Online Risk for People with Intellectual Disabilities

Dr. Darren D. Chadwick
The University of Wolverhampton

Abstract

Purpose: This review summarises the current state of empirical knowledge pertaining to online risk and cybercrime relating to people with intellectual disabilities (ID).

Approach: This narrative review summarises, synthesises and critically evaluates the current literature and state of knowledge and offers suggestions for extending current knowledge and practice.

Findings: Evidence regarding risk for people with ID is limited but growing. Existing findings highlight that: (i) risk may increase contingent upon higher levels of sociability, loneliness, anxiety and depression, poorer insight, judgement, discrimination and ability to detect deception online and reduced experience and life opportunities; (ii) people without ID perceive high online risk for people with ID which may lead to gatekeeping restrictions and controlling digital access; (iii) restriction may potentially impede online self-determination, participation and development by people with ID; (iv) experience of risk may enhance awareness, independence and resilience in managing future online risk amongst people with ID. Further research work is needed in this area to enhance understanding of risk experience and effective support strategies.

Originality/value: This review of current knowledge has highlighted the necessity for more research to better understand the propensity for engagement in different risky online behaviours and to better inform support practices to help people with ID to manage risk whilst maintaining digital inclusion.

Keywords: Online risk, Resilience, Cybercrime, Digital Inclusion

Introduction

Technology is increasingly intertwining with everyday life and is viewed as a basic human right. A digital divide remains between typically-developing individuals and people with disabilities, with inequity in technology usage, access and possession (Chadwick et al., 2019). A contemporary area of associated research is that of digital risk for people with ID. A core narrative surrounding people with ID is that of being eternal children with increased vulnerability (Pueschel and Scola, 1988). The risk of offline victimization and some types of offending appear greater (Gravell, 2012; Lindsay et al., 2011), but incidence of online victimization and perpetration are seldom studied within ID populations, so the scope and scale of online criminal activity and victimisation remains unknown. Research has highlighted the potential social, developmental, leisure, civic and informational benefits of being online, yet people with ID experience increased digital exclusion (Chadwick et al., 2019). This paper reviews existing literature on online risks for people with ID.

Method

This narrative review was developed from empirical and conceptual literature considering online risk for people with ID. Papers were gathered from recent review work focussing on the experiences and benefits of digital inclusion (cf. References omitted for anonymous review purposes). Papers were sourced from databases (EBSCO, Psychoinfo, Web of Knowledge) using search terms outlined in prior papers and subsequently reviewed for relevance. Papers deemed relevant to the review topic were selected.
Findings

Online Risk and Cybercrime

Alongside advances in technology and increased expectations of technological competence, there have been increases in societal concerns regarding cybercrime, cyber-deviance and associated online risks (Merritt, 2010). Typologies of cybercrime and online risk have been developed, but vary in how they have been explored and verified empirically, rarely being applied to people with ID. Wall (2002) distinguished four cybercrime categories: (i) cyber-deception and theft; (ii) cyber pornography; (iii) cyber-violence; and (iv) cyber-trespass, (involving unlawfully accessing others’ technology). Kirwan and Power (2012) identified three types of cybercrime: Internet-enabled crime (e.g. online grooming, hate sites, money laundering), Internet-specific crime (e.g. hacking, spreading viruses), and crimes in the virtual world (e.g. crimes against avatars).

European research work on online risk for young typically-developing people describe three primary risk types: (i) Exposure to harmful, manipulative or exploitative content (e.g. harmful sexual material, scams); (ii) Experiencing negative contact online (e.g. being bullied, being groomed for sexual contact/ radicalisation); and (iii) Engagement in criminal or antisocial behaviour or conduct (e.g. online bullying, trolling or flaming, sending inappropriate content) (Livingstone and Haddon, 2009). This typology was adapted to gather perceptions of the likelihood of different online risk for people with ID (e.g. Chadwick et al., 2017), however the appropriateness of adapting a typology based on young people without ID to those with ID is contentious. A framework specific to people with ID has been suggested (Seale and Chadwick, 2017). Moreover, the hypothesized negative impact of some online behaviours classified as risky (e.g. watching violent content or pornography) is contentious and sometimes lacks empirical verification.

