bossler, 2016).

In this article, we establish theoretical links between the *attributes of users,* the distinctive *features of technology* and the *delinquent uses made of it*. That is, we suggest that certain features of digital technologies empower individuals in the ways they learn about how to commit crime, as well as encounter others who encourage, facilitate, or join directly in the commission of delinquent acts. Furthermore, we draw upon key arguments made by Matza (1964, p. 29), who established that crime amongst young people is often "accidental or unpredictable", rather than being highly planned or anticipated by those committing them. In developing these ideas in contemporary and virtual contexts, we argue that criminology has been slow to respond to the scale and novelty of changes brought about by emergent digital technologies, and to grasp the implications for understanding adolescent pathways into cybercrime.

As the Internet today forms a central part of many young people's educational and recreational environment, and as adolescence is a time for exploration and risk-taking, this conjunction of circumstances raises myriad questions about pathways from 'innocent', 'playful' or 'experimental' engagements on the Internet by adolescents toward serious Internet-mediated illegality. This article seeks to explore and enhance understandings of the origins of such pathways. This will be accomplished by first, by reviewing the available literature examining both the centrality and significance of digital technology in the lives of developing adolescents. Next, we elaborate, theoretically, on the process of digital drift, as well as elucidate the criminogenic features of digital technologies. We then offer a preliminary empirical exploration of concepts that are possibly associated the nascent stages of digital drift within an adolescent context, accomplished through a study of a cohort of early teenagers enrolled in a secondary school in a large Australian city. The results of this analysis illustrate the nature and extent of adolescent digital engagement, and demonstrate links with online delinquency. A discussion of these findings flags the importance of developing enhanced theoretical and empirical understandings of criminal pathways within the broader cybercrime scholarship, which up until now has received fairly limited attention (e.g. Diamond & Bachmann, 2015; Holt & Bossler, 2016).

The Digital Lives of Adolescents

Digital technologies, and in particular, the Internet, play a significant and increasingly central part in adolescent life. In the United States, for example, a recent survey of

adolescents aged 13-17 found that nearly all (92%) used the Internet on a daily basis, including nearly one-quarter (24%) who reported being online 'almost constantly' (Lenhart, 2015). Similar trends are evident in both developed and developing economies. In Australia, for example, adolescents use the Internet more than any other age group (Green et al., 2011). Increasingly this use is reliant upon access to mobile devices and not tied to the home or school where adult supervision or peer oversight might moderate technological misuse. Limited wired Internet infrastructure within some nations may make mobile computing devices and the smartphone in particular, the only way of connecting online, especially in the developing world (Boyd, 2014). Within the next five years, access to mobile computing devices, including smartphones and tablets, are forecasted to have Internet traffic growth rates of 62 and 65 percent respectively (Cisco, 2015). In short, Internet use among young people is increasingly prevalent and pervasive in normal, everyday life, and as a consequence its criminogenic potential is massive (see also, Hawdon, 2012).

Within the discipline of criminology and indeed more widely within social science, the question of how the Internet potentializes adolescent behavior towards delinquency remains a largely unexplored, yet fundamental, question. Even before the advent of the Internet, adolescence has long been viewed by developmental psychologists as a period of tremendous (and often tumultuous) biological, psychological and social change. During puberty, adolescents experience rapid growth, expand their social skills and circles, as well as mature sexually (Tanner, 1978). Significant brain development also occurs during this period, resulting in expanded cognitive abilities that ultimately enable more sophisticated thinking when compared to children - particularly as it relates to abstract reasoning about hypothetical situations (Inhelder & Piaget, 1999; Steinberg, 2008). As adolescents negotiate the boundaries of this transition, they are "increasingly receptive or active with respect to risky, albeit not necessarily illegal or anti-social behavior" (van der Hof & Koops, 2011 p. 5). For some time now, scholars have widely acknowledged that experimental and risk-taking behaviors are in some ways central to the adolescent condition. Such experimentation has been visible in relation to the exploration of newfound sexuality (Weinstein & Rosen, 1991; Marcum et al., 2014), the development of independent and coherent identities (Erikson, 1968; Kroger, 2003), the formation of intimate and complex social relationships with peers and romantic partners (Furman & Shaffer, 2003; Pombeni et al., 1990), and the acquisition of values/ideologies consistent with the social groups to which they belong (Havighurst, 1972).

As a precursor to our present inquiry, educators and child welfare authorities in recent years have increasingly expressed concern about the cyber-risks faced by young people (e.g. Green et al., 2011). The discourse of risk has tended to place emphasis on young people as vulnerable victims of the abuses of such technologies by more experienced and manipulative individuals or groups. The sense of youth vulnerability has been linked to the novelty and extent of this 'net generation' (Tapscott, 1998) or breed of supposedly technically proficient 'digital natives' (Prensky, 2001; Stickel, 2017). Elsewhere, scholars have suggested that this (net) generation of young people is, through technology, *thinking* differently, *learning* differently, and *behaving* differently than those preceding it (Bennett & Maton, 2010). There is much to these arguments and the implications are significant. We agree with Subrahmanyam and Šmahel (2011) that digital technologies have dramatically altered the landscape upon which adolescents traverse developmental stages and

accomplish such tasks as establishing their own identity, exploring their sexuality and forming close relationships. As we detail below, however, we argue that relative to offline environments, features of these digital technologies (particularly the Internet) also provide augmented and amplified criminogenic potential, especially with respect to developing adolescents. Our focus is thus more upon the adolescent as perpetrator *and* victim of crime, and in particular, how the increased use of digital technologies have bearing upon the ways delinquent encounters take shape (accidental or purposeful exposure), and form criminal commitments (become motivated, construct criminal identities, enhance capabilities, and participate). In doing so, this study builds on related early empirical work seeking to establish links between technology use and specific forms of Internet-mediated delinquency (e.g. Costello et al., 2016; Marcum et al., 2014).

