Digital inclusion and online safety for adults in the UK:

A review of evidence, policy and practice

By Dr. Emma Stone,
Jennifer Llewellyn
and Joseph Chambers

December 2020

Good Things Foundation

With support from:

BT

contents >

Contents

Summary

Good Things Foundation has a vision of a world where everyone has the skills to benefit from digital, especially those who experience wider social and economic barriers.

Online safety is integral to our vision of what being 'digitally included' means. It is especially important for people who are new or limited users of the internet (often older people, and working-age adults with low educational attainment and low incomes) and those who are more vulnerable.

Covid-19 has revealed the value of digital technology in our lives - enabling many of us to learn, earn, stay safe, informed and connected. It has also raised major concerns about digital exclusion, as too many have been locked out of these benefits. The pandemic has spurred innovation and acceleration in digital services and use of data, not least in supporting the public health and healthcare response. There have also been reports of a rise in online abuse, online scams, online consumer harms relating to mental health, and the spread of misinformation and disinformation during the pandemic.

At the time of writing, the UK government is finalising its response to the consultation following the Online Harms White Paper alongside developing a new Media Literacy Strategy, UK Digital Strategy, and much-needed work on digital identity. A Data Strategy is out for consultation. UK Research and Innovation funding has recently been announced for online safety technologies. The Scottish Government is consulting on its new Digital Strategy, with greater emphasis on making Scotland an ethical digital nation and eliminating digital exclusion. The Welsh Government has started to engage on a new Digital Strategy for Wales, with clear links to the seven national well-being goals enshrined in the Wellbeing for Future Generations Act. Across combined authorities and some local authorities, public sector leaders are working with industry and civil society partners to develop or refresh digital and data strategies. All this points to the importance of improving approaches to online safety and security - for citizens and communities, as well as for our economy and society as a whole.

This paper presents a synthesis of available academic and grey literature, supplemented with insights from community organisations and those they support, and a review of the current policy and practice landscape. We set out to address a gap in understanding by focusing on adults who are more likely to be digitally excluded (most of the online harms literature focuses on children). We focused on 'everyday' internet risks (such as scams) rather than the worst excesses of internet behaviour (such as terrorism). We wanted to understand what the evidence tells us about the factors that shape people's ability to protect themselves and others online, and about public attitudes to online safety. We were particularly interested in the links between online safety and digital access, skills and confidence. Through this review, we have grown more aware of the important overlaps between digital literacy, media literacy, and data literacy (that is, people's understanding of the value of their personal data, how it is used and how to control this, rather than people's ability to interpret data).

This review was generously supported by BT as part of BT Skills for Tomorrow. Together with BT, we will be publishing a set of recommendations to encourage further discussion about how to address the findings and rise to the challenges ahead.

Findings

1 We can all be vulnerable in certain situations, but different groups face greater online risks

Too few studies have looked at the relationship between socio-economic and demographic factors and internet safety. Where this has been explored, evidence points to 'online' vulnerabilities reflecting vulnerabilities 'offline'. Disabled people, women and Black and minority ethnic groups face greater risk of online abuse. Adults who face social and economic barriers are less able or likely to take action to be safe online. For example: not being able to afford secure home WiFi forcing reliance on insecure free public WiFi even for online financial transactions; not being able to find and use free and trustworthy online safety resources; and only being able to afford a small-screen device. People on low incomes and with low education levels are more likely to be smartphone-only users, which can affect 'critical understanding' online. These factors can compound other challenges already faced - for example by parents, informal carers, people with cognitive impairments or mental health conditions.

46% of women

and non-binary people reported experiencing online abuse since Covid-19; this was even higher among those from Black and minority ethnic groups

(Glitch 2020)

2 Experience builds digital resilience, if people have support to reflect and recover

Personal and secondhand experiences (via media, friends or family) of online harms can create fear and make people step back from using technology. Digital resilience builds through personal experience - negative as well as positive - as long as people have support to reflect and recover from negative experiences. One of the best protections may be to use the internet fully as well as carefully. By contrast, being a 'limited user' - only using the internet for very few things (e.g. only using social media) can affect digital resilience and exposure to online risks. Being a limited user correlates strongly with low education and low income across all ages. For older people, disabled people and others who have gone online for the first time since the pandemic started - having access to support to reflect and recover will be critical in shaping their longer-term relationship with digital technology.

Around 6 in 10 adults

report having had a least one potentially harmful experience online in the past year

(Centre for Data Ethics & (Ofcom/ICO 2020)

3 There's a gap between people's self-reported knowledge and actual online behaviours

People's attitudes to risk are complex, contradictory, and contextual. There is overwhelming evidence of a gap between how confident people say they feel about online safety compared with what they actually do to protect themselves and others online. In the area of personal data, this has been called a 'privacy paradox'. What lies behind the paradox is less clear: apathy; a sense of powerlessness or resignation (that companies will do what they want regardless); trade-offs (for convenience); or a lack of understanding about data and the digital world. There is evidence of the everyday value of simple signifiers (like 'the padlock' in an HTTPS bar). Less positively, many studies report that even those who are digitally confident feel they do not know where to get help when they face problems online.

77% of respondents

felt they 'know enough to stay safe online' but 45% did not always use secure WiFi for online transactions

(Nominet 2019)

4 Public levels of trust in how organisations use personal data is of growing importance

The last two years have seen an increase in research on personal data. A recurring theme is lack of public trust and confidence in how organisations use and safeguard personal data. This is of growing importance in the context of a data-powered economic recovery and digitalisation of goods and public or consumer services - which rely on willingness to share personal data. People appear most likely to trust healthcare institutions, then banks, then local government, then central government. People are less likely to trust retailers and least likely to trust marketing and social media companies. Good previous experience, or legislation, are reasons why people trust institutions with their personal data. Evidence highlights a gap in public understanding about personal data security, sharing and use.

Only 33% of respondents

believe companies will do what users request through their settings & preferences

(Centre for Data Ethics & Innovation 2020)

5

In a complex policy and regulatory context, digital exclusion risks being overlooked

There is a window of opportunity with several significant pieces of work underway relevant to online safety, but also a risk that digital exclusion and 'everyday' online safety issues (such as consumer harms) fall between policies and regulatory frameworks. Research shows that most people see online safety as a shared responsibility - across government, regulators, industry and individuals. People also expect more robust regulation, accountability and transparency - with social media platforms in particular doing more to reduce online harms. Some regulators are developing their approaches to consumer vulnerability - recognising the role of digital access and skills in shaping vulnerability.

75% of the public

are at least 'fairly concerned' about how organisations use and protect their personal data

(Carnegie UK Trust 2018)

6

As digital technologies have evolved, so the set of skills people need has grown

Evidence points to the growing overlap between media literacy, digital literacy, and personal data literacy (that is, people's understanding of the value of their personal data, how it is used and how to control this, rather than people's ability to interpret data). The UK government's work on a media literacy strategy is a timely opportunity for joining up. In recent years, a number of important frameworks have been developed (or are currently being developed) by academics and civil society institutions which highlight the need to evolve concepts of digital inclusion to encompass digital resilience, understanding of the digital world and personal data, and digital citizenship. What is now needed is an enhanced understanding of practical, effective ways to empower people to protect themselves and their communities to stay safe in a digital world.

43% of respondents

felt Adtech was unacceptable after being given information about how it works compared to 14% before having this information

(ICO 2019)

7

Despite some excellent resources, most people don't know where to find help

Recent years have seen a rise in campaigns, resources and initiatives to tackle online harms through public awareness and education - but there is little evaluation evidence about what works; and across most studies it is clear that many people still don't know where to find help when they need it. Most available resources are online, and assume people have the digital access, skills and confidence to find, use and apply them. Community partners we spoke to wanted clearer messages and simpler rules of thumb, taking a more holistic approach to the internet and striking a balance between conveying the risks and benefits of the internet. They also wanted opportunities to share and learn best practice, including on 'newer' online harms impacting their communities, such as misinformation.

Only 34% of respondents
know where to go for help when they experience a problem online
(Doteveryone 2020)

Introduction: Why online safety matters

Good Things Foundation's vision is a world where everyone has the skills to benefit from the internet - safely and confidently - especially those who face greater barriers to going online or using the internet fully.

Being able to be and stay safe online is integral to what being 'digitally included' means. And it is especially important for people who are new or limited users of the internet (often older people, and working-age adults with low educational attainment and low incomes) and those who are more vulnerable.[1]

Even before the pandemic, worries about online safety and security posed a barrier to going online, especially among older people and those on lower incomes.[2] Lack of trust or worries about internet safety were cited by 17% of 55+ year olds who were offline; and 14% of all adults in social grades C2DE (but not by any adults in social grades ABC1).[3] Similarly, Lloyds Bank's latest analysis found lack of motivation is the main barrier, but cost, complexity, concerns about data privacy and security, and about how organisations use personal data, remain significant.[4] There is a clear link between low digital skills and worries about using the internet for online or mobile banking.[5]

Among internet users, when asked about the internet generally, adults are most concerned about personal information being stolen (43%), scams/frauds (42%) and their data being processed without prior consent (37%); nearly half (47%) were concerned about how their data is used by organisations.[6] So, while two-thirds of adults feel the benefits outweigh the risks, there is little doubt that online safety matters for non-users and internet-users alike.[7]

Covid-19 has transformed the digital landscape in the UK. For children and adults of all ages, Covid-19 has further highlighted the significance of digital technology in our lives. Digital inclusion has enabled most of us to learn, earn, stay safe, informed and connected; but too many have been left behind. Covid-19 has raised particular concerns about digitally excluded older people and adults facing wider social and economic disadvantage.[8]

Sadly, Covid-19 has also triggered an increase in online harms like fraud and scams; the spread of misinformation and disinformation; and online abuse and harassment.[9] Charities working with older and vulnerable adults have flagged an increase in cybercrimes masquerading as NHS, government or charity support. Analysis of cybercrimes data confirms an increase in crimes targeting individuals, especially online shopping and auctions, and social media or email hacking.[10] Fraud and scams carry a heavy economic cost: £1.2 billion was stolen through fraud and scams in 2019.[11] For victims, the impacts can be devastating: older people defrauded in their own homes are 2.5 times more likely to either die or go into residential

1 Yates et al (2020a); Good Things Foundation (2018)
2 Lloyds Bank (2020, 2019); Ofcom (2020a, 2019)
3 Ofcom (2020a)
4 Lloyds Bank (2020, 2019)
5 Lloyds Bank (2020): 51% of all adults (59% with low digital engagement) feel online or mobile banking is not safe; Broadband Stakeholder Group (2020)
6 Ofcom/ICO (2020)
7 Ofcom/ICO (2020)
8 Good Things Foundation (2020a, 2020b); Older People's Commissioner for Wales (2020)
9 Money & Mental Health Policy Institute (2020); Carnegie UK Trust (2020); Ofcom (2020d); World Wide Web Foundation (2020); Glitch (2020)
10 Buil-Gil et al (2020)
11 UK Finance (2020)

care within a year.[12] COVID-19 has also exacerbated the risk of online abuse for women and non-binary individuals. Women from Black and minority ethnic backgrounds were even more likely to have experienced an increase in online abuse, and feel their complaints had not been addressed.[13] Online abuse (including harassment and 'hate speech') can have serious impacts on mental and physical health, and a 'silencing' effect - inhibiting internet use and self-expression, alongside damaging effects on communities and society as a whole.[14]

Covid-19 has also spurred an acceleration of digital services and data innovation. The Centre for Data Ethics and Innovation identifies numerous ways in which the outlook for use of data and AI has been transformed by Covid-19, from supporting the public health response, to using publicly-held data to identify vulnerable people, to the use of video calls in care homes to connect relatives. However, rapid transformation also creates risks, digital exclusion and digital literacy among them.[15] An overarching risk is loss of public trust and confidence around personal data, especially by the public sector.[16]

This paper aims to stimulate discussion and generate solutions about how we can protect, empower and support older people, vulnerable and disadvantaged adults to be safe online. Our focus reflects our work as a digital inclusion charity; and the much larger body of evidence, policy and practice thinking already available about children, young people and online harms.[17] We look at these areas: online fraud and scams; misinformation or disinformation; online abuse; and concerns about personal data privacy and security - including use and sharing of personal information. While these are not all in the scope of the Online Harms White Paper, they are all areas that reflect major or growing concern among UK adults and for community partners in our network.

In the sections that follow, we explore the factors that shape people's ability to use the internet safely, and review the policy and practice context for online safety with regard to digital inclusion of older people, vulnerable and disadvantaged adults.

[12] Age UK (2017) citing National Trading Standards
[13] Glitch (2020)
[14] Vidgen et al (2019), Glitch (2020)
[15] CDEI (2020a). Digital exclusion is identified as a risk for financial services, and essential utilities; lack of digital health literacy is identified as a high risk in the area of health and care.
[16] Doteveryone (2020), CDEI (2020b), Kennedy et al (2020)
[17] For example, 5Rights Foundation (2019), Livingstone et al (2017, 2018)

Chapter 1:
What factors shape our attitudes and behaviours to online safety, and affect our vulnerability to online harms?

Our focus is older people and vulnerable adults - including those whose vulnerability may reflect digital exclusion and wider social or economic disadvantage.

We want to understand more about what helps and what hinders online safety; and test our assumptions about the links between digital inclusion (or exclusion) and online safety (or harms). To what extent are people with low or limited digital access and skills at greater risk of online harms? A better understanding of factors which affect vulnerability to harms, and shape our attitudes and behaviours, can help us to improve support, and enable more people to be and stay safe online. Below, we summarise relevant findings from academic and grey literature, and also draw on insights from engagement with community partners in the Good Things Foundation network of online centres, and from other civil society organisations.

This chapter begins with an overview of people's concerns about online safety. It then explores some of the different factors that contribute to people's ability to stay safe online: social and demographic factors (such as older age, vulnerability); types of device and internet use; the role of skills, knowledge and experience; and finally what the evidence says about our attitudes, actions and behaviours towards online safety.

People's concerns about online safety

According to research for Ofcom and the Information Commissioner's Office, eight in ten adult internet users have at least one unprompted concern about online harms, primarily in relation to children; but when asked about the internet more generally, the main concerns are identity theft (43%), scams or frauds (42%) and their data being processed without prior consent (37%). Around six in ten adults report having had at least one potentially harmful experience online in the past 12 months. Nearly half of adults (47%) were concerned about how their data is used by organisations.[18] Similarly, Doteveryone's latest survey into digital attitudes found high levels of concern about online harms, especially scams (83%) and bullying (74%); as well as rising concern about newer developments such as AI-decision making (58%) and online targeted advertising (39%).[19] Concerns are well-founded; the ONS reports that 7% of all adults suffered fraudulent credit or debit card use during the last 12 months from using the internet; and both lack of skills and privacy or security concerns were cited as barriers to internet use, at 34% and 33% respectively.[20]

[18] Ofcom/ICO (2020)
[19] Doteveryone (2020), ICO (2019), CDEI (2020c)
[20] ONS 2019

Insights from community partners are in line with this wider evidence. Consultation with four community partners confirmed that online safety is primarily seen as being about fraud, scams and phishing emails.[21] Misinformation, disinformation and fake news are less of a concern, although community partners and people can see these being shared on social media. With regard to using the internet for things like online banking, community partners reported that people tend to be either fully onboard and confident or very fearful. Last year, Good Things Foundation worked with One Digital to identify problems and solutions to helping people be safe online. Common problems were:

- Remembering multiple & complex passwords
- Ignoring safety as unsure what to do
- Not knowing how to protect personal data or privacy
- Wanting to stay connected instead of logging out (for convenience, memory or lack of awareness about the risks)
- Costs of online safety and security – in terms of money and also time and effort
- Delegating responsibility to others (such as assuming their service provider protects them)
- Downplaying internet risks and not believing they might be a victim
- Overconfidence in their ability to respond
- Feeling overwhelmed by different messages about online safety

How socio-demographic factors shape people's ability to be safe online

Older age

Around 13% of UK adults do not currently use the internet (some will never have gone online; some may have used it in the past). This equates to around 7 million people. The most cited reason is that people feel 'the internet is not for me'; this can be compounded by fear or mistrust of technologies and feeling the internet is not safe. This matters for digital inclusion.