These aforementioned typologies may inform studies identifying prevalence and experiences of online risk and cybercrime but whether they encompass the main risk for people with ID is debatable. Digital exclusion is arguably a greater risk to wellbeing than other more obviously negative and risky aspects of being online (Chadwick, under review), but is less likely to be considered a risk. Many services, such as banking, access to health, social care and welfare systems, are increasingly accessed online. If people with ID are to be full members of society, then they also need access to digital technology. The Internet can also be used to challenge social and digital exclusion, though change will likely require ongoing advocacy and political pressure from people with ID and their allies (Chadwick et al., 2013; Chadwick and Wesson, 2016).

Perceptions of risks to people with ID of information and communication technology use

Negative beliefs regarding the Internet and people with ID are likely to influence inclusive digital design, gatekeeping and digital inclusion and have received attention in the literature.
General population perceptions of risk

Members of the general population without disabilities rate people with ID at greater online risk compared with self-ratings (Chadwick et al., 2017). Risks perceived as greatest included being bullied, threatened or harassed online, being susceptible to online marketing scams and providing too much personal information. Shpigelman and Gill (2014) suggest that using social media and the potential loss of privacy may pose a greater risk to people with ID due to potential stigmatisation. Perceptions and concerns about increased vulnerability and the ability of people with ID to manage online risk may contribute to digital exclusion (Seale and Chadwick, 2017).

Carer and professional perceptions of risk

Carers similarly view people with ID as having heightened levels of risk online. A qualitative investigation of professional and parent views of Internet use for the purposes of love and sex found that young people with ID were viewed as more vulnerable than other young people (Löfgren-Mårtenson et al., 2015). Molin et al. (2015) found that parents and teachers had anxieties about online risks. Teachers had concerns regarding isolation, comprehension of Internet content accuracy and around naivety online. Parents were concerned about children trying new things, that they may be too trusting, unable to detect deception and more sensitive to content and contact online. However, this was balanced with reported benefits where teachers noted that some students with ID were too cautious in seeking activities on the Internet. Participants viewed both risks and benefits as greater for people with ID.

Differences in perception of risk between carers and people with ID

Löfgren-Mårtenson (2008) highlighted the discrepancy between perceptions from people with ID and those providing support regarding potential online benefits and risks. They found that support staff had more negative perceptions of being online, seeing it as unsuitable for young people with ID. Young people however had more positive perceptions about the Internet. Lough and Fisher (2016a) compared vulnerability ratings of 102 pairs of people with Williams syndrome and their parents. Parents reported higher vulnerability whereas people with Williams syndrome viewed themselves at less risk. This may lead to a potential disconnect between the wishes of people with ID and their carers around Internet use.

Experiences and awareness of risk

Accounts of being online are increasing, however few investigations have explored the experiences of online risk, deviance and cybercrime amongst people with ID. Empirical evidence that people with ID are at comparatively greater risk of online victimisation is also sparse.

Holmes and O’Loughlin (2014) found that social media presented cyber bullying sites, unwanted messages and being targeted for financial and sexual exploitation. Buijs et al. (2017) described three composite case vignettes, based on actual clinical cases of adolescents and adults with 22q11 deletion syndrome highlighting incidents of severe sexual and financial online victimisation. Sallafranche-St-Louis and
Normand (2017) interviewed eight people, five with ID and two who were autistic. Seven reported distressing online experiences, including being insulted, having false rumours spread and being targets of sexual solicitation. Conversely, a survey study of the prevalence of mobile phone and Internet cyberbullying found a reduced likelihood of children with ID being victims of cyberbullying (7%) (Didden et al., 2009). Although this is a positive finding, the authors counter-intuitively concluded the need to develop programmes to prevent cyberbullying and for more parental control (Seale, 2014).