The Features of a Criminogenic Internet

The Internet exhibits features that make it uniquely criminogenic relative to offline environments, which require specification. For example, we can see the Internet as its own distinct 'place'. The concept of 'place' or 'setting' has been important within criminology with respect to understanding criminal associations, offender convergence, and the social accomplishment of crime (Felson, 2006). While it is indeed another place to 'meet' or encounter others, there are features of this setting of criminogenic significance which distinguish it from 'real' places (Yar, 2005). The Internet de-territorializes encounters, removing the need for face-to-face interactions and making encounters across distance possible. These encounters can occur in 'real' or near-real time (synchronous encounters) but can also occur asynchronously; a post on a website may be accessed hours, days or indeed months and years after its posting, for example (see further, Costello et al., 2016; Reyns et al., 2011). These features enable the assumption of digitally-curated identities, at times used to establish anonymity on the Internet, such that users' identities and motives are concealable and potentially fraudulent or false. Encounters in these milieu will often be ephemeral and the kinds of criminal associations forged can be more at-a-distance and be fleeting in nature (Goldsmith &Brewer, 2015).

The general structure of the Internet and the various connectivity points also affect the criminogenic nature of this environment. The architecture of the Internet permits users to connect regardless of where they are located in the world through virtually any resource–enabling various forms of criminal participation as the self-directed individual may enter, exit and inhabit myriad virtual spaces at will. Moreover, the complex and often invisible ways in which knowledge and communication channels are structured based on the HTML language used to link websites and services makes the Internet a potentially seductive and often surprising place. Users can easily move from a point of predictable use (e.g. targeted information searches) to apparently random and unpredictable discoveries of information, images and points of view due to the multiple 'hidden' linkages between websites and services that are often driven by commercial considerations. Moreover, the proliferation of 'pop-up' advertisements or hashtag link information/resources in sometimes tangential or tenuous ways to an original query.

The relatively hidden features of the Internet also create a substantial power of suggestibility that goes unnoticed by users. New media scholars have noted the suggestive power of the algorithms driving now omnipresent Internet platforms and systems, such as search engines like Google, social networks like Facebook and Twitter, mapping services

including Apple and Google Maps, and even free email services from Gmail and Yahoo. The predictive features now built into mobile operating systems, including the likes of Siri, Cortana, and Google Assistant, as well as messaging bots may also direct users to certain resources or experiences on the basis of their algorithms. These play a significant role in directing the ways individuals engage with information, and interact with others through digital technologies (Lanier, 2010; Tucker, 2014; Pariser, 2011; Vaidhyanathan, 2011). Using vast quantities of user data[5] harvested both directly and indirectly, these service systems are able to glean insight into some of the most personal aspects of an individual's life - for example, what they like to eat, watch, buy, where they live and spend time, where they plan to spend their next holiday, what hobbies they have, what they read, who their friends are, and even what they fantasize about. Such information is routinely used by these 'semi-intelligent systems' to actively nudge users toward engaging with the Internet in certain ways. The use of algorithms can be specifically designed "to indulge our desires and weaknesses' and to 'capitalize on our...cravings and curiosities" (Vaidhyanathan, 2011 p. 52-54). The provision of previously un-thought possibilities and the pandering to adolescent curiosity can therefore make the Internet a hazardous place from a risk management perspective – for parents and law enforcement alike. These technical features of the Internet contribute, we suggest, to the 'accidental' nature of at least some adolescent delinquency on the Internet (McEwan & Wellman, 2013; Meyrowitz, 1997), in line with Costello et al.'s (2016) finding that delinquent encounters can be both, deliberate, but also unplanned or serendipitous.

In addition, research has illustrated potential behavior patterns of youth who are drawn to Internet use, particularly deviant or delinquent uses. There is a psychological perspective to be acknowledged here, one that considers individual traits and looks in particular, for signs of Internet-related pathology including addiction (Burnay et al., 2015). Impulsivity and low self-control also appear to have an association to a range of risky on-line behaviors such as sharing personal information, as well as various forms of delinquency and crime (see Diamond & Bachmann, 2015; Holt & Bossler, 2016). There are also cultural dispositions that, Passini (2013) argues, are inherent in many of its users (e.g. narcissism, present-time orientations, and a utilitarian approach to relationships). These, it can be supposed, promote a high degree of ephemerality in terms of the potential for new online encounters and how they might develop into criminal engagements. Matza (1964 p. 28) identified commensurate transitions into deviance in terrestrial settings, noting the susceptibility of juveniles lacking in self-control and prone to risk-taking to "casually, intermittently and transiently [become] involved in a pattern of illegal action". In particular, he stressed the "unpredictable" ways that such individuals or "delinquent drifters" as he labels them, negotiate various cultural identities and sites, and move *in to* and *out of* criminal pathways (p. 29).