Older age remains the strongest predictor of being a non-user of the internet, even more where it overlaps with having a health condition or disability, being retired, or having a more limited education.[22] Among non-internet users - who are predominantly older people - lack of skills and fears about online privacy and security are cited as reasons for staying offline (34% and 33% respectively).[23] For those offline, the potential risks of going online often come from secondhand experience (stories from friends or family or in the news), while negative firsthand experience can be a reason for stepping back from use.

In 2019, a review of evidence by the Home Office found that fraud victims were more likely to live in higher income households and aged 25-54 years; however, the review also found that the impacts of fraud - including emotional, health and psychological - can be far more damaging for older people; and even a small financial loss may result in a high impact.[24] This aligns with evidence from National Trading Standards that older people defrauded in their own homes are 2.5 times more likely to either die or go into residential care within the year.[25] Single older people, those aged over 75 years, and living alone are also more likely to be targeted by fraudsters and scammers.[26] As more older people go online, so too the incidence of online fraud and scams targeting older people is growing.

[21] Community partner consultation, September 2020
[22] Lloyds Bank (2020), Yates et al (2020a)
[23] ONS (2019), see also Ofcom (2020a), Lloyds (2020)
[24] Home Office (2019)
[25] National Trading Standards, cited in Age UK (2017)
[26] Age UK (2017)

Perceptions of internet risks can compound feelings that 'the internet is not for me'.[27] Qualitative research with older people learning to use the internet found that worries about online safety did not stop them from carrying out activities which they felt to be safe, but it was consistently cited as a reason to avoid certain activities, especially online banking.[28]

> *"I haven't [done any financial transactions online], because at the moment I don't feel that secure, you know, with all the fraud and, you know, the negative things you hear all the time."*[29]

> *"I'm a bit scared of what you could do because there's so much fraud, fraudsters and wrong people but if they're used in the right way they're alright aren't they?"*[30]

Worries about online safety overlap with other factors, including fears about making a mistake, and a wider mistrust of technology and the online environment.[31] Evidence on people's attitudes to how their personal data is used found lower levels of knowledge and support for public health data practices among older people.[32] Confidence in abilities to avoid personal data risks also appears lower among older age groups.[33] By contrast, exposure to online abuse is significantly less likely among older than younger age groups, likely reflecting use of social media platforms and online social networks.[34]

Intersectionality

Available data points to the importance of intersectionality, particularly in the area of online abuse (including harassment and 'hate speech') and the need for more research.

Research by Glitch into online abuse and Covid-19 found that 46% of women and non-binary people reported experiencing online abuse since the beginning of Covid-19, and 29% of those who had previously experienced online abuse reported it being worse during Covid-19.[35] Experiences of online abuse were higher among women from Black and minority ethnic communities. The vast majority of online abuse (84%) was from strangers; most took place on mainstream social media platforms.[36]

An evidence review for the Alan Turing Institute found that disabled people, Black people and those of 'other' ethnicities, and younger people are more likely to be targeted and exposed to online abuse. In this survey, gender did not make a big difference.[37] Worryingly - and again pointing to an urgent need for more research into online abuse, safety and intersectionality - the researchers found a significant contrast between people's self-reported exposure to online abuse and government data on the level of illegal online abuse.[38] Analysis of survey data including the Oxford Internet Survey found that between 30-40% of people in the UK have seen online abuse, while 10-20% of people have personally been targeted.[39]

[27] Blank & Dutton (2013) in Good Things and Centre for Ageing Better (2018)
[28] Good Things & Centre for Ageing Better (2018)
[29] New learner, female, 65-74, social grade C1; in Good Things and Centre for Ageing Better (2018)
[30] New learner, male, 55-64, social grade C2; in Good Things and Centre for Ageing Better (2018)
[31] Good Things and BT (2019), Good Things and Centre for Ageing Better (2018); Office of the e-Safety Commissioner (2020)
[32] Kennedy et al (2020) citing Understanding Patient Data.
[33] Ofcom (2020a)
[34] Vidgen et al (2019)
[35] Glitch (2020)
[36] Glitch (2020)
[37] Vidgen et al (2019)
[38] Vidgen et al (2019)
[39] Vidgen et al (2019)

Disability

Disabled people are among those less likely to be digitally included, and more likely to report benefits when they are digitally included, including through use of assistive technologies.[40] Accessibility of websites remains a major barrier to full internet use.[41] This may make it harder for disabled people to protect themselves online; a significant issue in the face of disability-related hate crime.[42]

Lloyds Bank data indicates that disabled people are on average 23% less likely to have the essential digital skills for life than those without an impairment (61% vs. 84%); even more so where people have limited mobility (46%). Data also suggests that disabled people were 40% less likely to have received digital skills support at work.[43]

A recent study by Demos explored fraud protections for adults with a health condition that affects their cognitive abilities in a way that may make financial decision-making harder, estimated at around 4.8m adults in the UK.[44] This puts them at risk of exploitation, including by those close to them. Such conditions are more common among older people; and 17% have less than £5,000 annual income - so even a small financial loss can be significant. They are more likely to be targeted or victimised by fraudsters; almost twice as likely to have their account or debit card used without their permission.[45] Research for the Money and Mental Health Policy Institute suggests sharing of personal details with partners, family members, friends and carers is widespread; an estimated 7.7 million people (15%) know someone's online banking password.[46] For people with limited or fluctuating cognitive abilities (such as learning difficulties or dementia or severe mental health problems), approaches to online safety need to include but go beyond providing education or information.[47]

The effects on disabled people of online fraud or scams, and disablist online hate speech, can be especially harmful - resulting in people limiting their use of the internet or staying away from it entirely, and even being too afraid to leave their own homes.[48] Some disabled people have been advised by others to stay away from the internet, even though this impacts negatively on their wider life chances and freedoms. The same advice has been reported by women and others from marginalised groups, drawing criticism that staying offline shouldn't be seen as an acceptable or sustainable response.[49]

Being a parent

Whether an adult is a parent or has a child in the household shapes attitudes and behaviours around online safety. Parents' concerns around online safety focus more on their children than themselves. Parents generally see themselves, and are seen by others, as being responsible for looking after their children's safety online.[50] Parents widely report using platform or device parental controls, locks and filters.[51] While research suggests that 75% of parents felt online safety education for their children is very important, only 55% felt they had what they needed to teach their children about online safety.[52]

[40] Lloyds Bank (2020,2019)
[41] Lloyds Bank (2020) citing Scope UK; also see Ability.Net
[42] Epilepsy Society (2019)
[43] Lloyds Bank (2020)
[45] Demos (2019)
[45] Demos (2019)
[46] Demos (2019) citing Money and Mental Health Policy Institute (2016)
[47] Demos (2019), Good Things (2018)
[48] Davidson et al (2019) citing House of Commons (2019)
[49] Davidson et al (2019), Glitch (2020)
[50] Ofcom/ICO (2019, 2020)
[51] Ofcom/ICO (2019, 2020)
[52] Digital Schoolhouse (2020)

Linking back to intersectionality, research identifies differences in concerns and experiences of online abuse reflecting education levels, socio-economic status, household composition, gender, ethnicity and whether their child has a disability or special educational needs. Parents with higher socio-economic status cited privacy as their main concern; lack of time was the top barrier for parents with lower socio-economic status.[53] Barriers to internet use were reported more by parents from Black, Asian and minority ethnic backgrounds or parents of a child with special educational needs.[54] Online harms were reported more by single parents and parents of a child with special educational needs - for both themselves and their child. Parents who frequently used the internet had double the digital skills (4 out of 10 of skills tested) of infrequent users (2/10), but only just over half of parents were able to perform privacy related skills.[55]

Being a carer

According to Carers UK, there could be 8.8 million adult carers, of whom over 2 million may be aged over 65 years. Almost 2 in 5 carers report 'struggling to make ends meet', and over two thirds regularly use their own income or savings to pay for care or support services, equipment or products for the person they care for. Eight in ten carers report using some form of technology but of those using technology (mainly the internet), only a quarter used it for online or remote health care, and fewer than one in ten were benefiting from the 'internet of things'.[56]

Being a carer, especially an older carer, makes it more likely that someone is a 'limited' internet user - using the internet only for a very few things - reflecting lack of disposable income but also lack of time to learn how to benefit fully.[57] A recent pilot project supporting family carers of people living with dementia in their own home to build their digital skills and confidence found the benefits of introducing new technologies into the home - such as smart speakers - could be life changing.[58]

> *"Having NHS information and advice so easily, I can ask [Alexa for] advice around health symptoms and I know it's NHS approved information."* (Carer, Alexa user)

> *"Finding something like this iPad to give me enjoyment in the everyday, giving myself some 'me time' and to use it to have more lovely moments with [my wife], it's given us both a bit of our old life back"* (Carer, iPad User)

While the benefits were significant, some raised important concerns about financial safety:

> *"She asked it to play Jerusalem and it said you need an Amazon subscription so I worry if they sign up to it and run up a massive bill as it is connected to [her carer's] account."*[59]

This raises wider questions about smart devices in the home, and what people - especially those who may be more vulnerable to consumer harms - need to know to be safe and secure online.

[53] Davidson et al (2019) , Livingstone et al (2018)
[54] Davidson et al (2019) , Livingstone et al (2018)
[55] Davidson et al (2019) , Livingstone et al (2018)
[56] Carers UK (2019)
[57] Good Things (2020b)
[58] Good Things (2020d)
[59] Good Things (2020d)

Socio-economic disadvantage

There is a clear correspondence between digital exclusion and other forms of social and economic exclusion - particularly low educational attainment and low socio-economic status.[60] How far does this impact on people's ability and means to use the internet safely? A recent research review is critical of the lack of attention paid to this question with regard to public understanding of data practices.[61]

A significant body of European comparative research with children and young people found that socioeconomic status (as well as age and gender) impacts on their chance of benefiting from digital; their likelihood of experiencing online harms; their resilience, resources to cope, and level of parental support.[62] The relationship between social and economic disadvantage, experience of online harms, and having the resilience and resources to protect oneself online is not fully explored among adults.[63]

In 2019, Ofcom reported on differences by socio-economic group in levels of critical engagement with online information and spaces and found that search engine users in lower income (DE) households were less likely to demonstrate a critical understanding of search engine results compared to those in affluent (AB) households (46% to 65% respectively); this pattern was similar for awareness of funding and online advertising.[64]

The small proportion who say they are not at all confident in managing their personal data are more likely to be older people above 75 years (13%) and adults in DE households (9%).[65] A review of public attitudes to health data found people in lower socio-economic groups are less likely to see the benefits of sharing their data, and more likely to feel powerless to address data-related harms; and that ethnic minority groups are slightly less likely than ethnic majority groups to trust that their data will remain secure.[66]

Doteveryone's research found a correlation between income levels, frequency of internet use, attitudes towards the internet, and data literacy: internet users on higher incomes were more likely to say the internet has made life better for them (85%) than those who are less well off (75%).[67] People on higher incomes were also more likely to have taken measures such as checking their privacy settings, looking outside their filter bubble or using an advertisement blocker; and to have a higher level of understanding about personal data sharing.[68]

Socio-economic status impacts on the levels of activities undertaken and the digital and data capabilities of those online: internet users aged 65+ (53%) and in DE households (46%) are less likely to bank online (compared to 73% of internet users overall) or to complete most public or civic processes online.[69] Research into parents found a clear link between higher digital skills and educational attainment.[70] It follows that people's exposure to some online harms may be lower; but this is offset by being less able or less likely to take action to be safe online.

[60] Good Things & BT (2019); Yates et al (2020a); Davidson et al (2019)
[61] Kennedy et al (2020)
[62] Smahel et al (2020)
[63] Carnegie UK Trust (2018)
[64] Ofcom (2019)
[65] Ofcom (2020a)
[66] Kennedy et al (2020) citing research by Understanding Patient Data
[67] Doteveryone (2020)
[68] Doteveryone (2020)
[69] Ofcom (2020a)
[70] Davidson et al (2019), Livingstone et al (2018)

People who face social and economic barriers may be less able or likely to take action to be safe online. Cost - financial as well as time and effort - will play a part in this, especially in the current context of social distancing restrictions where many are unable to access the internet in public places they can trust. Data poverty (not being able to afford home broadband or mobile data connectivity) has implications for online safety. For example: where people have to do online transactions using public or free WiFi, which may not be secure; where people cannot afford technical support or antivirus software, or do not know how to access free software they can trust; and where people are limited to mobile smart devices (discussed below).[71]

Vulnerability

Vulnerability is an important concept when exploring online safety and security. Vulnerability is dynamic, and often shaped by a range of characteristics and contexts which intersect. This makes defining and identifying consumer vulnerability a challenge. For example, older age is associated with increased vulnerability, but being older does not necessarily make someone more vulnerable. Vulnerability in older age is also shaped by other characteristics, such as living alone, a physical or mental health condition or disability, low income, or barriers relating to literacy, language, and experiences of discrimination. Meanwhile, research on young people's experience of online risks found a high correlation between vulnerability in the offline world and in the online world.[72]

People move in and out of vulnerability depending on what's happening in their lives; this is called 'situational vulnerability'. Life events which bring significant change and stress increase someone's vulnerability. For example, bereavement, redundancy, and onset of poor health. Covid-19 has increased the level of situational vulnerability among the UK population.

The Financial Lives 2020 survey found that just under half (46%) of UK adults (24.1 million people) display one or more characteristics that fall under the four drivers of financial vulnerability: being over 75, being unemployed, renting, and having no formal qualifications.[73] These characteristics map onto characteristics associated with digital exclusion. Using an enhanced vulnerability algorithm, the survey found that consumers often display more than one characteristic of vulnerability. Vulnerable consumers are more likely to experience harms: financial exclusion, difficulty accessing services, partial exclusion, disengagement with the market, scams, over-indebtedness, exposure to mis-selling, and inability to manage a product or service.[74] Further analysis shows that people who experience adverse life events are more likely to share their personal details (such as online account details) with someone they trust (26% compared to 19%).[75]

[71] Yates et al (2020a)
[72] El Asam & Katz (2018)
[73] FCA (2020)
[74] FCA (2020)
[75] Demos (2019)

In evidence to the Home Affairs Select Committee on online harms and the coronavirus period, the Money and Mental Health Policy Institute explained that even before the pandemic, people with mental health problems were more vulnerable to online financial harms (such as difficulties managing online borrowing and spending, scams, and problem gambling). Common symptoms of mental health problems can make managing money harder; and shape how people engage with the internet. The online environment amplifies certain risks; 24/7 access and ability to save payment details makes it easy to shop or get credit however well someone feels.[76] In research with over 350 people (April/May 2020), 71% reported being worried about online scams during lockdown (17% had past experience of being scammed). Some felt vulnerable due to low digital confidence. Only 52% felt confident dealing with essential services like banks and energy companies online, but felt required to do so.