Digital exclusion, underpinned by societal and individual factors, may interact with gatekeeping to reduce exposure to digital risk. Risks are likely to vary between individuals. An individual support approach may prove useful in preventing or managing risk (Seale and Chadwick, 2017). Future research should explore experiences of specific risks and cybercrimes amongst distinct groups of people with ID with particular support needs.

Recent research has begun to quantitatively explore the prevalence of online risk experience. A cross sectional study of 77 adults with ID found people were being blocked from online groups or activities (48%), insulted (46%), threatened (35%), sent unwanted sexual media (35%) and had other people using their passwords without consent (36%) (Chiner et al., 2017). Caregivers (n=68) were also surveyed and 39% reportedly ignored the problems those they cared for had encountered online. These included: being insulted (66%), being told unpleasant things (60%) and being blocked (50%). Though seldom self-reported, people with ID also engaged in anti-social behaviours including being insulting, threatening or engaging in unwanted flirting. Caregivers reported engagement in these anti-social and inappropriate online behaviours more than the people with ID did, suggesting possible social desirability bias in self-reporting.

Contrary to the findings of increased risk, research with adults with ID who had low support needs suggested few risks were experienced (Chadwick, under review). Where there were risks, these seldom reduced wellbeing. Instead respondents utilised their social networks to gain support, building resilience by either developing awareness and skills to manage future risks, or excluding themselves from previous online risks. Awareness of risk was evident in participants and linked with the amount of use and interest in the digital world.

Whether risk is associated with particular technology usage patterns has not been adequately explored. However, Jenaro et al., (2017) found that young people with ID were significantly more likely to have moderate to severe mobile phone (19.4% vs. 8.0%) and Internet addiction (27.3% vs. 7.8%), based on DSM-V criteria, than typically developing peers. Whether these criteria represent pathology or the normal range of use for a group that tends to be socially disadvantaged or excluded is debatable. There certainly exists controversy over the notion of Internet addiction (Kardefelt-Winther, 2017). Nonetheless, problematic Internet use remains understudied in people with ID.
Risk factors for online victimisation of people with ID

Limited available literature highlights various factors that may be at play in underpinning the belief that people with ID are more vulnerable. Understanding of online content, the ability to discern the accuracy of online information and to detect online deception were viewed as more challenging for people with ID by carers and teachers (Molin et al., 2015). Plichta (2010) stated that the characteristics of modern technology in concert with the perceived lack of success, need for acceptance, and limited social skills of people with ID can have negative repercussions online. Norman and Sallafranque-St-Louis (2016) highlighted loneliness and depression as possible factors increasing the potential for online sexual victimization. Poorer insight, awareness and judgement were also reported by Buijs et al. (2016) as predisposing factors to increased risk.

Phenotype-related predispositions may also underpin elevated risk. People with Williams syndrome often display a pro-social drive to engage. Lough and Fisher (2016b) presented e-safety scenarios to 28 people with Williams syndrome and found participants were more likely to engage in socially risky behaviours (e.g. meeting a stranger offline) compared with non-social risks (e.g. sharing bank account information after winning a contest).

Jenaro et al. (2017) found that greater mobile phone use predicted Internet use and vice versa, and that depression and unhealthy behaviours also predicted overuse. They cite the need for further research into causal factors that may increase risk for young people with ID and whether lack of opportunities in other aspects of life (lack of ability to discriminate, reduced functional ability, reduced confidence or self-determination and choice-making) are influential. They also suggested reduced opportunity for relationships, making friends and participation in leisure activities as possible causal factors, linked with increased loneliness.

Wright (2017) in a survey of young autistic people (some with ID), found experience of cyber-victimization was associated positively with anxiety, depression and loneliness. It also supported parental mediation of technology-use as protective against the negative adjustment consequences associated with cyber-victimization. This demonstrates a complex and conflicting relationship between support, autonomy and resilience as protective against online risk and merits further exploration.