Along with Matza, the notion of digital drift is less interested in trait-based explanations and is more focused on the often unpredictable nature of deviance given the 'normality' of Internet use in everyday life as providing a readily accessible and indeed tempting setting for 'normal cyber-deviance' that are not trait-based or reliant upon a strong

[5] e.g. what search terms they have used in the past, what links they clicked where, they are located, who their friends are, the content of personal their emails, profile pages and comments, what images/videos they stop to watch, what posts they 'like', hashtags they follow and tweets they favorite, (amongst countless other data points).

socialized notion of a serious commitment to a criminal lifestyle (i.e. having explicit motivations, the requisite technical competencies for complex forms of engagement, or attachment to a criminal identity). In this way, we suggest that drift in the digital realm is both normal and commonplace within adolescent cohorts, a conclusion borne out in studies of youth attitudes to music piracy (e.g. Wingrove et al., 2011). In this sense we concur with Garland (2001 p. 128) that very often crime "requires no special motivation or disposition, no abnormality or pathology". Elsewhere, researchers flag the relationships between time spent online, and the increased likelihood of encountering delinquent materials online (Costello et al., 2016; Holt & Bossler, 2016). Drift therefore arises from the dynamic engagement between the attributes of the user, the features of the technology, and the uses made of it.

These features (or affordances) of Internet technologies and environments, we propose, can have profound implications for how crime is organized, and particularly for how adolescent delinquency arises. As noted, it is now possible for individuals to 'connect' or 'interact' through technology without themselves necessarily being 'networked' (see also Wellman et al., 2003) or at least maintaining said connections through consistent/persistent activities (Becker, 1960). Mediated communications over the Internet make *when*, *how* and *whether* communications take place very different than how they might occur in face-to-face encounters (Meyrowitz, 1997; Yar, 2005). Many approaches to crime analysis, including Social Network Analysis, typically place excessive reliance upon the co-presence of others (often in a physical sense), and current conceptions of "social ties' do not capture well the new ways of interacting and the types of associations that emerge through new forms of 'technologically mediated sociality" (Tufekci, 2008 p. 21). Following Sheller (2004, p. 39), we think the 'fluid' and 'gel-like' qualities of virtual encounters offer "opportunities for new kinds of publics to assemble or gel momentarily (and then just as quickly dissolve) as a result of newly emerging places and arenas for communication". Even more than before, adolescents are becoming "flexible constellations of identities on-the-move" (Sheller, 2004 p. 49), rendering their delinquent activities episodic and harder to predict, often easier to do and often trifling, and the result of individual, rather than group, manipulation of these digital environments and features.

Study Aims

This study provides a preliminary exploration of connections between the constituent concepts associated with the nascent stages of digital drift amongst a cohort of Australian adolescents. In particular, we explore what variables are associated with a variety of delinquent online encounters, and discuss implications and prospects for further criminal engagement. In the current context, this includes individual participant attributes (key demographic variables and propensity for risk-taking), access (to and preference for various technologies) usage (time online), technical competency (capabilities), interactional opportunities (exposure to online activities), and various types of delinquent online encounters.

Methodology

Participants and sample

The participants included an entire cohort of Year 8 students (n=43) at a metropolitan secondary school present on the day of data collection, and on whose behalf written consent to participate in the survey had been received from a parent/guardian (see Table 1 for sample description). The school itself was located in an affluent neighborhood of a large Australian city (greater than one million inhabitants), as confirmed by a high score on the *Socio-Economic Indexes for Areas* metric (Australian Bureau of Statistics, 2011).

Procedures

To examine the themes described above, this study draws upon quantitative data collected via a computer-assisted self-report survey, administered by the research team in-class across all homeroom classes over a two-day period in June 2016. Surveys took students on average 25 minutes to complete. Ethics approval was obtained through the host University Social and Behavioral Research Ethics Committee. Further approval was granted by the Head of School, as well as individual classroom teachers. Parents and students were required to provide their consent to participate in this project. Participants were assured that they would remain anonymous, and instructed that they could withdraw from the survey at any time without prejudice.

Measures and analytic strategy

This study uses a variety of measures, based on and adapted from several instruments previously validated by Holt and colleagues (i.e. Holt et al., 2011; Holt et al., 2010; Holt & Kilger, 2012; Li et al., 2015), to explore relationships between delinquent encounters and the key concepts associated with the nascent stages of digital drift - namely, access, usage, technical competencies, interactional opportunity, and participant attributes. Measures of such 'encounters' were constructed to determine the nature and extent of illicit online engagements. These measures were derived from self-report questions constructed to ascertain 12 delinquent encounters over the Internet (be they active or passive), across several thematic areas. These include forms of *harassment* that involve (1) communicating or searching for information about another person after being asked to stop; various forms of *illicit transactions* that include (2) stealing, or (3) buying/selling illicit items online; device *hacking* that involves (4) accessing another's device without permission; *sexual encounters* that involve (5) viewing, or (6) creating sexual/pornographic content; *encountering violence,* insofar as (7) viewing or, (8) creating content approving of violence toward others; *encountering discrimination and bigotry* which, entails (9) viewing or (10) creating content discriminating against others; and involvements that constitute *intellectual property infringements*, including (11) downloading or, (12) distributing copyrighted content. Participants were asked to provide information about the nature and extent of their engagements for each specific encounter (i.e., how often), and their intensity (i.e. the duration of each session). For analytical purposes, 12 separate items (constituent elements of each area) were summed and divided by 12 to create a measure of exposure (0-1) of delinquent Internet engagement where a score of one would represent 100% engagement with all 12 items and a score of zero would represent zero engagement with any.

The various conceptual elements of digital drift were measured in the following ways. First, *access* was measured using data collected about the spectrum of connected devices participants used to go online (e.g. smartphones, desktops, laptop/tablets), as well as device preferences (estimates of time spent using each device). Second, *usage* was measured as the participant's estimate of the average amount of time spent online daily across all devices.