"Good for social contact but the adverts led me to spend money I can't afford, both on buying things and on donations."

"Online can make things easier as long as you are well and in control. I.e. if not well you could easily over spend, gamble or increase credit."

"(I) am forced to do some things online even though I do not feel happy about doing any banking online. It makes me feel incompetent and stupid and terrified of being scammed."

How types of internet use shape people's ability to stay safe online

Types of device

Changes in how we access the internet carry implications for online safety; for digital, media and data literacy; and how we interact with the online environment. More of us are using smaller, mobile and smart devices for going online. The choices we make are shaped strongly by age, and by income.[77]

According to Ofcom's latest data: 34% of adults only use devices other than a computer to go online, and 11% of adults only use a smartphone to go online. Overall, 81% of adults have a smartphone; 22% had a smart speaker at home and 11% of households own some kind of smart home technology.

Take-up varies and is shaped by age and income. In January to February 2020, 49% of adults in Great Britain aged 25 to 34 years used a virtual assistant smart speaker or app, compared with 17% of those aged 65 years and over; 35% of all adults used 'internet of things' devices.[78] Those in AB households are more likely than those in DE households to have smart devices and a wider range of devices at home.[79] Adoption and acceptability of smart home devices is higher among younger people and more educated people; older people were the least trusting about smart home device reliability.[80]

Dependence on small screens can create problems for using the internet more fully, and for critical engagement (a key element of media literacy). For instance, those who are smartphone-only are less likely than other internet users to recognise sponsored links at the top of search engine results (44% vs. 61%). Ofcom suggests that this, combined with the smaller screen size reducing the number of results shown without scrolling, could lead to people being more susceptible to paid-for results.[81]

[76] Money & Mental Health Policy Institute (2020)
[77] Yates et al (2020), also citing US evidence (Fernandez et al, 2019)
[78] ONS (2020; January and February 2020)
[79] Ofcom (2020a)
[80] Cannizzaro et al (2020)
[81] Ofcom (2020a)

Evidence from other studies raises questions about online safety practices by smartphone users. The latest data from ONS found that - among adults who have a smartphone for private use, 17% did not have security on their smartphone and a further 32% did not know whether they had security.[82]

Community partners find that being able to use mobile smartphones and social media has given some people they support a false sense of security and online safety.[83] Whereas people may feel more nervous about using laptops or computers, community partners regularly have to remind about the risks associated with smartphones.

Taken together these findings have implications for smart technology take-up and the coverage and reliability of smart data, as well as for online safety. How much do we need to understand about how the internet - and smart technologies - work; how our personal data is accessed and used; what is classed as personal data; what it means to be 'online' as well as to be safe online?

Type of internet use

Analysis of Ofcom data has identified seven different types of internet user, and explored the characteristics associated with each type. Of particular interest to issues of online safety are 'limited' users (who do very few tasks online) and 'social and entertainment media only' users.

'Limited' users are more likely to be older retired citizens from lower socio-economic groups, who lack a post-16 education and may have a chronic health condition. Limited use can include social media. 'Social and entertainment media only' users are most likely to be younger adults, from deprived areas, who may have already left education or intend to leave before eighteen.[84] This matters because social media sites are the most commonly cited sources of harm. Nearly 7 in 10 of the people who reported an online harm experienced it on social media.[85] Social media users are less likely to check the information in articles they see on social media to establish its truth; 29% wouldn't tend to check.[86]

Around 72% of all UK adults have a social media profile. Facebook is the most widely used social media site, especially among older users.[87] Around one quarter of adults say they often actively engage in social media; a similar proportion say they passively engage.[88] Last year, research found that more than half of British social media users (57.7%) came across news in the past month on social media that they thought was not fully accurate.[89] More recently, analysis by ethnicity of Ofcom data on news consumption in March/April 2020 found that social media is more popular as a news source among minority ethnic groups (54%) than adults from a white ethnic group (40%); in particular, WhatsApp (27% vs 7%).[90]

[82] ONS (2020; January and February 2020)
[83] Consultation with community partners, September 2020
[84] Yates et al (2020a)
[85] Ofcom (2020a)
[86] Ofcom (2020a)
[87] Ofcom (2020a)
[88] Ofcom (2020a)
[89] Chadwick & Vaccari (2019)
[90] Ofcom (2020e)

Consultation with community partners confirmed that social media plays a negative role in enabling (even encouraging) people to share misleading or harmful information; some community partners try to tackle this by responding to comments online.[91] Some have raised concerns about the potential harmful impacts on community relationships when divisive content is shared through social media.

Combating hate speech online is a particularly important and challenging area. In an evidence review on adult online hate, harassment and abuse for the UK Council for Internet Safety, researchers explore the spectrum of online abuse, and how new technological advances (alongside online anonymity and invisibility) have enabled greater sophistication and more instantaneous and potent spread of online hate.[92]

Social media platform business models rely on an 'online attention economy'. The use of sensational and click-bait content opens up questions about what level of knowledge, understanding and skills are needed to use social media.[93]

How skills, knowledge and experience shape ability to stay safe online

Digital, personal data, and media literacy

As digitalisation evolves, and our attitudes and engagement with the internet changes, so too our approach to digital skills needs to evolve. Digital and social media and smart technologies create new challenges. As researchers at University of Liverpool have noted, the types of literacy which citizens need today are much more complex than even a couple of years ago:

> *"Hence, the types of digital and data literacy that citizens need today are complex. They involve not only being able to read and verify news and content, but also, understand the technical and media economics of digital platforms, how they are funded, what their different features and affordances mean and how they function, how to change their privacy and content settings and importantly their individual and collective rights."*[94]

Low media, digital and personal data literacy leaves people open to risks and harms: financial, social, emotional, personal and psychological.

Knowledge of personal data - how data is used and shared, and how to control this - is increasing but it is higher in those who are better off, highlighting issues around digital literacy, online safety, and wider disadvantage.[95] People in lower socio-economic groups are less likely to see the benefits of sharing their data, and more likely to feel powerless to address data-related harms; while ethnic minority groups are slightly less likely to trust that their data will be secure.[96]

[91] Consultation with community partners, September 2020
[92] Davidson et al (2019)
[93] Carmi et al (2020), Behavioural Insights Team (2018)
[94] Carmi et al (2020)
[95] Doteveryone (2020)
[96] Kennedy et al (2020)

Ofcom data reveals a gap between perceived and actual awareness of online targeting: 85% of internet users are confident that they can recognise online advertising; yet only half of search engine users could accurately identify advertising on Google search results.[97] Those who only use smartphones are less likely than other internet users to recognise sponsored links.[98] Research for the Information Commissioner's Office found that people's attitudes towards online advertising changed significantly after they were given information about how it works - triggering a rise in perceptions of unacceptability from 14% to 43% of participants.[99] People are particularly concerned about the potential exploitation through online targeting of vulnerable consumers (older people, children, those with poor mental health or addictive tendencies).[100]

Building understanding of personal data use and sharing is not easy. With regard to public health data sharing, Understanding Patient Data (an initiative which supports conversations about the use of health and care data) found that providing only a little information raised patients' concerns - whereas what patients needed was 'enough information' to reassure them so they could feel comfortable and confident about how their data would be used, and especially why their data was needed.[101]

More broadly, researchers and civil society organisations identify the need for research on the relationship between initiatives aiming to improve understanding of data practices and changes in perceptions, use and trust; on areas such as what 'critical' means in the context of 'critical thinking' or 'critical understanding' about online media, data use and the digital world; and on what the standards of 'good' privacy protection should be as well as raising awareness about these standards.[102]

There is an opportunity here to evolve existing frameworks to empower citizens to develop their digital skills and confidence in ways which integrate digital, data and media literacy together; and support people to become digital citizens in making the internet a safer place which benefits society.

Personal experience

Research suggests that trust and confidence in the internet grows in line with use, including negative experiences as these are likely balanced by an even greater number of positive experiences and by people building their knowledge of how to deal with problems.[103] By contrast, those who are offline hear secondhand information about online harms or internet risks which are not counteracted by information about the benefits. Both direct and indirect experience of online harms can prompt people to step back from using the internet wholly or partially:

> *"I'm a little bit wary of putting my banking details on the computer. They [the bank] showed me that it's absolutely secure and all the rest of it, but my daughter was conned out of two or three thousand because somehow or other they got her details and somebody had ordered all this carpeting from somewhere."*[104]

Since Covid-19, research for the Broadband Stakeholder Group similarly found that - for existing and new internet users - using the internet on a more regular basis during lockdown eased the minds of many who had been more tentative, as they grew their digital skills and confidence.[105] Increased familiarity led to awareness that internet fraud/scams were not as prevalent as they had thought, and confidence in keeping themselves safe online - for example, checking for the secure padlock in the corner of an HTTPS site.[106]

[97] Ofcom (2020a)
[98] Ofcom (2020a)
[99] ICO (2019) with Harris Interactive
[100] CDEI (2020c)
[101] Understanding Patient Data (2017)
[102] Kennedy et al (2020), Carmi et al (2020), Carnegie UK Trust (2018)
[103] Good Things & Centre for Ageing Better (2018) citing Blank & Dutton (2013)
[104] New learner, female, 65-74, social grade B; in Good Things & Centre for Ageing Better (2018)
[105] Broadband Stakeholder Group (2020)
[106] Broadband Stakeholder Group (2020)

Personal experience of online abuse can have devastating effects, as civil society organisations like Glitch, Scope, and the Epilepsy Society have reported and research has shown.[107] This extends beyond individual effects to repercussions for families, friends, communities, and society. Recent research by Demos for BT on public attitudes to different ways the worst internet behaviour could be tackled, found over half of those surveyed (53%) had experienced online harm - some of whom were less likely to see it as a big problem for society, or to propose the strongest action; others had withdrawn from online spaces given their experiences.[108]

Experience of fraud and scams is high; whereas experience of personal data theft is low. That said, among those who experience online harms, personal data theft recorded the greatest negative impact score (59%), followed by non-consensual use of personal data (48%), content promoting terrorism (44%), and fraud or scams (43%).[109] Spam emails were frequently experienced but carried low impact. According to ONS, 7% of adults suffered fraudulent debit or credit card use from using the internet in the last 12 months in 2019.[110]

Older people and more vulnerable adults may be more at risk of repeat targeting. Scammers and fraudsters buy and sell lists of soft targets (known as 'suckers lists') - people who are less able to protect themselves through mental health related issues, older age, or adverse life events, such as a bereavement.[111] As already noted, the effects of this can be devastating.

Worryingly, many victims may not realise they have been scammed or may feel ashamed to report it. In March, research found 8 in 10 people would feel embarrassed if they fell for a financial scam (more than if their social media account was hacked).[112] A quarter said that hearing stories and information from their friends would have the biggest impact when it comes to protecting themselves.[113] Victims of online hate can face even greater barriers to reporting; and where they do report online hate, their experiences are not always positive.[114] One survey found that Black and minority ethnic women and no-binary people were more likely to report that their complaints were not properly addressed.[115]

Sharing stories about online harm can break through the stigma, promote reporting, and encourage digital citizenship. There is also a need to balance these with personal positive stories of benefiting from the internet to counteract fear. Community partners, experienced in building digital skills and confidence, described the value of sharing their own positive stories, and the benefits of using the internet, to avoid people becoming too scared to go online or use the internet fully.[116]

Both evidence and experience suggest that one of the best protections against online harms might be using the internet more fully - learning through experience, with 'on tap' support and knowing that there are people you can trust and ask when you are unsure.

[107] Davidson et al (2019), Vidgen et al (2019)
[108] Demos (2020) for BT
[109] Ofcom/ICO (2020)
[110] ONS (2019)
[111] Demos (2019)
[112] UK Finance (2020b)
[113] UK Finance (2020b)
[114] Glitch (2020), Vidgen et al (2019)
[115] Glitch (2020)
[116] UK Finance (2020b)

Trust

Trust in technology, especially in how organisations (public and commercial) use data and how secure data is, is an important area of concern - for governments, companies and public sector bodies as much as for individuals (if not more so). Trust shapes attitudes and decisions about going online and how people use the internet, including how they feel about sharing personal data. Trust (fear, mistrust) emerges as a recurring theme through the research and from the experience of community partners.

Research in the area of online data privacy reveals varying levels of concern. This can be highly context dependent. An evidence review by Carnegie UK Trust in 2018 found that on average around 75% of the UK public were at least fairly concerned about the privacy and security of their data online, although this varied widely and was very context dependent. More recently, a survey for Deloitte found that UK consumers are becoming less concerned about data privacy and content to share data online with a growing range of companies, from more devices, despite awareness of misuse of data and breaches. The research speculates that COVID-19 may result in increased readiness by consumers to relinquish control over data. In 2018, almost half of UK adults reported that they were 'very concerned' about the use of personal data; by mid-2020, only 24% were 'very concerned' with 50% being 'fairly concerned' (a rise from 33% in 2018) and 23% being 'not very concerned' (a rise from 15%). Increased devices and connectivity is unlikely to see this trend reverse. What is unclear is how far this reflects familiarity, awareness but apathy, or a lack of understanding, and lack of trust in companies to act where people have exercised greater control.[117]

According to research by Nominet on attitudes towards cybersecurity, 52% of adults don't trust the government, intelligence agencies and law enforcement to keep them safe online. Anecdotal evidence from community partners has highlighted lower levels of trust among some groups and communities, including for institutions like the NHS or high street banks where levels of trust are generally high.[118] This resonates with emerging insights from NHSX community engagement in London and Birmingham and elsewhere, and from community partners involved in a digital financial inclusion pilot currently underway.[119]

In a recent study by the Center for Data Ethics and Innovation, only 36% of people believed they have meaningful control over online targeting systems; only 33% believed that companies will do what users request through their settings and preferences.[120] People did not trust online platforms to act in the interests of individual users or society more widely.