Recent evidence from qualitative research suggests young people with ID demonstrate awareness of online risk (Löfgren-Mårtenson et al., 2015; Bannon et al., 2015). Bannon et al., (2015) conducted focus groups with 38 young people with ID, some of whom were autistic and some of whom had social, emotional and behavioural difficulties and highlighted that some individuals had good understanding of online risk and built coping strategies and resilience from their experiences. However, some participants lacked understanding of risks and this related to more risk-taking behaviour. A number of young people also took intentional risks and linked this to peer influence. To better illuminate support for online risk future research should seek to better disaggregate people based on phenotypic and diagnostic support needs.
**Support, Protection & Restriction in Managing Online risk**

Paid and family carers perceive people with ID to be more vulnerable to online crime and deviant behaviour and thus in greater need of protection and safeguarding. Carers of people with ID can act as gatekeepers controlling and monitoring access to ICT potentially undermining skill development, self-determination and digital participation (Bannon et al., 2015; Löfgren-Mårtenson et al., 2015; Seale and Chadwick, 2017). Bannon et al. (2015), found restriction varied among young people interviewed with supervision and monitoring put in place by some parents, along with blocks on sites. Some of the young people reported circumventing these gatekeeping strategies and protective controls because they were more technologically skilled than their parents.

There have been calls for a less risk-averse approach in supporting people with ID to use technology and the Internet (see Seale and Chadwick, 2017). Arguments have been made for a model of positive risk-taking (Alaszewski and Alaszewski, 2002) incorporating creativity, possibility thinking and resilience (Seale, 2014). In their study of typically developing young people, Livingstone et al. (2015) found that exposure to opportunities brings exposure to increased risk and efforts to reduce risk may concurrently reduce opportunities. Exposure to more risks did not always lead to greater harm. The negative impacts and protective properties of experiencing online risk and cybercrime need further exploration.

Encouraging supporters to avoid underestimating the ability of those they support to cope with online risk and to recognize resilience is one potential solution to enable more self-advocacy and determination online. This might be facilitated via interdependent collaborations between those providing and receiving support (Chadwick and Fullwood, 2018; Seale, 2007; Seale and Chadwick, 2017). Indeed, people with ID do look to others for support, guidance and advice, including peers, parents and other family members (Bannon et al., 2015; Chadwick, under review).

Some practical guides exist about staying safe online for people with ID (e.g. Foundation for People with Learning Disabilities, 2014). Empirical investigation of the development, processes and efficacy of these interventions in promoting online knowledge, understanding and resilience, appropriate support-seeking, and prevention of online risk is limited with few intervention studies. Some research has encouraged introducing protocols into home settings to manage risk and training for staff and people with ID prioritising online safety concerns (e.g. Lough and Fisher, 2016b; McLimens and Gordon, 2008).

Holmes and O’Loughlin (2014) developed a psycho-educational therapeutic group to address the negative online experiences of people with ID. Self-esteem and assertiveness training were delivered, providing service users with skills to enable better informed decision-making regarding what was safe to share online. A greater willingness to say ‘no’ when they were online was also encouraged. Participants reported enhanced confidence in problem-solving and discussing online risk. The authors also remarked that some strategies and supports put in place by agencies (e.g. Facebook, UK Child Exploitation and Online Protection Centre) to support online safety required a level of digital literacy which may serve to exclude young people with ID.
Discussion

Research work focussing on the digital inclusion of people with ID is growing, with most being survey-based or qualitative and small scale. Some groups of people with ID are currently not considered, for example, older adults with ID, those with mental health issues alongside their intellectual disability, those living in the global south and people with profound and multiple ID. With increased digital inclusion comes increased exposure to potential online risks and cybercrime alongside increased opportunity for engagement in anti-social online behaviour. Existing evidence suggests that there may be some predisposing factors that put people with ID at increased risk (e.g. difficulty discerning deception online and loneliness) but that this is tempered by digital exclusion making the actual prevalence of risk experiences difficult to determine. Moreover, taking a risk-averse approach may not be in the best interests of people with ID, and may serve to further increase digital exclusion preventing development of online competence and resilience.