Third, *technical competency* was measured by assessing a participant's relative competency (i.e. capabilities/digital literacy) using digital technologies (i.e. very/somewhat/not very/not at all comfortable with) using a variety of Internet services, software (e.g. installing applications, dealing with viruses/malware, programming, etc.) and hardware tools (e.g. using external peripherals, etc.). The items were summed to create a technical competency scale.

Fourth, *interactional opportunities* were measured by assessing the extent to which participants had taken up opportunities to access or create content online (based on 15 separate items). Access related items refer to a variety of simple, intermediate and advanced activities, including: (1) using search engines; (2) browsing social media; (3) streaming video and music; (4) seeking out new friends online; (5) banking; (6) shopping online; (7) using file-sharing programs to download/distribute software and music; (8) using VPNs; and, (9) using TOR to navigate the Internet anonymously. Content creation items include: (10) sending emails; (11) instant messaging; (12) uploading photos and videos; (13) engaging in video chats with others; (14) programming/scripting; and (15) working on a web page. In total, the 15 separate items were then summed and divided by 15 to create a measure of exposure (0-1) of generic Internet engagement where a score of one would represent 100% engagement with all 15 items whereas a score of zero would represent zero engagement.

Finally, we examined key related theoretical *individual attributes* including attitudes towards risk-taking behavior and whether respondents engaged in any broad types of offline delinquency. In terms of attitudes towards risk-taking, respondents were asked a series of six questions based on the six ratings of propensity for risk-taking drawn from the *National Longitudinal Survey of Youth, Children and Young Adults* administered in the United States. Respondents rated the following six statements on a four-point Likert scale (strongly disagree, disagree, agree, strongly agree): (1) I often get in a jam because I do things without thinking; (2) I think that planning takes the fun out of things; (3) I have to use a lot of self-control to keep out of trouble; (4) I enjoy taking risks; (5) I enjoy new and exciting experiences, even if they are a little frightening or unusual; and, (6) life with no danger in it would be too dull for me. The items were summed to create a scale reflecting propensity for risk taking, with higher scores reflecting greater willingness to engage in risky activities.

With respect to offline delinquency, respondents were asked whether they had ever engaged in any of the four following behaviors: (1) destroyed/damaged property; (2) stolen something that did not belong to them; (3) used illegal drugs; and, (4) beaten someone up. Respondents were also asked to indicate how many times they had engaged in each of these behaviors in the past 12 months, and whether and how often they were with others when they committed these behaviors.

Results

Participant characteristics and user attributes. As the sample was composed of a cohort of Year 8 students, participants were aged between 13 and 14. Table 1 shows that the gender of participants was evenly distributed (51.0% male, 49.0% female) and the overwhelming majority were Caucasian (92.9%). In terms of offline delinquency, given the small sample size and relatively low base-rate of self-reported delinquency, we recoded the four types of offline delinquency into a variable reflecting 'any' offline delinquency. Just under one-fifth of participants (18.6%) reported engaging in any form of such delinquency, and although males were overrepresented in reporting having engaged in delinquency, this relationship was not statistically significant. On the other hand, males were marginally more likely than females to score higher in terms of propensity for risk-taking.

Table 1. Individual attributes, access and usage

Participant characteristics and Internet use	Total sample (n=43) % / x(sd)
Participant attributes	
Gender	
Male	51.2%
Female	48.8%
Caucasian	92.9%
Risk-taking scale (α=0.74)	2.5 (0.5)
Delinquency (any/not online)	18.6%
Devices used to go online in the past year	
Desktop computer	53.5%
Laptop/tablet	100.0%
Smartphone	93.0%
Internet usage	
Avg. hours per day in last year spent online	4.7 (2.4)
Avg % of time on desktop computers[a]	15.1 (19.9) %
Avg % of time on Laptop/tablet	61.0 (24.2) %
Avg % of time on smartphone	33.5 (22.6) %

Access and *usage:* In this particular school, all students are provided with a laptop/tablet upon commencement of their studies, and accordingly, they have all used this medium to go online. The vast majority (93.0%) also reported using a smartphone to access the Internet, while approximately half indicated using desktop computer (53.5%). Participants reported an average of approximately five hours per day online (x=4.7, sd=2.4), and of this time, reported that approximately two-thirds of it (61.0%) was spent accessing the Internet on their laptop/tablets, followed by smartphones (33.5%) and finally desktop computers (15.1%).

Technical competencies: Participants were asked to rank their level of comfort performing various technical functions with software and hardware (measured as a five-point Likert scale). Table 2 shows the dichotomized proportion of participants who reported feeling either somewhat or very comfortable (comfortable, hereafter) performing selected tasks

(ordered according to the prevalence). The vast majority of respondents (i.e. >75%) reported feeling comfortable installing computer and smartphone software and setting up external hardware devices such as printers. Smaller proportions reported being comfortable with technical tasks involving installing/configuring networks (43.9%), using programming languages (39.5%), reinstalling operating systems (37.2%) and/or configuring antivirus/malware protection programs (35.7%). Finally, less than one-fifth of the participants reported being comfortable using alternate operating systems such as Linux (17.5%).