The latest insights from Ofcom's in-depth longitudinal research (Adults' Media Lives) indicate rising concern about technology 'spying' on them. Even so, most said they accepted cookies, terms and conditions and privacy policies without question.[121] People are most likely to trust healthcare institutions, followed by banks, local government, then central government; people are much less likely to trust retailers; marketing and social media companies are least trusted.[122] Distrust in commercial companies is mostly about their data being sold; distrust in government is mostly about data security and past missteps.[123]

Public levels of trust matter more than ever - in the context of economic recovery and use of AI for societal as well as economic benefit. Evidence suggests that good previous experience or legislation are the most common reasons why people trust institutions with their data.[124]

[117] Carnegie UK Trust (2018), Deloitte (2020)
[118] Nominet (2019)
[119] Presentation on NHSX pilots at Digital Leaders Week 2020; Good Things (2020e); digital financial inclusion pilot supported by Mastercard - Nobody in the Dark.
[120] CDEI (2020c)
[121] Ofcom (2020c)
[122] Kennedy et al (2020)
[123] Kennedy et al (2020)
[124] Kennedy et al (2020)

How we feel and what we do to stay safe online

A 'reality gap'

Our attitudes towards online risks - and risks generally - are complex, contradictory and contextual. How we perceive risk, even if we think it might happen to us, doesn't correspond with the likelihood or likely level of impact. Knowing more about online harms does not necessarily change what we do online. Across several studies, a clear gap emerges between how confident people feel about being safe online, and what they actually do to protect themselves - or others.[125] Recent research with both parents and children found marked differences between what parents felt they do to protect their children and what children say their parents do.[126]

In a survey for Nominet, whereas 77% of adults felt they knew enough to stay safe online, only 55% knew how to change their privacy settings on social media; 45% said they do not always use secure WiFi for online transactions; 20% had never changed their online banking password; and 71% did not understand two-factor authentication.[127] Of those who had experienced hacking, nearly a quarter did not change their password afterwards.[128]

In relation to misinformation or disinformation, people express high levels of confidence in their ability to identify and manage their interactions, yet their behaviours do not fully support this. Ofcom data on adults' media use found that internet users were less likely in 2019 than in 2018 to make checks on the factual information they find online: 29% don't make any checks (23% in 2018).[129]

With regard to personal data, Ofcom's survey gives internet users four ways in which online companies can collect their personal information. Positively, 88% are aware of at least one of these ways (an increase from 2018) but only 39% are aware of all four ways. Most worryingly, 44% of those who say they are confident in managing their personal data are unaware that information about them can be collected through their smartphone apps. Despite this, nearly three-quarters of internet users felt very or fairly confident in their ability to manage their personal data online.[130] A similar picture emerges from research conducted for the Office of the e-Safety Commissioner in Australia. While most adults surveyed said they need online safety information, only one in ten adult Australians searched for or received this.[131]

[125] Carnegie UK Trust (2018), Kennedy et al (2019)
[126] Digital Schoolhouse (2020)
[127] Nominet (2019)
[128] Nominet (2019)
[129] Ofcom (2020)
[130] Ofcom (2020a)
[131] Office for e-Safety Commissioner (2020)

A 'privacy paradox'

Several studies on online safety and data privacy, suggest a sense of 'apathy', 'digital resignation' or 'powerlessness' about what an individual can do to protect themselves.[132] Indeed, half of respondents in one survey felt it is 'part and parcel' of being online that people will try to cheat or harm them in some way; a similar number felt they had no choice but to sign up to online services despite misgivings; 45% felt there's no point in reading terms and conditions because companies will do what they want anyway.[133]

The term 'privacy paradox' has been used to explain why people say they are concerned about data privacy yet do not act in ways that support this.[134] As consumers, people may want contradictory things - for example, opposing targeted advertising yet valuing the benefits.[135] And, as community partners and digital champions also identified, some of this is about familiarity and convenience - saving time, making life and decisions easier, and getting accustomed to the online everyday world.[136] This can be even more so when people may be newer to the internet or have limited digital skills and confidence; it is easier, simpler and quicker to stay logged on, accept all cookies, save online payment details, and not change default privacy settings.[137] Understanding the beliefs and factors that underlie this privacy paradox matter because they carry implications for interventions. As noted by the Carnegie UK Trust in their review on data privacy, there appears a need for greater awareness about what 'good' privacy protection means.[138]

The need for better public understanding about personal data and the digital world is also supported by a recent study for the Information Commissioner's Office which compared people's views towards targeted online advertising (Adtech) before and after receiving information about how it works. After finding out how Adtech works, 43% or participants felt it was unacceptable (compared to 14% before having information); 36% felt it was 'acceptable' (compared to 63% before having this information).[139] With regard to online harms, a report by the Centre for Data Ethics and Innovation found limited data on the direct consequences of online targeted advertising but noted that absence of evidence is not absence of harm. Potential harms include: manipulation of behaviours or beliefs, exploiting first-order preferences, exploiting vulnerabilities, internet addiction, amplification of harmful content, polarisation, discrimination and potential use for malicious intent. At the same time, online targeted advertising is seen by many as desirable, even essential, for improved user experience such as better product suggestions and finding like-minded people.[140]

[132] Kennedy et al (2020), Carnegie UK Trust (2018)
[133] Doteveryone (2020)
[134] Kennedy et al (2020), Carnegie UK Trust (2018)
[135] Kennedy et al (2020)
[136] Deloitte (2020), Broadband Stakeholder Group (2020)
[137] Community partners consultation, September 2020; One Digital (2019)
[138] Carnegie UK Trust (2018)
[139] ICO 2019 (with Harris Interactive)
[140] CDEI (2020c)

Actions people take to protect themselves

Research for Ofcom and the Information Commissioner's Office (2019) looked at the steps people take to protect themselves online. The most common actions to avoid online harms were only using trustworthy websites and ignoring requests from strangers; the least common responses were blocking pop ups, deleting browser histories and changing passwords regularly. As regards responses to online harms, the most common responses were scrolling past content, treating stories with scepticism and ignoring upsetting content. The least common responses were reporting to the police and reporting to platforms.

Among parents, using platform or device parental controls, locks and filters was reported widely but this was much less so among adults without responsibility for children - some of whom were surprised that these existed and wanted to learn more.[141] People felt individuals and parents should take responsibility for protecting themselves - alongside more regulation and tech companies and social media platforms doing more to protect people online.[142]

Reflecting the earlier discussion about experience - people said they developed their approaches to being safe online through their experience of using the internet. How people felt about using the internet and their own ability to use it safely tended to reflect past experiences; those most confident had no or few bad experiences online. Some felt much less in control, and saw no alternative - reflecting bad experiences they had, or knew about through others. People's approaches ranged from more and less active, for example reporting or ignoring harmful online content. Some protected themselves through avoiding certain platforms, only using websites they'd used before, or only using websites with the secure padlock in the corner of the HTTPS bar.[143] These strategies chime with the experiences of community partners, digital champions and individuals (discussed in the next below).

[141] Ofcom/ICO (2019)
[142] Ofcom/ICO (2019); also chimes with Doteveryone (2020), Nominet (2019), Demos (2020)
[143] Ofcom/ICO (2019); Ofcom (2020c)

As part of this project, we spoke with five people (contacted through community partners) to find out their views on online safety and available resources - we particularly wanted to learn from people who are already active in using strategies to protect themselves (and in some cases, to protect others) online. Their approaches reflect wider insights from the evidence base (such as the added online risks faced by disabled people, and the worries about 'consumer' harms as well as online abuse). Spanning different ages (from twenties to eighties), all five people regard themselves as confident online; all still feel it needs to be easier for people to find information and support to stay safe.

Case studies

Lucy

Being younger, disabled and now required to shield during Covid-19, safely accessing the online world is crucial for Lucy to continue with her learning, stay in contact with friends and to get support with her health. Lucy relies on her mobile and tablet for online shopping, banking and learning. After being a victim of online harassment, which later manifested in physical harm, Lucy is acutely aware of the ease with which people can access personal data and use it maliciously and to harm. Lucy feels she was always relatively safe online (changing passwords, avoiding suspicious websites) but experience of online abuse has made her more aware of the dangers of social media. One of her friendship groups of younger disabled people regularly shares tips and scam warnings via Whatsapp. Lucy feels disabled people are particularly vulnerable to online scams and abuse. Often, everyone in Lucy's Whatsapp group gets the same fake emails about being entitled to support or financial aid. When Lucy has a worry about online safety, her first port of call is Google search, followed by checking with her parents. Lucy feels there needs to be more information for disabled people about online safety, covering both threats and harms as well as tips about how to stay safe online.

Abeo

Abeo, an asylum seeker in his twenties/thirties who came to the UK just over a year ago, is adept with computers - volunteering as a digital champion in his community. He has used resources such as Learn My Way, Make it Click and Future Learn to improve his English and digital skills simultaneously. Abeo feels staying safe online is part and parcel of how he uses the internet everyday. Abeo's main concerns about online safety are scams and theft of personal information. He actively checks on the latest scams and regularly participates in online forums to 'keep one step ahead' of anyone trying to cause trouble. Abeo worries that other refugees and asylum seekers fall prey to scams - reflecting language barriers and trust. For Abeo, online privacy is a key issue; he no longer trusts social media and has removed himself from many platforms: "nothing or nobody is really safe online anymore. Whatever you have said or done in your past will always come up later". Abeo is a digital champion at the community organisation which supported him when he arrived in the UK, and now he provides support to others to get online safely. He has become a key point of contact for lots of other learners, especially from refugee and asylum seeking communities.

Case studies

Susan

Susan is in her fifties and a confident laptop and mobile phone user. She uses the internet to shop online, compare products, do bills, and use chat forums. Lockdown has helped her develop her Skype and Zoom skills. Even so, online safety is still a concern. She makes sure she is 'on top' of her passwords and is scam aware but still finds herself being lured into scams that seem very real. Susan knows some adverts, even on trusted websites, can be harmful. For Susan, online safety is "all about using your common sense and you can get a sense when something doesn't feel right". She limits internet use, only going through trusted companies she knows. Recently, she found out the hard way about fake reviews for products on websites she trusts such as Amazon. Susan has learned about viruses, but has not yet paid for any anti-virus software as she is unsure what to get. Susan suggests that online safety resources could be improved by including examples of current scams and phishing emails; or a place where people could add in ones they have received.

Graham

Since retiring, Graham (now in his seventies) has remained a fairly confident laptop user. He is aware about online risks and uses different strategies to stay safe. Scams and phishing emails are the main issue. He deletes those that appear suspect, but feels alarmed when they contain personal details such as his phone number or postcode. He always calls his bank to check when emails appear to come from them. Misinformation through Facebook is another concern; he sees a lot being shared that he knows isn't true and sees his friends sharing it. For Graham, it is all about "spotting the little signs". Whether it is an email, an advert or a news story, things such as spelling mistakes and poor quality photos always make him suspicious. He worries that other older people "tend to think that everything on the internet is legitimate and free" and "don't know how to do proper searches on Google". Graham feels there aren't a lot of places he can turn when he wants support with online safety. He used a BT resource for a while, but he felt the information was too broad and more focused on statistics. Graham would like a good website with lots of resources, including about updating your computer, and how to assess whether a website can be trusted. Graham actively shares information about scams with groups he is in.

Mary

Although now widowed, Mary and her husband got their first laptop 6 years ago and she loves it (although her husband refused to use it). Mary, in her eighties, says she "is not brilliant on the laptop by any means", but she is able to do lots of tasks such as banking, shopping and Duolingo. She has a smartphone, but prefers the laptop. Although Mary is confident about being online and feels that she can recognise scams, she is alarmed when her landline gets called saying she has a problem with her computer; and when she gets emails from friends which look like their account has been hacked. Mary finds the constant popup adverts hard to navigate and has sometimes ordered things she didn't want. She is less worried about misinformation as she only uses websites she trusts (BBC, Wikipedia). If Mary ever has a problem on her computer or is worried about something, there is a young man in her area who comes over to help her for free. He can support her over the phone or remotely by logging into her computer from his. Mary has trusted him for many years and heeds his advice, as he is always very up to date. Mary would like a website which listed the most recent scams or things to watch out for.

These five stories also reveal some of the actions that people take to protect others online.

Actions people take to protect others

Across reports, it is clear that most people see protection from online harms as a matter for shared responsibility across individuals (adults and parents), government and regulators, and companies. Less explored - but important - is the responsibility that people feel towards each other, including the practical actions they take to protect others from online harms.

Qualitative research exploring people's actions found that some participants clearly saw online safety as a collective (as well as individual) responsibility; talking to others, sharing information about scams, and in particular encouraging older relatives to get in touch if they were unsure about anything online, and helping them update security settings on their devices.[144] Evidence from the USA suggests that 30% of US adults have intervened when witnessing the online harassments of others.[145] Evidence from the UK finds that most people initially ignore or block observed online abuse, although they are more inclined to report attacks where they identify the individual as vulnerable.[146]

As part of the Nuffield Foundation / University of Liverpool exploration of citizens' data literacies, researchers have asked people a number of questions to understand how they support others:[147]

- 'Have you ever used internet search during a conversation with your friends or family to verify information that you discuss? ("let's Google this…")'
- 'Have you ever encouraged/ taught others how to stay safe online (e.g. by showing them privacy settings of software tools? (e.g. virus checkers)'
- 'Have you ever encouraged others to fact-check? (e.g. by conducting other searches or using other media)'
- 'Have you ever helped others to protect their personal data online?'[148]

Analysis of the data - including by socio-demographic characteristics known to correspond with digital exclusion (such as age and educational attainment) - reveals that people's actions differ according to the type of internet user they are.

People categorised as the most extensive internet users participated most in these practices - whether through online forums, showing people how to fact-check or set up secure passwords. This type of internet use is mostly found among those who are better off and better educated. Even this group did not demonstrate a deep engagement with data as part of their civic or personal lives. By comparison, the researchers found that people with lower levels of education and socio-economic status were less likely to encourage others to stay safe or fact check or help others to protect themselves online.[149] People in these groups are more likely to be 'limited' users of the internet (using the internet for very few things, or for social media and entertainment only). The next phase of the research will bring together citizen groups to explore these issues more fully.[150]

[144] Ofcom/ICO (2019)
[145] Davidson et al (2019) citing Pew Research Centre
[146] Ofcom/ICO (2020)
[147] Yates et al (2020b)
[148] Yates et al (2020b)
[149] Yates et al (2020b)
[150] Me and My Big Data project (University of Liverpool with Nuffield Foundation)

This raises important questions about how adults - especially those who may have lower digital confidence and face additional disadvantages and marginalisation - can access support to stay safe online, and can be empowered to support others in their families and communities. This is becoming critical for online safety as - according to the latest research by Doteveryone - only a third of respondents (34%) said they know where to go for help when they experience a problem online.[151]

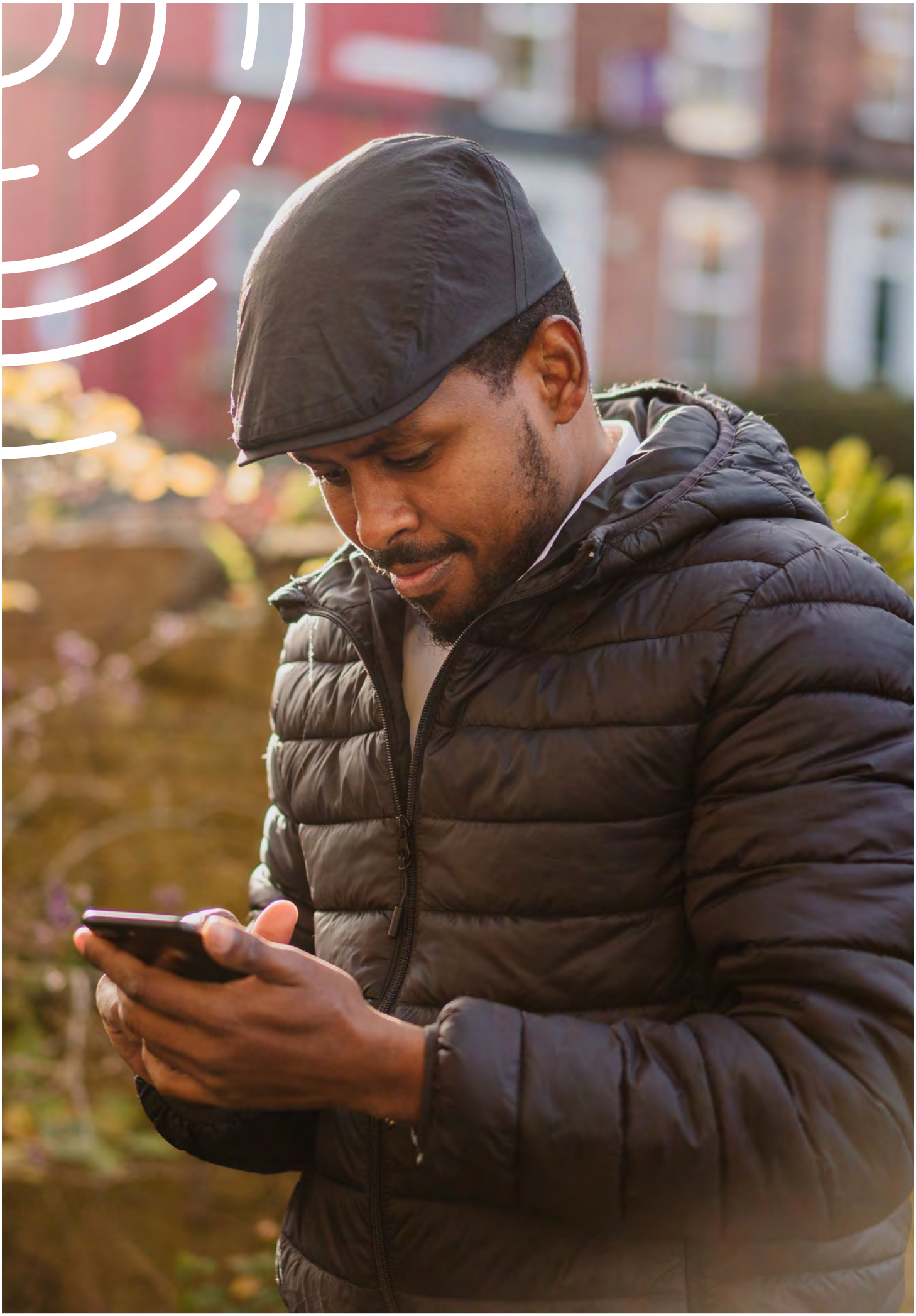
As recently championed by Glitch with regard to online abuse - to complement robust regulation and online harms legislation:

> *'The government should invest more resources into digital citizenship education in the UK, including how to stay safe online, how to respond to online abuse and how to be an active online bystander. Digital citizenship programmes remain severely underfunded in the UK. As COVID-19 pushes citizens to spend more time at home and rely increasingly on the internet and social media for work, socialisation and volunteering, greater investment in ambitious digital citizenship programmes and support to civil society organisations carrying out this work is vital.'*[152]

Conclusion

Available evidence shows that everyone can be vulnerable in some situations, but certain groups of people are more likely to be targeted, or more likely to experience negative impacts from online harms such as abuse or fraud. Disability, ethnicity, gender, age, low education, low income - are all among the factors that shape people's ability to protect themselves and others online, and their exposure to online harms. Several of the factors that correlate strongly with digital exclusion (low socio-economic status and low education) also appear to shape people's ability or capacity to protect others they know - whether as parents, friends or members of the community. The evidence also points to the importance of personal experience in building digital resilience, and the value of being able to access support to reflect and recover from negative experiences as part of building this resilience.

[151] Doteveryone (2020)
[152] Glitch (2020)



Chapter 2:
What is the policy context for online safety, with regard to digital inclusion and older, vulnerable or disadvantaged adults?

From a policy perspective, there is a window of opportunity with a number of significant pieces of work underway of relevance to online safety and digital inclusion. Yet - despite increased awareness of digital exclusion and data poverty among civil society organisations[153] and in the media[154] - there is a risk that digital inclusion and everyday online safety are getting missed in an increasingly complex policy and regulatory environment.

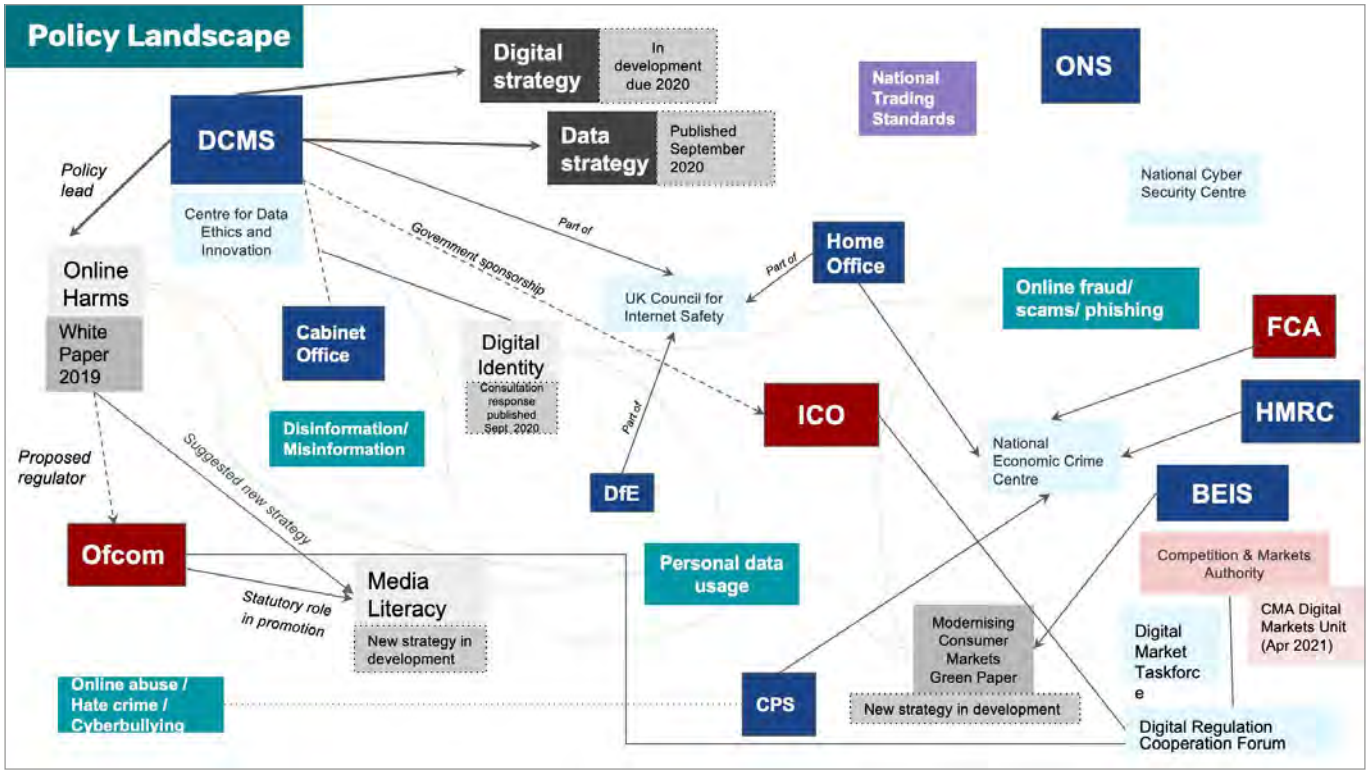
At time of writing, the UK government is finalising its full response following the Online Harms White Paper consultation (the government's interim response was published in February 2020) as it prepares for new legislation and regulation.[155] A Media Literacy Strategy is also being developed as part of the government's approach to online harms.[156] In September, the Government published its National Data Strategy, which is now out for consultation.[157] Important work on digital identity is underway in the context of Covid-19 and Government Digital Services.[158] A new Digital Strategy (to follow the current Digital Strategy[159]) is being developed, with an expected focus on using data and digital technologies to power economic recovery.[160] As of September 2020, there is entitlement to funding for adults with low digital skills to take Ofqual approved Essential Digital Skills courses in England, building on the Essential Digital Skills Framework.[161]

Alongside these developments, led by the Competition and Markets Authority, following direction from BEIS, UK regulators have been reviewing their approaches to consumer vulnerabilities in the context of smart and open data and the digitalisation of goods, products and services.[162] The UK government recently announced that a new Digital Markets Unit will be set up in the Competition and Markets Authority to write and enforce a new code of practice on technology companies.[163]

The Scottish Government is consulting on a renewed Digital Strategy, in the context of Covid-19, with greater emphasis on eliminating digital exclusion and setting a vision for Scotland as an ethical digital nation.[164] The Welsh Government has started to engage on a new Digital Strategy for Wales, with clear links to the seven national well-being goals enshrined in the Wellbeing for Future Generations Act.[165] Combined and local authorities across the UK are also developing or reviewing their responses to digital in the context of Covid-19.

[153] For example: APLE Collective (2020), Nesta (2020), Older People's Commissioner Wales (2020)
[154] For example: Blair (2020), Kelly (2020)
[155] DCMS & Home Office (2020)
[156] DCMS & Home Office (2020, 2019)
[157] DCMS (2020)
[158] Cabinet Office & DCMS (2020)
[159] DCMS (2017)
[160] DCMS & Rt. Hon. Oliver Dowden MP (2020)
[161] DfE (2019)
[162] BEIS (2019); CMA (2019); FCA (2020a)
[163] BEIS & DCMS (2020)
[164] Scottish Government (2020)
[165] Welsh Government (2020)

This breadth of activity in policy and regulatory spheres speaks to the significance of data and digital technologies across government departments, and at all levels of government. It also highlights the challenge of where responsibility lies to ensure that citizens are protected from online harms - including consumer harms; empowered and supported to navigate the internet safely; able to make informed decisions about their data; and able to assess the trustworthiness of online content.



Online Harms White Paper

The Government has prioritised making the UK the safest place in the world to be online, and is developing significant legislation to tackle online harms. Online harms are defined as 'online content or activity that harms individual users, particularly children, or threatens our way of life in the UK, either by undermining national security, or by reducing trust and undermining our shared rights, responsibilities and opportunities to foster integration.'[166] Measures are likely to follow the recommendations of the Online Harms White Paper, including a new statutory 'duty of care' to make companies take more responsibility for the safety of their users and tackle harmful user-generated content - enforced by a new regulator (or Ofcom) and a new regulatory framework.[167] The White Paper outlines the proposed online safety measures, both legislative and non-legislative, that will make companies more responsible for their users' safety online.

One of the challenges inherent in legislating against online harms is the fast pace of technological change, making it difficult to predict or understand harmful consequences. This is heightened where online practices may be legal but potentially harmful to individuals, businesses and wider society. The pace of evolution underlines the importance of a statutory 'duty of care' which applies a 'precautionary principle' - placing responsibility for managing and mitigating risks of harm onto tech companies, recognising their role in making design choices which enable, and even encourage, the spread and promotion of harmful user-generated content.[168]

Over 2,400 responses were submitted to the consultation following the White Paper, and debates have continued on what was proposed and equally what was considered to be absent or overlooked.

From the perspective of older people, vulnerable adults and disadvantaged adults, the absence of 'consumer' or 'economic' harms (such as online fraud or scams) has been challenged by a number of stakeholders - including UK Finance, the collective body representing the banking and finance industry, and civil society organisations such as Carnegie UK Trust and the Money and Mental Health Policy Institute. They cite the rising use of social media for scams and fraud, the damage caused, and the limited effectiveness of existing regulators such as the Financial Conduct Authority to address this with social media companies. From the perspective of women, Black and minority ethnic communities and non-binary people, gender-based and intersectional online abuse has been highlighted for greater attention.[170] These calls have grown stronger since the outbreak of coronavirus, reflecting the mental, physical, financial, and emotional damage caused by online fraud and scams and online abuse; and evidence in an upsurge since the pandemic started.[171]

Irrespective of whether consumer harms are brought within scope of future legislation, there is a compelling case for stronger regulation around consumer online harms, and better coordination across regulators. The new Digital Regulation Cooperation Forum is a positive step.

There is strong evidence that the public sees online safety as a shared responsibility - across government, regulators, industry and individuals - and that the public also expects more robust regulation of the internet, with 58% believing that the tech sector has too little regulation.[172] According to Ofcom/ICO, eight in ten people would like websites to do more to keep them and others safe.[173]

[166] DCMS & Home Office (2019)
[167] DCMS & Home Office (2019, 2020); Ofcom may be given the role outlined for the new regulator.
[168] Woods & Perrin (2019), Carnegie UK Trust (2020)
[169] Carnegie UK Trust (2020)
[170] Glitch (2020)
[171] Carnegie UK Trust (2020) citing the National Crime Agency and Victim Support; Glitch (2020), Money and Mental Health Policy Institute (2020)
[172] Doteveryone (2020)
[173] Ofcom/ICO (2020)

As part of their work with Carnegie UK Trust on online harms reduction in social media, Woods and Perrin have produced detailed proposals for a model to reduce harms through an ongoing process of: platform design, continuous risk assessment, Terms and Conditions and software (reflecting the risk assessment), software that distributes content, the tools users have to protect themselves, and clear approaches to complaints and enforcement when these processes fail and harm is still manifest. More recently, Woods and Perrin have done further work on how to address concerns around online harms which are currently outside scope, the roles of other regulators (assuming Ofcom is appointed as the regulator), and the need for more certainty for companies and victims.[174] They propose that any new regulatory framework should be accompanied by or incorporate 'a system of regulatory interlock based on existing principles of regulatory co-operation.'[175] A framework of 'interlocking regulation' would allow or require regulators to work together on issues that fall within a specialist regime but also constitute or contribute to harm within the online harms regime. This would be particularly important if 'consumer' harms (such as online scams) remain outside the scope of online harms legislation.

Media Literacy Strategy

Ofcom has a responsibility around citizenship and children's and adults' media literacy, including reporting every year on trends in media literacy and convening others as part of its Making Sense of Media programme. Throughout the pandemic, Ofcom has been monitoring the spread of misleading information.[176] At the height of the crisis, around half of the UK population had been exposed to misleading information about Covid-19 within the past week.[177] Since then, this has decreased but remains a significant problem, with social media being the main source. Other research found that those getting information from social media appear both more likely to believe conspiracy theories and to have broken lockdown rules.[178]

In July 2020, the DCMS Select Committee reported on an inquiry into the impact of misinformation about COVID-19, and the efforts of tech companies, the regulator and other public sector bodies to tackle it. It found that innovations to tackle misinformation (such as warning labels and tools) were applied inconsistently, and business models disincentivised tech companies to act. The Committee expressed concern that the proposed Online Harms legislation would not do enough to address harms caused by misinformation.

Identifying misleading information requires a level of media literacy. While Ofcom has a clear role in monitoring trends, it is less clear about whose responsibility it is to help adults - including older people and vulnerable adults - to develop critical skills around sourcing information online, verifying information, and improving their online media literacy.

Recent reviews of literature on public understanding of data practices, and analysis of digital and media literacy among limited users of the internet, point to the growing overlap between media literacy, digital literacy and data literacy.[179] As technologies, services and devices have evolved, so the set of skills people need have become more complex.[180] Given this, the forthcoming Media Literacy Strategy is a timely opportunity for future-proofing.