Further intelligence gathering is needed regarding how to provide sensitive, warm and facilitative support around online risk to people with ID. The literature on support appears to be growing but tends to lack well-controlled experimental designs which can enhance the credibility of causative assertions regarding the benefits of particular support strategies. These strategies also often focus on young people, excluding adults and older people. More evaluation of support strategies applied to all stakeholder groups is needed. Service providers should consider incorporating such work into the online safety training they develop and commission for support staff, families and people with ID.

A one size fits all approach will not suffice for supporting people to manage online risk. Individual factors including cognitive levels of attention, information processing, conceptual and sequential processing and memory need to be considered alongside people’s motor and sensory functions, including visual and auditory impairments. Behavioural phenotypic characteristics may also play a role in increasing potentially risky behaviour online.

Despite needing to take an individual approach to supporting people with ID to get online and stay safe, existing literature demonstrates some practical, conceptual and ideological considerations that may benefit support staff, family carers and other stakeholders.

When considering whether to support someone to access the online world, the human rights pertaining to digitally including people may provide useful leverage when advocating for support and arguing against digital exclusion. Being online forms a large part of societal interaction, and is considered by some to be a human rights issue in relation to articles 9 (Accessibility), 12 (Right to equal recognition before the law), 19 (Right to be included within the community), and 21 (Freedom of expression and opinion). Belief in online freedom of online expression and self-determination is embodied with Article 21 of the UNCRPD. Hence excluding people with ID due to concerns regarding risks is not an appropriate solution for those countries which have ratified the convention. Policy makers need to adequately support research endeavours to better support digital inclusion and identify effective ways to support online risk taking and management.
Whether someone with ID has the capacity to engage safely with the Internet should also be considered closely and with detailed observation and analysis of each individual's abilities, needs and wishes. This is best decided alongside the person with ID, their carer or family member and appropriate supports from practitioner groups e.g. psychologists, occupational therapists and speech and language therapists. Similarly, assuming that people cannot understand online risks or lack an awareness of risks should not be the default position. Introducing online engagement as part of general discussions in shared conversations about daily activities could be considered instead as a starting point.

Those supporting people online need to be mindful of the right that people with ID have to take risks. By enabling individual self-determination which may involve making risky decisions, the supporter’s role becomes one of supporting how these decisions can best be made.

Family and paid carers should consider how information about the repercussions of potentially risky online behaviour is given. The use of scare tactics around risk may frighten people into digital self-exclusion. Opting out may be a more parsimonious and easier option both for those providing support and the person with ID themselves and only through sensitive and timely support is online inclusion likely to be maintained once negative aspects of the online world have been experienced. There are numerous risks, and approaches to support may vary considerably across these. Further research into practice is urgently indicated to understand positive support approaches for different online risks.

Finally, ICT and the online world is vast and varied and the skills and supports needed to access it will differ based on the hardware, software and requirements in terms of input and comprehension needed to engage with it. These include a range of different types of engagement (e.g. subscribing, social media, online shopping, advocacy). Internet providers and software designers also need to work towards making support and guidance more usable for people with ID to manage potential online risks in the future.

Publication Information:
Published in: Tizard Learning Disability Review
Accepted for Publication: 04-Sep-2019
Article DOI: TLDR-03-2019-0008
Article ID: TLDR634665
References


Chadwick, D.D. (under review), “You want to know that you’re safe’: Experiences of Risk, Restriction and Resilience Online among People with an Intellectual Disability”.


**Publication Information:**
Published in: Tizard Learning Disability Review
Accepted for Publication: 04-Sep-2019
Article DOI: TLD-R-03-2019-0008
Article ID: TLDR634665