Table 2. Technical competencies

Item	Proportion reporting somewhat/very comfortable Total sample (n=43)
1. Adding ext. hardware (USB/printers)	83.7%
2.Installing software (computer)	81.4%
3. Installing software (smartphone)	76.7%
4. Installing/config. network at home	43.9%
5. Using comp. prog. Lang.	39.5%
6. Reinstalling an OS	37.2%
7. Antivirus/malware config.	35.7%
8. Using an OS like Linux	17.5%
Technical competency scale (α=0.87)	**x=2.7 sd=0.8**

Note. Digital literacy scale items coded as: 1=not at all comfortable, 2=not very comfortable, 3=somewhat comfortable, 4=comfortable, 5=very comfortable.

Interactional opportunities: In Table 3, the extent of Internet use and exposure to online activities is ordered by prevalence and frequency and are organized into two categories. The first is generic Internet activities that provide an overall measure of exposure to and familiarity with navigating the Internet. These items are those presented in Table 3 that are not bolded. The most prevalent types of online activity reported by a majority of participants (56-100%) involved such basic activities as using search engines, emailing, streaming videos or music, sending instant messages and social networking. These specific activities were also among the most frequent activities reported, all somewhere between several times a week to several times a day.

Delinquent online encounters: Table 3 also includes the various activities used to measure online encounters (bolded items). Just under one-third (30.2%) of participants reported they had illegally downloaded copyrighted material at some point previously, and just one-quarter (25.6%) reported viewing discriminatory material online. The next most commonly reported encounter was having viewed sexual content (11.6%), and the remaining forms were reported by a few individuals, with the frequency of specific activities suggests that they were infrequent and intermittent. Only five respondents reported viewing content online that encouraged violence, four accessed another person's

device over the Internet without permission, and one individual reported online theft or actively encouraged violence through online mechanisms.

Table 3. Interactional opportunities and cyber-deviance (n=43)

	Total sample (n=43)	
	Prevalence	Frequency, x(sd)
Ever used search engines	100.0%	4.5 (0.7)
Sent/received email[a]	97.7%	3.2 (1.4)
Streamed videos or music online[a]	95.3%	3.9 (1.4)
Sent instant messages[a]	93.0%	4.0 (1.5)
Uploaded personal photos or videos[a]	79.1%	1.6 (1.5)
Checked/posted messages to networking sites	74.4%	2.7 (2.1)
Sought out new friends on social media	62.8%	1.5 (1.7)
Used a webcam to send live video	62.8%	1.4 (1.5)
Shopped in online stores	55.8%	0.7 (0.9)
Illegal download	30.2%	0.6 (1.2)
Seen discriminatory material	25.6%	0.3 (0.4)
Computer programming/scripting[a]	25.6%	0.5 (1.0)
Worked on a personal website[a]	18.6%	0.3 (0.9)
Used a VPN[a]	14.0%	0.2 (0.6)
Ever done online banking[a]	14.0%	0.2 (0.7)
Seen sexual content[a]	11.6%	0.2 (0.7)
Seen online content encouraging violence	11.6%	0.1 (0.3)
Used file sharing programs[a]	9.3%	0.1 (0.5)
Accessed another person's device	9.3%	0.2 (0.6)
Used programs such as TOR[a]	2.3%	0.1 (0.5)
Stolen something online	2.3%	0.0 (0.2)
Encouraged violence online	2.3%	0.0 (0.2)
Illegal upload	0.0%	-
Taken revealing pictures of self or others	0.0%	-
Sent or posted discriminatory material	0.0%	-
Bought/sold something illegal	0.0%	-
Harassment of others	0.0%	-

Note. Cyber-deviance items bolded. Frequency based on the following scale: 0=never, 1=less than weekly, 2=once x week, 3=several x week, 4=once x day, 5=several x day.
a. Low expected cell counts

Table 4 (Part A) displays scales measuring the variety of delinquent encounters and non-delinquent online activity of participants in the study. The entire cohort, unsurprisingly, admitted to non-delinquent activities online. However, the average score on the variety scale was 0.5, indicating that on average, participants engaged with approximately half of the non-delinquent online activities queried.

Overall, approximately half (48.8%) of respondents reported having a delinquent online encounter in one form or another. Among these respondents, the average score on the

variety scale of online delinquency was 0.1, indicating that on average these individuals encountered only approximately 10% of the items queried, or in other words, only a single form of delinquent encounter. Given the low Cronbach alpha value for this scale, individual items were scrutinized further (see Table 4). The intermittent engagement with delinquency online was reflected to some extent in terms of the modal duration of engagement in delinquent activities. As illustrated in Table 4 (Part B), modal duration amongst delinquent encounter items was episodic for nearly all participants at 0-5 minutes per session.

Table 4. Nature and extent of cyber-deviance

A.	Total sample (n=43) x(sd), range
Interactional opportunities	
Prevalence	100.0%
Variety (α=0.63)$_a$	0.5 (0.1) range= 0.3-0.9
Cyber-deviance	
Prevalence	48.8%
Variety(α=0.49)$_a$	0.1 (0.1) range= 0.0-0.3
B. Modal duration of activities for those reporting cyber-deviance items	
Illegal download (n=12)	0-5min
Seen discriminatory material (n=10)	0-5min
Seen sexual content (n=5)	0-5min
Accessed another person's device (n=4)	6-15min
Seen online content that encourages violence (n=4)	0-5min
Encouraged violence online (n=1)	0-5min
Stolen something online (n=1)	-
C. Exposure types cyber-deviance (prevalence)	
Intellectual property infringements	30.2%
Discrimination and bigotry	25.6%
Advocating violence	14.0%
Sexual activity$_b$	11.6%
Hacking	9.3%
Illicit transactions	2.3%
Harassment	0.0%

Note. Section B: respondent that indicated they stole something online did not report the duration of the activity.
a. Variety scales = sum of different activity per category/#of items. Internet use and familiarity = 15 items. Cyber-deviance: maximum variety score = 12 items.