[174] Woods & Perrin (2020)
[175] Woods & Perrin (2020)
[176] Ofcom (2020d)
[177] Ofcom (2020d)
[178] Duffy & Allington (2020)
[179] Kennedy et al (2020), Carmi et al (2020), Yates et al (2020a), DCMS Select Committee (2019)
[180] Carmi et al (2020)

The Government recognises that all users should be empowered to understand and manage risks so that they can stay safe online: this goal cannot be realised without bringing together digital, data and media literacy, rather than seeing them in silos; seeing these skills in the context of real-world online safety (e.g. how people have the digital health literacy to spot misleading health information or the digital financial literacy to use online banking safely). Positively, the Government has recognised that there are gaps in provision and that adults also need support, both for themselves and as parents or carers.[181] It is critical that this includes older adults, vulnerable adults and those who face wider disadvantage, alongside disabled adults. More broadly, there is a need to evolve concepts of digital inclusion to encompass digital resilience, understanding and citizenship. [182]

Data Strategy

In September 2020, the UK Government published its National Data Strategy, setting out a framework for how data is approached, used and invested to be a powerful driver of UK economic growth and innovation. The strategy recognises the need to improve public trust and confidence in the use of their data, especially public sector data. It acknowledges that people should 'be empowered to control how their data is used and supported to have the necessary skills and confidence to take active decisions around the use of their data' and 'recognise their responsibility to consider how their data – used responsibly and fairly – can create a better society for all'.[183]

One of the planned actions is a national engagement campaign on the societal benefits of the use of government data. This reflects findings from the Centre for Data Ethics and Innovation about the need to conduct sharing of personal data in ways that are trustworthy, aligned with society's values and people's expectations.[184] However, such efforts may falter if citizens are not empowered and supported to develop their understanding of data, given worries about personal data security, identity theft, and how organisations use their data.[185] As noted in Deloitte's latest survey on digital consumer trends, while consumer trends may show increasing acceptance and diminishing concern about personal data, this does not mean the issues will come off the table: 'With every year, more data will be generated from more devices. And with every year the precision of policies on data privacy will need to become more refined and resilient. Data privacy will continue to be a core discussion among companies and their regulators and deservedly so.'[186]

[181] DCMS & Home Office (2019)
[182] Digital resilience - UK Council for Internet Safety (2020); Digital understanding - Doteveryone (2018); Data citizenship - Yates et al (2020b); Digital citizenship - Glitch (2020)
[183] DCMS (2020)
[184] CDEI (2020b)
[185] Ofcom/ICO (2020), Ofcom (2020c), Kennedy et al (2020)
[186] Deloitte (2020)

Digital Identity

The recent Digital Identity Consultation Response brings the fast-changing digital landscape into sharp focus. Covid-19 has meant that being able to identify digitally has become essential for everyday life - whether managing money online, ordering a repeat prescription, or using government digital services. This has heightened the need for secure and trusted online solutions. Civil society organisations, responding to the call for evidence, highlighted instances where digital identity systems increase the exclusion of vulnerable adults.[187]

There is an opportunity here for inclusive design, carefully testing with people who have low or limited digital access or skills, to mitigate risks of unintended exclusion. Alongside this, however, there is a case for continued investment in the provision of remote and face-to-face digital support (or digital assistance) for national and local government services. Evaluation of a face-to-face digital support service for use of HM Courts and Tribunals Services found that the reasons people need to use the face-to-face digital support service fell into five groups, which often overlapped:[188]

- Low digital skills, limited internet access or low digital confidence
- Low confidence completing, or difficulty understanding, HMCTS forms
- No or low English language proficiency for speakers of other languages
- Stress caused by a life transition or negative experience with government services
- Multiple and complex support needs.

Essential Digital Skills

The Essential Digital Skills Framework outlines the skills needed to 'safely benefit from, participate in and contribute to the digital world of today and the future'. The framework outlines five categories: communicating, handling information and content, transacting, problem-solving, and being safe and legal online. Being safe and legal online wraps around the other four categories. The five online safety skills are:

- Password security – able to use different and secure passwords
- Able to respond to requests for authentication of own online accounts and email
- Able to set privacy settings
- Able to identify secure websites (e.g. by looking for padlock/https in address bar)
- Able to recognise suspicious links (e.g. in emails, social media, pop-ups)

The category of 'handling information and content' is relevant to media literacy:

- Able to understand that not all online information and content is reliable
- Able to evaluate what information or content may, or may not, be reliable.

In 2019, a new National Standard for Essential Digital Skills Qualifications, was created ahead of the introduction (September 2020) of an entitlement to funding for adults with low digital skills to gain an approved entry-level qualification in essential digital skills.[189] This relates to the recent announcement of employer-led, sector-specific digital skills boot camps[190] and the significant drive to increase digital skills to power economic recovery. What is less clear is whether the Government will invest in supporting more people - including older people who may be retired or full-time carers - to get online and build their digital skills and confidence.

[187] Cabinet Office and DCMS (2020)
[188] Good Things & HMCTS (2020)
[189] Ofqual (2020)
[190] More detail on digital skills bootcamps is expected in the Further Education White Paper.

More broadly, the Essential Digital Skills Framework provides an excellent foundation for developing digital skills and confidence. Nonetheless - just as the current framework was an evolution of the 2015 Basic Digital Skills Framework - there is a case for further evolution to reflect the skills and confidence required to navigate the internet, make decisions about personal data sharing, feel empowered to protect oneself and others from online harms and seek redress, and be a resilient and active digital citizen.

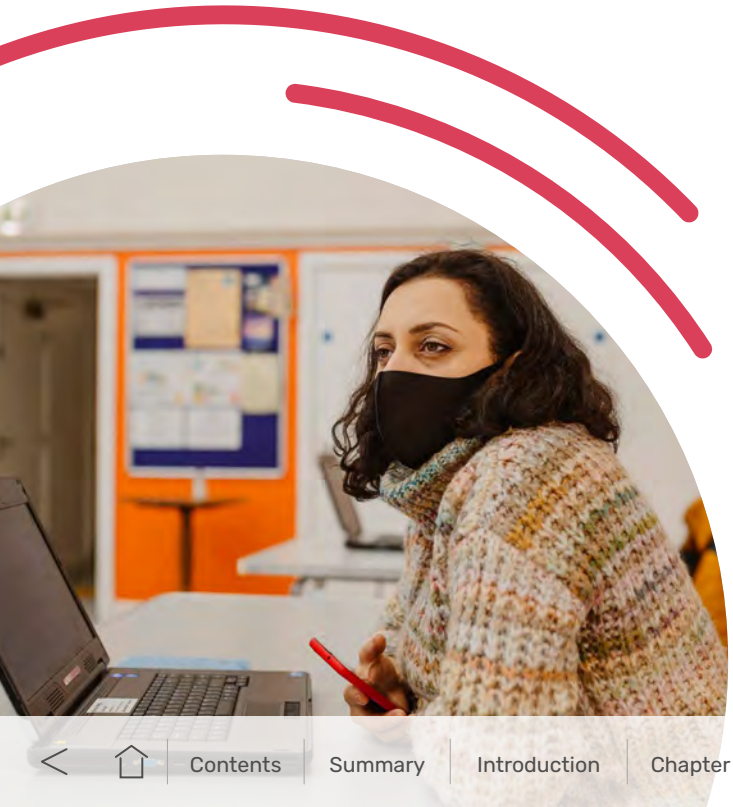
A New UK Digital Strategy

The outgoing Digital Strategy focused on building digital skills (basic to specialist) - including free access to basic digital skills training and the creation of a new Digital Skills Partnership to bring together the public, private and charity sectors. Early comments from Minister Oliver Dowden on a new Digital Strategy indicate a likely shift in focus to a data-powered and technology-led economic recovery.[191]

It remains uncertain to what extent issues around online safety and security will feature in the new strategy, or the prioritisation of digital inclusion - access, skills and confidence - for the millions of people who are offline, or lack the skills and support to use the internet fully.[192]

In a recent paper, Good Things Foundation has called on the government to invest in a 'great digital catch-up' for those who are unable to use the internet independently. According to Lloyds Bank's Consumer Digital Index, around 9 million people are unable to use the internet without help and a further 2.7 million people lack the essential digital skills for life.[193] Recent research found that 75% of people think that every community in the UK needs a place people can visit to get help with internet skills, such as how to use online banking or access online education.[194]

Digital inclusion is a necessity, not a nice-to-have. As such, it should be a critical plank of the new UK Digital Strategy - to power up the economic recovery; to develop the level of social and civic understanding needed for public consent around personal data sharing; to prevent a deepening of digital inequalities, and to ensure that this is a Digital Strategy for everyone.[195]



[191] DCMS & Rt. Hon. Oliver Dowden MP (2020)
[192] Good Things (2020a, 2020b)
[193] Lloyds Bank (2020)
[194] Research by Ipsos MORI on behalf of Good Things, cited in Good Things (2020b); a nationally representative quota sample of 2,219 UK adults aged 16-75; online I:Omnibus; 28.08.20-31.08.20.
[195] Good Things (2020b)

Modernising markets and consumer vulnerability

As already noted, the policy and regulatory framework in this area is complicated, and changing. A new Digital Regulation Cooperation Forum (DCRF) has been set up to bring together the Competition and Markets Authority with Ofcom with the Information Commissioner's Office to coordinate online regulation affecting the digital economy. The regulatory environment will also be significantly shaped by decisions about an independent online harms regulator. The government has recently announced (in response to the CMA review on digital advertising) that the CMA will gain a new Digital Markets Unit from April 2021 - a 'tech regulator' which will write and enforce a new code of practice on technology companies, setting out the limits of acceptable behaviour, and aiming to create a more level playing field for technology companies as well as a fairer market for consumers.[196]

In the context of smart and open data, and the digitalisation of goods, products and services, the CMA has already asked all regulators to review their approaches to consumer vulnerabilities.[197] This presents an important - and in some cases, overdue - opportunity to consider digital exclusion as a contributing factor to consumer vulnerability.

Defining and identifying vulnerability is complex, requiring consideration of both individual characteristics (such as age, or low literacy) and situational factors (such as bereavement or poor health). While older age and disability are common flags of consumer vulnerability, not all older people or disabled people would be (or consider themselves) vulnerable. Anyone can find themselves in a situation where they are vulnerable to online harms.

In their report on fraud protections for people at risk due to a health condition or cognitive impairments, Demos highlights the challenges to practitioners (across police, health, care, and other sectors) arising from variation in definitions of vulnerability, while also recognising the value in different sectors taking different approaches which reflect their priorities.[198]

Self-disclosure and proactive identification are the two main approaches to identifying vulnerable consumers. However, low trust in organisations, time constraints, and concerns about personal data - as well as stigma - are barriers to self-disclosure; while lack of understanding and consistency can make proactive identification less effective.[199]

Definitions of vulnerability differ across regulators. The Financial Conduct Authority has been at the forefront of identifying the lack of digital skills (alongside low knowledge of financial matters, low financial capability, and low literacy) as contributing to vulnerability.[200] Ofcom encourages providers to take an inclusive view of vulnerability, and recognise that non-digital routes must also be provided. Even so, more could be done to define and identify digital exclusion as a factor in consumer vulnerability - with regard to access, affordability, digital skills, confidence and understanding (including about personal data and online safety) - and to incorporate this into guidance to firms, training of staff, and plans to use AI and data to identify potentially vulnerable consumers.

[196] BEIS & DCMS (2020)
[197] BEIS (2019); CMA (2019); FCA (2020a)
[198] Demos (2019, p.12)
[199] UKRN (2020a, 2020b)
[200] FCA (2020a, 2020b)

Conclusion

There is a window of opportunity with several significant pieces of policy in development relevant to online safety and digital inclusion. At the same time, this review of the policy and regulatory landscape shows how complicated the environment is and exposes a clear risk that digital exclusion and 'everyday' online safety issues (such as consumer harms) will fall between policies and strategies.

More regulators and companies are recognising the role of digital access and skills in shaping consumer vulnerability; but there's considerable scope for sharing best practice and - as the digital world evolves - for bringing different elements together as part of coherent strategies (for example - digital exclusion, consumer vulnerability, inclusive design, online safety and responsible technology).

Research shows that most people see online safety as a shared responsibility - across government, regulators, industry and individuals. Across research studies, it is clear that most people expect more robust regulation, greater accountability and transparency - with social media platforms in particular doing more to reduce online harms, particularly for those who may be more vulnerable.

The importance to the government, public sector bodies and industry of getting this right is also growing. Public trust and confidence in how organisations use and protect personal data is essential to realise the ambitions for a data-powered economic recovery and digital services for public benefit.


Quick and convenient shopping
Welcome to our new website
Register
Sign in
Help
83%
New to Tesco
Register

Chapter 3:
What is the practice context for online safety, particularly for older people, vulnerable and disadvantaged adults?

Recent years have seen a welcome increase in campaigns, collaborations, institutions and initiatives which aim to tackle online harms and raise public awareness and understanding. A list of relevant initiatives and useful resources is in the Annex.

Unsurprisingly, there are more resources around online harms and safety (including media literacy) for children and young people; some targeting parents, teachers and other professionals. There are also useful resources to support individuals, businesses and organisations to stay safe. Most are online, and assume that people have the access, motivation, knowledge and skills to find them, use and apply them in real life. However, as recent research into the attitudes of people who use the internet found: only a third of people (34%) said they know where to go for help when they experience a problem online.[201]

Older people, vulnerable and disadvantaged adults who experience some level of digital exclusion may face additional barriers to accessing support around online safety:

- Low digital, data, media literacy - which may affect ability to find, use, understand and apply information about staying safe online
- Not being able to afford devices, data connectivity, or technical software which would make it easier to stay safe online; or not knowing which option to choose
- Not being able to understand the advice and information provided due to English language, literacy or accessibility barriers (given literacy required to understand available resources)
- Not feeling able to ask other people for advice or support; not knowing anyone to ask or anywhere to look for support (online or locally)
- Not getting advice or support which is relevant or feels relatable (for 'people like me').

Below, we draw on insights from community partners and other civil society organisations, alongside evidence from research, to review the practice landscape.

[201] Doteveryone (2020)

Research, resources and campaigns

The role of technology in protecting people from online harms is a vital area for exploration. The Centre for Data Ethics and Innovation has highlighted the use of AI to identify vulnerable consumers. The Behavioural Insights Team has called for more work on use of digital tools (for example, to set a limit or self-exclude from gambling sites) to protect consumers, particularly vulnerable consumers, and encourage take-up of tools; and novel approaches to build consumers' resilience against challenges like disinformation and online fraud.[202] The DCMS Select Committee has called for introduction of 'friction' on social media sites so people think before they post or share.[203] Recent research reminds us of the value of simple signifiers - like the secure padlock in the corner of an HTTPS site - in helping people to stay safe online.[204]

In this context, the Government's recent announcement of £29m research funding to six research centres for work on online safety and privacy is a significant and much needed investment.[205] The new National Research Centre on Privacy, Harm Reduction and Adversarial Influence online (REPHRAIN) has been funded to develop automated tools to flag online harms in social media, and a map to identify and avoid different threats such as fraud or disinformation.[206] The Safety Tech Innovation Network will create a community of practice to use tech to make the internet safer.[207] Importantly, this includes how to design tech which addresses diversity, fairness, inclusivity and vulnerability.

Personal data (understanding; security; privacy) is another area where new initiatives have emerged to keep pace with smart technologies, open data, and use of AI and machine learning. The Centre for Data Ethics and Innovation was set up in 2019 to advise the government and regulators, and to give the public a voice in the governance of data-driven technology. 'Be Data Aware' is a public education initiative from the Information Commissioner's Office to help people understand how companies might use their personal data, and how they can take more control. The Government's new UK Data Strategy commits to a national public education campaign to build public confidence in data sharing for societal benefit.[208]

In the area of online abuse, tools are being developed by the Alan Turing Institute for automatically identifying and categorising hateful content online.[209] Civil society organisations like Glitch have developed toolkits for employers to improve online safety in the workplace, alongside undertaking research into intersectionality and online abuse.[210] Unsurprisingly, most resources and support with reporting online abuse are focused on children and young people - such as the important work of the 5Rights Foundation, Internet Watch Foundation and UK Safer Internet Centre.