Table 4 (Part C) displays the prevalence of delinquent encounter response items arranged according to the seven thematic areas of involvement. Here, the most prevalent

encounters were evident in the conceptual category of intellectual property infringements, just under one-third of the sample (30.2%) reported engaging in these activities. This was followed by both active and passive encounters involving discriminatory (25.0%) violent (14.0%) and sexual (11.6%) content. Only one individual reported engaging in illicit transactions and none reported perpetrating harassment online.

We conducted a series of Pearson correlations to explore some preliminary conceptual relationships between delinquent encounters and the other variables pertinent to the concept of digital drift examined in this study (Table 5). Males scored marginally higher on propensity for risk-taking than females (r=0.27, $p<.10$), higher on technical competency (r=0.40, $p<.01$), and were more likely to access, or come across, sexual content online (r=0.35, $p<.05$) in keeping with prior research (e.g. Holt & Bossler, 2016; Marcum et al., 2014). Not surprisingly, there was a moderate correlation between propensity for risk-taking and offline delinquency; those scoring higher on propensity for risk-taking were more likely to report engagement in offline delinquent behaviors (r=0.47, $p<.01$). A similar relationship was evident with respect to delinquent online encounters; those scoring higher on propensity for risk-taking showed more engagement in terms of the variety of online encounters (r=0.46, $p<.01$). Furthermore, there were similarly moderate correlations between risk-taking and the specific types of online encounter, with the exception of hacking and illicit transactions. Though these two latter forms of deviance were among those with the lowest prevalence in the sample, they may also reflect the connection between higher levels of self-control and involvement in serious forms of cybercrime generally (see Holt & Bossler, 2016 for review).

Table 5. Correlation matrix

Item.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
1. Gender[a,b]	-	.27+	.11	.40**	-.07	.02	-.07	-.17	-.01	.35*	.15	-.16
2. Risk-taking scale		-	.47**	.30+	-.10	.46**	.27+	.31*	.30*	.38*	.17	-.05
3. Any delinquency (offline)			-	.22	.27	.45**	.47**	.41**	-.02	.20	.05	.32*
4. Technical competency scale				-	.08	.03	-.02	.13	-.05	.09	-.15	.14
5. Interactional opportunities variety scale					-	.15	.06	.39**	.02	-.21	.07	.07
6. Cyber-deviance variety scale						-	.80**	.51**	.56**	.54**	.45**	.28
7. Intellectual property infringement[b]							-	.31*	.17	.39**	.31*	.23
8. Discrimination and bigotry[b]								-	.07	-.05	-.19	.26
9. Advocating violence[b]									-	.27	.33*	-.06
10. Sexual activity[b]										-	.13	-.06
11. Hacking[b]											-	-.05
12. Illicit transactions[b]												-

+$p<.10$, *$p<.05$, ** $p<.01$

Note.

a. 0=female, 1=male.

b. Point-biserial correlation.

As expected, technical competency was not related to any of the online delinquent encounter items. This may be due to the fact that delinquent encounters online are predominantly of a less serious nature and do not necessarily require stable criminal commitments (and thus enhanced technical capabilities). On the other hand, interactional opportunities scale was associated with at least one form of delinquent encounter: viewing

discriminatory content (r=0.39, p<.01). As we hypothesize above, and consistent with the previous work of Costello et al. (2016), it is suggested that these individuals may be more likely to come across such material, either intentionally or unintentionally, through increased exposure to opportunities online. These results possibly point to differences in how young adolescents come across and engage with different materials online. The likely influence of offline activities and associations, as well as the different affordances encountered through online activity, requires further examination in future research.

At the same time, the results point to some congruence between online and offline delinquency, and may emerge quite early in adolescence. In this sample of young adolescents, there were moderate to strong correlations between having engaged in offline delinquency and delinquent online encounters (variety measure) (r=0.45, p<.01). Furthermore, relationships were also evident between offline delinquency and specific types of online encounters, particularly intellectual property infringement (r=0.47, p<.01) and discrimination and bigotry (r=0.41, p<.01). Again, although these findings are based on a small sample, the results suggest some association between delinquency in the real-world and online, consistent with other larger studies (e.g. Udris, 2016). Moreover, the results from this current analysis indicate that there may be specific patterns in terms of the development of delinquency and engagement in particular forms of problematic online behavior (see also Holt & Bossler, 2016).

Discussion

The current exploratory study was based on a small cohort of early teenagers in Australia and the findings offer some important initial insights into the emergence of adolescent delinquency in digital contexts. Overall, delinquent encounters, on- and offline were reported by a considerable proportion of the participants. Adolescents experiencing such delinquent encounters can be characterized by a higher propensity for risk-taking than their non-delinquent counterparts, and their online activities paralleled offline delinquency (e.g. Holt & Bossler, 2016; Marcum et al., 2014). While some forms of online encounters were more prevalent than others, particularly intellectual property infringement and viewing discriminatory material, the findings are too preliminary to suggest whether specific developmental pathways are evident. Any specific relationships that emerged between these delinquent online encounters may simply be artifacts of a relatively high base-rate of those activities within a relatively small sample.

Nonetheless, these results shed initial insight into the early encounters of some young adolescents with delinquent behavior in a digital world. On the one hand, pirating content using the Internet is an active engagement where youth may or may not know, appreciate or care about any potential consequences of their actions (see Holt & Bossler, 2016 for review of these themes). On the other hand, the implications of inadvertently stumbling across particular content on the Internet, be it discriminatory, sexual, violent or otherwise, are not well understood in terms of their impact or influence subsequently on other aspects of online delinquency (Diamond & Bachmann, 2015). The adolescents in the current study reported a vast range of, and frequent, engagement with digital technologies and the Internet which increases the likelihood of exposure to what may be considered deviant or harmful material. Participants reported using search engines, streaming media, and communicating digitally once a day or more, making it more likely that they

experience 'accidental' or 'unpredictable' exposure to deviant material or delinquent others.

As with certain types of crimes, certain forms of online delinquency have a higher requisite skill level (e.g. hacking). What is clear in the current study is that among young adolescents, more complex forms of online delinquency had yet to emerge. As educational institutions increasingly focus on early skills development in technical knowledge (e.g. coding classes at school, exposure to new technologies) it will be critical to understand if and when this exposure plays a role in engaging in new or more complex illicit behaviors.

In terms of engagement in online deviance, while about half of the sample reported having any delinquent online encounters, their overall involvement was sporadic or intermittent at best. Of these adolescents, the modal duration across the wide range of delinquent online activities reported was very low (i.e. 0-5 minutes total session duration), suggesting very low engagement with these type of behaviors, and rather, likely reflect more a fleeting curiosity. Elsewhere, new media scholars have noted different degrees of online engagement by users, including the category of 'timid encounters' (see Bossewitch & Sinnreich, 2012). At this stage of life, we might anticipate more 'timid encounters' than a few years later into adolescence. Such early tentative engagements are certainly consistent with the idea of being a step on a pathway to greater criminal engagement, or alternately could reflect the outer limit of some users' exposure to risky Internet behavior. Although the sample is small, the base rate of both delinquency (digital and of a non-digital kind) is relatively low and in line with what would be expected based on samples from the general population, particularly from among young adolescents. Future work studying such pathways into criminality would be well served to not only study larger adolescent cohorts, but also to track the patterns, and especially the escalation, of involvements (whether it be seriousness, frequency, or intensity of delinquent activities online) longitudinally over time. Recognizing this gap, the authors have embarked upon such a longitudinal project, funded through the Australian Research Council, involving a larger cohort of adolescents across secondary schools in a large Australian city.

Conclusion

The aim of this study was to explore the potential basis for early pathways into cybercrime through a review of pertinent theoretical literature, and particularly *digital drift* (Goldsmith & Brewer, 2015), and to undertake an empirical exploration of associated variables via a study of a cohort of Australian adolescents. The results of this study provide some initial empirical evidence on relationships between the prevalence of online delinquent encounters among adolescents and their uses of various technologies and services (including interactional opportunity and usage). It also showed that the nature and extent of these encounters by this cohort appeared to be in their infancy, with delinquent involvements being episodic and at the least-serious end of the spectrum. The results also suggest the importance of other developmental considerations pertinent to adolescents, including measures of risk-taking and delinquency in offline settings.

We acknowledge that this study suffered from several methodological limitations. First, it is based on a small convenience sample from a single school in an affluent Australian suburb. Therefore, the results cannot be generalized to other contexts in either developed and/or developing nations. Furthermore, in terms of developing nations, differences in technical infrastructure compared to developed nations possibly may introduce stark contrasts with respect to the nature and extent of delinquent encounters online, and is

therefore a crucial area for future research. However, given the exploratory objectives of the study, we believe the results offer some initial insights into potential mechanisms associated with engagement in cyber-deviance. Future research should explore the reliability and validity of the concepts explored in the current empirical study, particularly those concerning technical competency and interactional opportunities. Furthermore, another crucial question that emerges from this current study is whether online delinquency manifests differently across different populations, particularly when vulnerable segments of the community are included. Finally, the exploratory work described in this article echoes calls made elsewhere (see Diamond & Bachmann, 2015; Holt & Bossler, 2016) for further robust longitudinal study of Internet-mediated delinquency.

Acknowledgements

The authors thank Tahlia Hart, Caitlan Miller and Morgan Sayer for their research and administrative assistance. We also thank the anonymous reviewers for their helpful comments on an earlier draft of this article. This project was funded by an Australian Research Council Discovery Project Grant (DP170103538).

References

Australian Bureau of Statistics. (2011). *Census of population and housing: Socio-economic indexes for areas (SEIFA), Australia, 2011,* (Catalogue No. 2033.0.55.001). Retrieved from http://www.abs.gov.au/ausstats/abs@.nsf/mf/2033.0.55.001.

Becker, H. (1960). Notes on the concept of commitment. *The American Journal of Sociology, 66*(1), 32-40.

Bennett, S., & Maton, K. (2010). Beyond the digital nativesdebate: Towards a more nuanced understanding of students' technology experiences. *Journal of Computer-Assisted Learning, 26*(5), 321-331.

Bossewitch, J., & Sinnreich, A. (2012). The end of forgetting: Strategic agency beyond the panopticon. *New Media & Society, 15*(2), 224-242.

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

Burnay, J., Billieux, J., Blairy, S., & Larøi, F. (2015). Which psychological factors influence Internetaddiction? *Computers in Human Behavior, 43*(2), 28-34.

Cisco. (2015). *The zettabyte era: Trends and analysis*. San Jose: Cisco Systems.

Cloward, R. & Ohlin, L.E. (1960). *Delinquency and opportunity: A theory of delinquent gangs*. New York: Free Press of Glencoe.