Similarly, in the area of misinformation and disinformation, most resources relate to children and young people (or adults in their role as parents or educators). As the Government identified in the Online Harms White Paper (2019), there is a notable gap in messaging and resources around online media literacy for adults, which the forthcoming media literacy strategy is set to address.[211] This offers an opportunity to support initiatives that bring media literacy together with data and digital literacy. Ofcom's Making Sense of Media Network convenes relevant stakeholders as well as monitoring trends. The UK Council for

[202] Costa & Halpern (2018)
[203] DCMS (2020)
[204] Broadband Stakeholder Research Group (2020)
[205] DCMS, BEIS & Rt. Hon. Caroline Dinenage MP (2020)
[206] DCMS, BEIS & Rt. Hon. Caroline Dinenage MP (2020)
[207] DCMS, BEIS & Rt. Hon. Caroline Dinenage MP (2020)
[208] DCMS (2020)
[209] Vidgen et al (2019)
[210] Glitch (2020)
[211] DCMS & Home Office (2019)

Internet Safety (UKCIS) is a voluntary, non-statutory forum for the government, tech community and voluntary sector. For many years focused on children, it has since expanded its remit to include adults, especially parents and carers. Its Digital Resilience Framework is highly relevant to older, disadvantaged and vulnerable adults; it focuses on learning how to recognise and manage risk, learn from difficult experiences, recover and stay well.[212]

Public awareness of cybercrimes, especially fraud and scams, has also seen increased attention. Cyber Aware is part of the Government's National Cyber Security Centre (set up in 2016). The website has been updated as the place to get UK Government advice on staying safe online during the coronavirus period. Take Five is a campaign led by UK Finance (the collective body of the finance and banking industry) to equip people to protect themselves and others from fraud or scams. Friends Against Scams is an initiative of National Trading Standards. Citizens Advice also runs an annual Scams Awareness campaign.

Many companies are playing their part to educate and inform their customers through coalition campaigns, and by providing or promoting resources for their customers and the public. For example, as part of BT Skills for Tomorrow programme, people can access digital skills (including online safety) courses and resources produced by BT, Good Things Foundation and others. In the area of digital financial inclusion - where fears about online safety are a barrier to using online financial services and support, Mastercard is partnering with Good Things, CleanSlate and others on a campaign to promote help-seeking around financial health and online safety. There have been calls for more transparency from tech companies about how much abusive content they host; a more robust response; and for more comprehensive training for online content moderators.[213]

Some charities - nationally and locally - are providing or signposting information to service users, volunteers and staff, particularly vulnerable adults. This includes easy-read information on online safety for people with learning disabilities from CHANGE; online safety toolkits for organisations working with older people, people on low incomes, and with learning disabilities from Good Things Foundation; Age UK resources on internet security; toolkits for employers from Glitch; and dementia-friendly postcards to combat scams from the Alzheimer's Society. The One Digital programme website provides top tips for digital champions and project coordinators, with a focus on the five online safety skills in the Essential Digital Skills framework:[214]

- Password security – able to use different and secure passwords
- Able to respond to requests for authentication of own online accounts and email
- Able to set privacy settings
- Able to identify secure websites (e.g. by looking for padlock/https in address bar)
- Able to recognise suspicious links (e.g. in emails, social media, pop-ups).

So while there is information out there, only a third of people (from a survey of internet users) said they know where to go for help when they experience a problem online.[215] Indeed, one of the drivers behind the One Digital programme was that Digital Champions (whether peers, volunteers or staff) can be unsure about how to include online safety messages in the support they provide, and can feel overwhelmed by different messages about online safety.[216]

[212] UKCIS (2019)
[213] Vidgen et al (2019), Glitch (2020)
[214] Age UK, SCVO, Citizens Online, Digital Unite, Clarion Futures, with National Lottery Fund.
[215] Doteveryone (2020)
[216] One Digital (2019)

Relying on customers to find information on public or commercial sector websites can present a barrier to online safety and security. Regulators, banks and telecoms companies provide useful information (in some cases, offering free security software) but this can be hard to find and access. There are questions about the reach of public sector information into communities; the effectiveness of messaging; and confusion about where to go to report an online harm, check if something is an online harm, or seek support. Most of the information available demands a high level of general literacy - as well as data, media and digital literacy. This is where community-based support and support from peer mentors and digital champions can help.

In 2017/18, Good Things Foundation worked with 24 community-based organisations to help vulnerable people to use the internet safely; the programme took a flexible approach - encouraging experimentation and outreach - balanced with a focus on safe sharing of personal information; privacy settings on social media; and spotting scams and spam.[217] People receiving support had very different starting points and needs; but all moved forward, learning to do new things to protect themselves and gaining confidence in their ability. Across the three target groups - older people, people (mainly parents, working-age) on low incomes, and people with learning disabilities - there were some broad differences in interests and issues, which resonate with wider research. Older people were least comfortable with online transactions; working-age adults on low incomes were interested in making safer online transactions; whilst people with learning disabilities and low-income parents were interested in safe online sharing and social media privacy settings.[218]

For community partners, participating in the project deepened their own confidence and commitment to including online safety - noting the benefits for their own staff and volunteers as well as service users.[219]

Mozilla Foundation's Internet Health report calls for specially tailored digital skills training and learning formats for specific disadvantaged groups (including older people, and those with lower education); and to address the reality that most of us do not understand how internet technologies work or the implications of using them.[220] A holistic approach to understanding data is needed to support people across multiple avenues of their lives, not limited to work or using specific goods or services.[221]

Evidence from evaluations is sparse on what works in supporting people around online safety, media and data literacy - including evaluations of public education and awareness raising. This gap has been flagged by several researchers, including the Behavioural insights Team.[222] As Costa and Halpern note in their report on what to do about online harm and manipulation:

> *"This is about as important a challenge as we face in society today, and one which we need to ensure that our citizens can themselves be involved in fashioning. How we respond to, and shape, the evolving character of the digital landscape is precious not just because it is pivotal to our economies, but because it is society and the human character itself that we are shaping."*[223]

[217] Good Things (2018)
[218] Good Things (2018)
[219] Good Things (2018)
[220] Mozilla Foundation (2019)
[221] Carmi et al (2020)
[222] Kennedy et al (2020), Costa & Halpern (2018)
[223] Behavioural Insights Team (2018)

A community partner perspective

To inform this report, BT and Good Things Foundation facilitated a virtual workshop in September with community partners, and posed two questions in a Good Things community partner online survey in October 2020 (which received 124 responses) to get a grassroots perspective on the issues and the practice context.

Community partners confirmed the importance of online safety in their work, which impacts staff and volunteers on a daily basis. Online safety is seen as an active process that involves working closely with those they support - and involves behaviour change as well as developing skills and knowledge. Partners felt it is a challenging but also enjoyable and rewarding aspect of their work.

Community partners identified that a big challenge for people they support is the frequent bombardment from scams and phishing emails. Lots of people are aware of the risks (especially of being scammed), and feel that being safe online is a daunting task. Partners reflected that people are generally told what to do, rather than why, which means that they don't fully understand what is going on. Furthermore, older people's fears around online safety can result in many people stepping back from using technology entirely or for certain activities. One community partner noted that some people have laptops and tablets but are fearful to even start using these - whereas using smartphones and social media can give people a false sense of security. So community partners regularly have to remind people who are newer to the internet about wider dangers associated with social media and smart technologies. There can be additional issues where people have been given smart speakers or smartphones by relatives, set up to use them, but may not understand that this means they are connected to the internet.

Some community partners have tried to tackle the spread of misinformation and disinformation through social media in their communities by responding to comments online. They felt that social media can play a negative role in enabling (even encouraging) people to share misleading or false information. For some disabled people, the fact that certain websites require audio/visual verification can be a barrier to staying safe and to internet use more generally. Partners also identified poverty as a challenge, as not everyone can afford anti-virus software (or know which anti-virus software to buy, or which free anti-virus software to trust).

In our survey, we asked community partners about what aspects of internet safety they support people with. Fraud/scams and password safety were the most covered (71% and 70% respectively), followed by personal data management (65%) and online privacy (58%). Phishing was addressed by just over a third of partners (37%). Significantly, and worryingly, only 23% covered areas relevant to online harms around misinformation and disinformation; 19% on cyberbullying; and 18% on media literacy.[224]

We also asked community partners about the range of resources that they use, and encourage their clients or learners to use, to stay safe online. Unsurprisingly (given their membership of the Good Things network), Learn My Way was used by nearly 8 in 10 community partners (78%), and Make it Click (a digital skills directory for more advanced learners) was used by 6 in 10 partners (61%). A small number of partners were using other resources: Internet Matters 7%), Future Learn (5%), NSPCC (4%) and Friends Against Scams (3%)[225]. In the workshop, partners also identified Take Five, Age UK and Avast as sources of useful resources for online safety.

[224] Good Things community partner online survey, October 2020 (n= 124)
[225] Good Things community partner online survey, October 2020 (n= 124)

Community partners described delivering online safety support through group workshops, peer to peer models and in one-to-one sessions. During Covid-19, they have provided online safety support over the phone, which has been challenging but essential. Reflecting wider evidence on the role of personal experiences in shaping people's feelings and knowledge, community partners commented that online safety can be highly personal, with support best provided face-to-face. Some community partners found that online safety courses were a good way to get people engaged - alongside sharing their own stories and finding ways to bridge the conceptual gap between 'online' and 'offline' risks.

We asked community partners to comment on what is missing from online safety resources. Community partners highlighted the challenge of conveying the benefits of being online, alongside highlighting the potential dangers. They felt that online safety resources can feel "very threat heavy". This lack of balance can deter people from going online or trying new things. They also commented that people are 'thrown in at the deep end' with online safety; many resources are too complicated - which compounds the feeling that the internet is 'not for me'.

Community partners wanted resources which took a more holistic approach to the internet, and encouraged people to draw on how they keep themselves safe 'offline', applying this to the 'online' world (for example, shredding confidential documents). Positive stories and multiple formats (videos, texts, leaflets) as well as short content for 'quick wins' were felt likely to engage people better. But the bottom line was felt to be knowing you can get support from someone you relate to and trust.[226]

There is also interest to learn from others' practice experience - especially where practice is less developed, such as misinformation and disinformation, and where online harms can undermine community relationships:

> *"When issues around race appear in the news you can imagine the stuff that is then shared [through social media]. It would be great to develop an opportunity to learn from others on tackling this."*[227]

These findings suggest three areas for further work: (1) making it easier for community partners and digital champions to get involved in other national campaigns around online safety, such as Friends Against Scams; (2) up-to-date curation of the best resources; (3) addressing the gaps and supporting community partners to evolve their messages and approaches - to keep pace with the changing context of online safety and protection against harms. This is explored further in the next section.

[226] Community partner consultation, September 2020; One Digital partner workshop 2019
[227] Good Things community partner, November 2019; Hope not Hate (2020)

Framing and reframing practice as digital evolves

This review of the practice context points to several disconnects between what people say they want, and what they can find and use; and between existing approaches to equip and empower people to stay safe online and the new skills required - in the context of rapidly changing technologies. Covid-19 has further accelerated the pace of digital transformation in goods and services; and the appetite among providers (across sectors) to harness the power of data for the benefit of the economy, society, consumers and shareholders. In the last two years, several frameworks have been developed to support practice. The recent surge in use of AI, smart and data-driven technologies; and concern about online harms, suggests an urgent need to update approaches and make it easier for people and communities to get the support they need to stay safe and benefit from digital.

Essential Digital Skills Framework (2018)[228]: This framework updates the previous Basic Digital Skills Framework, and was co-created by experts from government, industry and civil society. It is the basis for the National Essential Digital Skills Standards; and puts digital literacy on a par with literacy and numeracy. On top of the basic foundational skills, the five key areas are: staying safe and legal online, communicating, handling information, transacting, and problem solving. The Lloyds Bank UK Consumer Digital Index tracks national progress based on analysis of customer and survey data.

Digital Understanding Framework (2018)[229]: Developed by Doteveryone, this set out what digital understanding means for people across four life roles: individual, consumer, worker, member of society. 'Digital understanding is not a race to be won or a series of boxes to be ticked. What is important is that people grasp the implications of their use of technologies to a level that's appropriate to their lives'.[230] As people need different levels of understanding, and at different times in their lives, the framework is built around three levels of understanding: 'Aware', 'Discovering' and 'Questioning'.

UKCIS Digital Resilience Framework (2019)[231]: This framework from the UK Council for Internet Safety is for organisations, communities and groups to help people build digital resilience. This involves: understanding when you are at risk online and being able to manage risk and make informed decisions; knowing what to do to seek help from trusted sources; learning from experience, including difficult experiences online; recovering when things go badly. Digital resilience is built through experience, rather than learning, but being able to talk, confide and reflect with people you trust is a powerful way to foster resilience.

Data Citizenship (2020)[232]: This data citizenship model is being developed and tested as part of the Me & My Big Data project led by the University of Liverpool with support from the Nuffield Foundation. It is focused on personal data literacy, with clear read across to digital literacy and inclusion. It responds to the rise in use and sharing of personal data, including AI and open data. The framework is currently being tested through focus groups with citizens. It is designed to encourage and support people to be active citizens in a datafied world; and is framed around: Data Thinking (critical understanding of data); Data Doing (everyday engagements with data) and Data Participation (proactive engagement with data, including through their personal and social networks).

[228] DfE (2018; updated 2019), Lloyds Bank (2020)
[229] Doteveryone (2018)
[230] Doteveryone (2018)
[231] UKCIS (2019)
[232] Yates et al (2020b)

Digital Citizenship (2020): Glitch defines digital citizenship as respecting and championing the human rights of all individuals online, encompassing individual, social and institutional responsibilities. Individual responsibilities include digital literacy, digital safety, their digital footprint, and digital self care. Social responsibility includes active bystander interventions online, and responsible and positive engagement online. Institutional responsibilities include the efforts of government and tech companies to ensure individuals - including with intersecting identities - can exercise their online rights; also responsibilities of civil society organisations and employers.[233]

5Rights Framework (2019): Developed by the 5Rights Foundation as a framework for online safety for children, the seven pillars translate well into what is needed - in policy and in practice - for adults as well as children, especially where adults face greater risks online. The seven pillars are: parity of protection, design standards, accountability, enforcement, leadership, education and evidence-based interventions. Education - of children, parents, educators - is positioned as a key component but never a substitute for making the internet safer.[234]