Costello, M., Hawdon, J., Ratliff, T., & Grantham, T. (2016). Who views online extremism? Individual attributes leading to exposure. *Computers in Human Behavior, 63*, 311-320.

Diamond, B., & 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.

Erikson, E. (1968). *Identity: Youth and crisis*. New York: W W Norton & Company.

Felson, M. (2006). *Crime and nature*. Los Angeles: Sage.

Furman, W., & Shaffer, L. (2003). The role of romantic relationships in adolescent development. In P. Florsheim (Ed.), *Adolescent romantic relations and sexual behavior:*

Theory, research, and practical implications (pp. 3-22). Mahwah: Lawrence Erlbaum Associates Publishers.

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Chicago: University of Chicago Press.

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

Green, L., Brady, D., Ólafsson, K., Hartley, J., & Lumby, C. (2011). *Risks and safety for Australian children on the Internet*. Brisbane: ARC Centre of Excellence for Creative Industries and Innovation.

Havighurst, R. (1972). *Developmental tasks and education*. New York: Appleton & Company.

Hawdon, J. (2012). Applying differential association theory to online hate groups: A theoretical statement. *Research on Finnish Society*, 5, 39–47.

Holt, T., & Bossler, A. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40.

Holt, T., & Bossler, A. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. New York: Routledge.

Holt, T., Bossler, A., & May, D. (2011). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice, 37*(3), 378-395.

Holt, T., Burruss, G., & Bossler, A. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice, 33*(2), 31-61.

Holt, T., & Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime & Delinquency, 58*(5), 798-822.

Inhelder, B., & Piaget, J. (1999). *The growth of logical thinking from childhood to adolescence*. London: Routledge.

Kroger, J. (2003). Identity development during adolescence. In G. R. Adams & M. D. Berzonsky (Eds.), *Blackwell handbook of adolescence* (pp. 205-226). Malden: Blackwell.

Lanier, J. (2010). *You are not a gadget: A manifesto*. New York: Knopf (Random House).

Lenhart, A. (2015). *Teens, social media &technology overview 2015*. Washington: Pew Research Center.

Li, C., Holt, T., Bossler, A., & May, D. (2015). Examining the mediating effects of social learning on the low self-control—cyberbullying relationship in a youth sample. *Deviant Behavior, 37*(2), 126-138.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L., (2014). Sexting behaviors among adolescents in rural North Carolina: A theoretical examination of low self-control and deviant peer association. *International Journal of Cyber Criminology 8(2),* 68-78.

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

McEwan, R., & Wellman, B. (2013). Relationships, community, and networked individuals. In R. Teiglund & D. Power (Eds.), *The immersive Internet: Reflections on the entangling of the virtual with society, politics and the economy* (pp. 168-179). Basingstoke: Palgrave MacMillan.

Meyrowitz, J. (1997). Shifting worlds of strangers: Medium theory and changes in 'them' versus 'us'. *Sociological Inquiry, 67*(1), 59-71.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you 2011*. New York: Penguin Press.

Passini, S. (2013). A binge-consuming culture: The effect of consumerism on social interactions in Western societies. *Culture & Psychology, 19*(3), 369-390.

Pombeni, M., Kirchler, E., & Palmonari, A. (1990). Identification with peers as a strategy to muddle through the troubles of adolescent years. *Journal of Adolescence, 13*(4), 351-369.

Prensky, M. (2001). Digital natives, digital immigrants part 1. *On the Horizon, 9*(5), 1-6.

Reyns, B., Henson, B., & Fisher, B.(2011). Being pursued online: Applying cyberlifestyle -routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.

Sheller, M. (2004). Mobile publics: Beyond the network perspective. *Environment and Planning: Society and Space, 22*(1), 39-52.

Steinberg, L. (2008). *Adolescence*. New York: McGraw-Hill.

Stickel, L. H. (2017). Digital natives and digital immigrants: Exploring online harassment victimization by generational age. *International Journal of Cyber Criminology, 11(1),* 39-62.

Subrahmanyam, K., & Šmahel, D. (2011). *Digital youth: The role of media in development*. New York: Springer.

Tanner, J. (1978). *Growth at adolescence*. Oxford: Blackwell.

Tapscott, D. (1998). *Growing up digital: The rise of the Net generation*. New York: McGraw Hill.

Tucker, P. (2014). *The naked future: What happens in a world that anticipates your every move?* New York: Current (Penguin Group).

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science Technology & Society, 28*(1), 20-36.

Udris, R. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: A cross-national study. *International Journal of Cyber Criminology, 10*(2), 127-146.

Vaidhyanathan, S. (2011). *The Googlization of everything (and why we should worry)*. Berkeley, CA: University of California Press.

van der Hof, S., & Koops, B. (2011). Adolescents and cybercrime: Navigating between freedom and control. *Policy & Internet, 3*(2), 1-28.

Weinstein, E., & Rosen, E. (1991). The development of adolescent sexual intimacy: Implications for counseling. *Adolescence, 26*(102), 331-339.

Wellman, B., Quan-Haase, A., Boase, J., Chen, W., Hampton, K., Diaz, I., & Kakuko, M. (2003). The social affordances of the Internet for networked individualism. *Journal of Computer-Mediated Communication, 8*(3). doi: 10.1111/j.1083-6101.2003.tb00216.x.

Wingrove, T., Korpas, A., & Weisz, V. (2011). Why were millions of people not obeying the Law? Motivational influences on non-compliance with the Law in the case of musical piracy. *Psychology, Crime, and the Law*, *17*(3), 261-276.

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