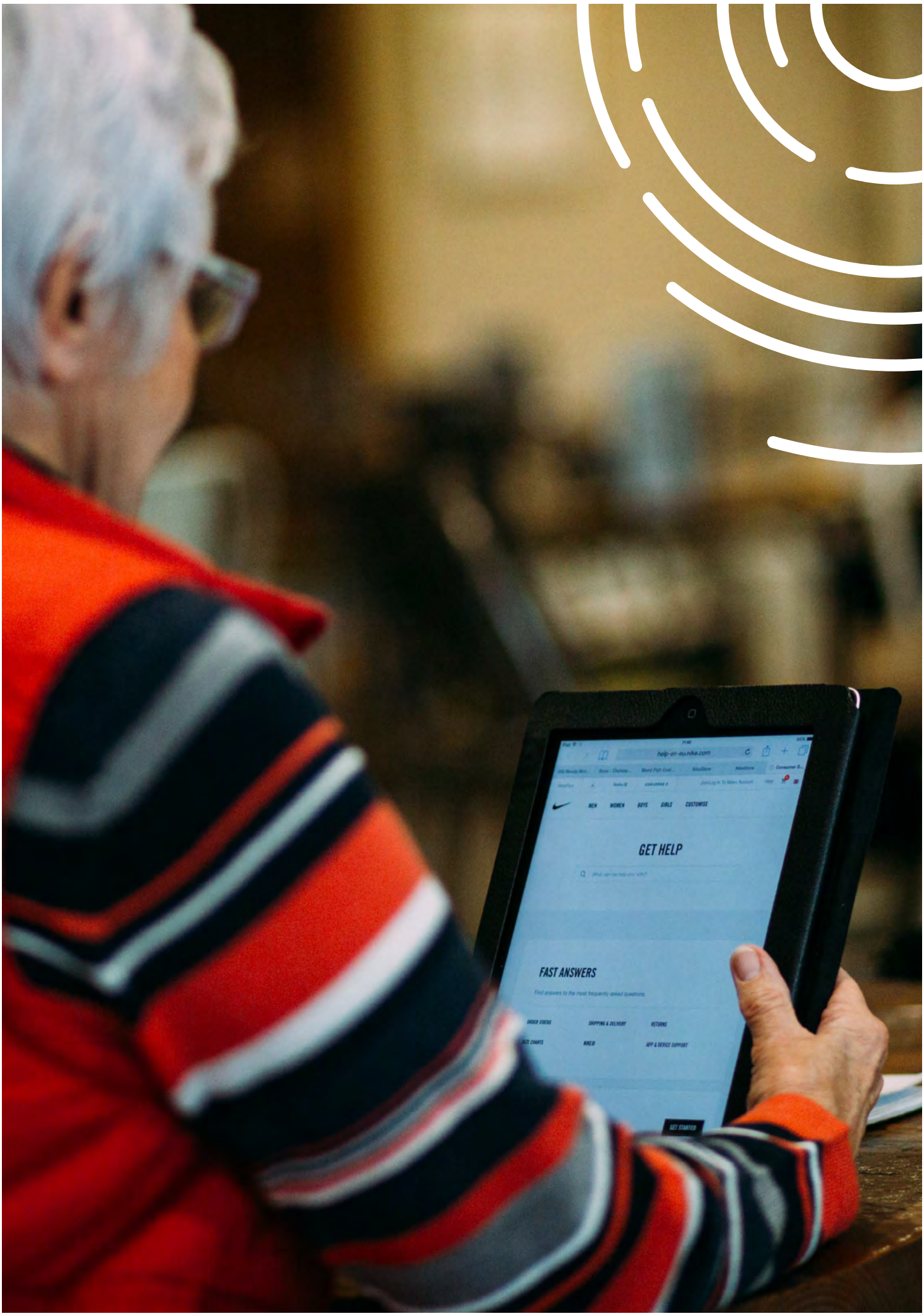
What is now needed - on the ground, in communities, and especially with regard to those most likely to face digital exclusion through older age, disadvantage and vulnerability - is an enhanced understanding of practical, effective ways to empower people to stay safe. Arguably, this needs to bring together the different aspects of digital, media and data literacy and understanding - rather than treating these as separate. It also needs to be situated as part of a better understanding of what we need to live well and safely in a digital world: a Minimum Digital Living Standard for the UK.[235]

Conclusion

There has been a welcome rise in campaigns, resources and initiatives to tackle online harms through public awareness and education - with a number of collaborations across companies, civil society and governments. There is little evaluation evidence about what works, which makes it hard to assess effectiveness and whether these resources are reaching those who could benefit most. Research suggests that many people still don't know where to find help when they need it. Most available resources are online, and assume people have the digital access, skills and confidence to find and use them. Community partners call for clearer messages and simpler rules of thumb, taking a more holistic approach to the internet and striking a better balance between conveying the risks and benefits of the internet. They also want opportunities to share and learn best practice with each other, including on 'newer' online harms impacting their communities.

Finally, the development of new frameworks by academics and civil society institutions is promising for practice - responding to the wider set of skills now needed in a digital world. Approaches to digital literacy and digital inclusion need to evolve to encompass concepts like digital resilience and digital citizenship, and public understanding of data and the digital world.

[233] Glitch (2020)
[234] 5Rights Foundation (2019)
[235] Good Things (2020b), Carnegie UK Trust (2020b)


help-en-au.nike.com
MEN
WOMEN
BOYS
GIRLS
CUSTOMISE
GET HELP
FAST ANSWERS
ORDER STATUS
SHIPPING & DELIVERY
RETURNS
SIZE CHARTS
NIKEID
APP & DEVICE SUPPORT
GET STARTED

4: Conclusion

Online safety is a shared responsibility between government, companies and citizens. As digital technology and use of data and AI evolves, we need to keep listening to people about what matters to them, how this differs for different groups, and how their concerns can be addressed.

Online safety is a shared responsibility between government, companies and citizens. As digital technology and use of data and AI evolves, we need to keep listening to people about what matters to them, how this differs for different groups, and how their concerns can be addressed.

Recent research by Demos for BT explored public attitudes on how the worst internet behaviours could be tackled, and found that many people were willing to trade some online freedoms to reduce harmful behaviours and the spread of hateful content.[236] Interestingly, while nearly two-thirds (64%) of people wanted to stop online user anonymity, there was less consensus about whether government agencies should be able to access private messages between two people. When people had a chance to deliberate this in focus groups, they were keen to discuss who decides what is harmful, and to consider the checks and balances required.[237]

The evidence is clear: people want more online safety information and trusted support which is easy to access, and protections especially for those who may be more vulnerable. Doteveryone found that only a third of respondents (34%) knew where to go for help if they had a problem online.[238] People we spoke to wanted to know where to find a list of current scams and threats; how to know which organisations they could trust; how to stop adverts and pop-ups; and where they could get help when they need it. Community partners we spoke to wanted a balance of positive stories to counteract fears; clearer messages and tips; and opportunities to share and learn best practice, especially on 'newer' online harms impacting their local communities (such as misinformation). Participants in a Citizens Advice survey wanted better information on what happens to their data and how profit is generated from data, as well as privacy guarantees.[239] Participants in a dialogue led by the Centre for Data Ethics and Innovation wanted to see more effort to improve people's understanding and control over online targeting systems, protections for vulnerable people, and greater accountability for online platforms. Almost 8 in 10 participants in an Ofcom/ICO survey said they would like websites to do more to keep them and others safe.[240]

[236] Demos (2020) for BT
[237] Demos (2020) for BT
[238] Doteveryone (2020)
[239] Kennedy et al (2020) citing Citizens Advice
[240] Ofcom/ICO (2020)

Evidence also shows that negative online experiences can make people (especially older people or newer users) step back from using the internet or avoid new technologies, as well as impact on financial, mental and emotional health. In some circles, concern is growing about online harms and large tech and internet companies, especially around social media and use of AI.[241] Any loss of public trust and confidence in how and why organisations use their data poses a threat to realising the individual and societal benefits of AI in areas such as public health, and in using the power of data to drive economic recovery and for innovations such as Open Banking.[242]

At the time of writing, the UK government is finalising its response to the consultation following the Online Harms White Paper alongside developing a new Media Literacy Strategy, UK Digital Strategy, and much-needed work on digital identity. A Data Strategy is out for consultation. UK Research and Innovation funding has recently been announced for online safety technologies. The Scottish Government is consulting on its new Digital Strategy, with greater emphasis on making Scotland an ethical digital nation and eliminating digital exclusion. The Welsh Government has started to engage on a new Digital Strategy for Wales, with clear links to the seven national well-being goals enshrined in the Wellbeing for Future Generations Act.

Across combined authorities and some local authorities, public sector leaders are working with industry and civil society partners to develop or refresh digital and data strategies. All this points to the importance of improving approaches to online safety and security - for citizens and communities, as well as for our economy and society as a whole.

Next steps

This review was generously supported by BT as part of BT Skills for Tomorrow. Together with BT, we will be publishing a set of recommendations to encourage further discussion about how to address the findings and rise to the challenges ahead.

[241] For example, 'The Social Dilemma' (Netflix documentary)
[242] CDEI (2020a, 2020b)


The
REALITY
FREE
INSIDE

References

5Rights Foundation (2019), Towards an Internet Safety Strategy.

Age UK (2017), Older people, fraud and scams. Briefing Paper.

APLE Collective (2020), Coronavirus response must include digital access to connect us all. JRF

Al-Muwil et al (2019), Balancing digital by default with inclusion: A study of the factors influencing e-inclusion in the UK. *Information Systems Frontiers* (21; 635-659).

APPG Financial Crime (2020), The impact of fraud and scams on vulnerable people.

BEIS & DCMS (2020), Government response to the CMA digital advertising market study.

BEIS (2019), The Government's Strategic Steer to the Competition and Markets Authority.

Blair, O (2020), Offline in Lockdown. Elle UK magazine.

Broadband Stakeholder Group (2020), Digital Exclusion Report 2020. Research by Savanta ComRes. (forthcoming).

Burgess, G (2020), Beyond the pandemic: Tackle the digital divide. University of Cambridge.

Buil-Gil, D et al (2020), Cybercrime and shifts in opportunities during COVID-19. *European Societies.* DOI: 10.1080/14616696.2020.1804973

Cabinet Office & DCMS (2020), Digital Identity Call for Evidence Response. Consultation Outcome.

Cannizzaro S, et al (2020), Trust in the smart home: Findings from a nationally representative survey in the UK. *PLoS ONE* 15 (5).

Carers UK (2019), State of Caring: A snapshot of unpaid care in the UK.

Carmi, E et al (2020), Data citizenship: Rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Review*, (9; 1-22).

Carnegie UK Trust (2020), Submission of evidence to the Home Affairs Select Committee call for evidence on online harms.

Carnegie UK Trust (2020b), Learning from lockdown: 12 steps to eliminate digital exclusion.

Carnegie UK Trust (2018), Online Data Privacy from Attitudes to Action. With Ipsos Mori.

CDEI (2020a), AI Barometer Report June 2020. Centre for Data Ethics and Innovation.

CDEI (2020b), Addressing trust in public sector data use. Centre for Data Ethics and Innovation.

CDEI (2020c), Review of online targeting. Centre for Data Ethics and Innovation.

Chadwick A & Vaccari C (2019), News sharing on UK social media. Online Civic Culture Centre, University of Loughborough.

CMA (2019), Consumer vulnerability: Challenges and potential solutions. Competition and Markets Authority.

Costa, E & Halpern, D (2018), The behavioural science of online harm and manipulation, and what to do about it. Behavioural Insights Team.

Davidson, J et al (2019), Adult Online Hate, Harassment and Abuse: a rapid evidence assessment. UK Council for Internet Safety.

DCMS, BEIS & Rt. Hon Caroline Dinenage MP (2020), £29 million government funding to boost digital revolution and help keep people safe online.

DCMS & Home Office (2020), Online Harms White Paper. Initial consultation response.

DCMS & Home Office (2019), Online Harms White Paper. Updated February 2020.

DCMS (2017), UK Digital Strategy 2017-20. Policy Paper.

DfE (2018), Essential Digital Skills Framework. Guidance. Updated 2019.

DCMS (2020), UK National Data Strategy. Policy Paper.

DCMS & Rt. Hon. Oliver Dowden MP (2020), Digital Secretary's closing speech to the UK Tech Cluster Group.

DCMS Select Committee (2019), Disinformation and 'fake news': Final report. House of Commons.

Deloitte (2020), Digital Consumer Trends 2020: Changing attitudes to data privacy.

Demos (2020), Online Harms: A snapshot of public opinion. Supported by BT.

Demos (2019), Protected by design: new fraud protections for people at risk.

Digital Schoolhouse (2020), Online safety: A parent's perspective.

Doteveryone (2020), People, Power and Technology: The 2020 Digital Attitudes Report.

Doteveryone (2020b), Better redress for the digital age.

Doteveryone (2019), Better redress: Building accountability for the digital age.

Doteveryone (2018), People, Power and Technology: The 2020 Digital Understanding Report.

Duffy, B & Allington, D (2020), Covid conspiracies and confusions. The Policy Institute / King's College London / Ipsos.

El Asam, A & Katz A (2018), Vulnerable young people and their experience of online risks. *Human–Computer Interaction*, 33 (4; 281-304).

Epilepsy Society (2019), Safeguard people with photosensitivity online. Epilepsy Society.

FCA (2020a), Guidance Consultation and Feedback Statement about Guidance for firms on the fair treatment of vulnerable customers. Financial Conduct Authority.

FCA (2020b), Financial Lives: The experiences of vulnerable consumers. Financial Conduct Authority.

Glitch (2020), The Ripple Effect: Covid-19 and the Epidemic of Online Abuse. With End Violence Against Women coalition.

Glitch (2020b), Digital Citizenship: Our definition.

Good Things (2020a), UK Digital Nation 2020. Infographic and explainer with sources.

Good Things (2020b), A Blueprint for a 100% Digitally Included UK.

Good Things (2020c), Covid-19 Response Report.

Good Things (2020d), Dementia and digital participation: Supporting carers and people living with dementia.

Good Things (2020e), Digital inclusion in health and care: Lessons learned from the NHS Widening Digital Participation programme (2017-2020).

Good Things & BT (2019), Digital Motivation: Exploring the reasons people are offline.

Good Things & Centre for Ageing Better (2018), I am connected: new approaches to supporting people in later life online.

Good Things & HMCTS (2020), HMCTS Digital Support Service Implementation Review.

Good Things (2018), Helping vulnerable people stay safe online: evaluation report.

Holmes, H & Burgess, G (2020), 'Pay the WiFi or feed the children'. University of Cambridge.

Home Office (2019), The scale and nature of fraud: A review of the evidence.

Hope not Hate (2020), A Better Web: Regulating to reduce far-right hate online.

ICO (2019), Adtech Market Research Report. Information Commissioner's Office with Ofcom. Research conducted by Harris Interactive.

Kennedy, H et al (2020), Public understanding and perceptions of data practices: a review of existing research. Living with Data / University of Sheffield / Nuffield Foundation.

Livingstone, S et al (2018), What do parents think, and do, about their children's online privacy?

Livingstone, S et al (2017), Children's Online Activities, Risks and Safety: A literature review by the UKCCIS Evidence Group. London School of Economics.

Lloyds Bank (2020), Lloyds Bank UK Consumer Digital Index 2020 Report.

Lloyds Bank (2019), Lloyds Bank UK Consumer Digital Index 2019 Report.

LSE Commission on Truth, Trust and Technology (2018), Tackling the information crisis. London School of Economics.

Mistry, P (2020), It is time to put trust, transparency and fair value at the centre of digital health and care. The King's Fund.

Money and Mental Health Policy Institute (2020), Submission of evidence to the Home Affairs Select Committee call for evidence on online harms.

Mozilla Foundation (2019), Internet Health Report 2019.

Nesta (2020), Dinner or Data: What is data poverty and why don't we know more about it.

Nominet (2019), Digital Futures: Security Report. Based on a survey sample of 2,080 UK adults including 505 aged 18–24 and 1,032 UK children aged 11–17, between 30.01.19- 06.02.19.

Ofcom (2020a), Adults' Media Use and Attitudes 2020 Report and Data.

Ofcom (2020b), Online Nation 2020 Report.

Ofcom (2020c), Adults' Media Lives Wave 15: A report for Ofcom 2020. Research conducted by Knowledge Agency.

Ofcom (2020d), Covid-19 News and Information: Consumption and attitudes surveys.

Ofcom (2020e), Results by ethnicity (Combined Waves 1-4) of Covid-19 News and Information: Consumption and attitudes.

Ofcom (2019), Adults' Media Use and Attitudes 2019 Report and Data.

Ofcom/ICO (2019), Internet users' online experiences and attitudes: Qualitative research summary. Ofcom and Information Commissioner's Office. Research conducted by Ipsos.

Ofcom/ICO (2020), Internet users' experience of potential online harms: summary of survey research. Ofcom and Information Commissioner's Office. Research conducted by Jigsaw Research.

Office of the e-Safety Commissioner (2019), Encouraging the digital participation of older Australians through mentoring

Office of the e-Safety Commissioner (2020), Building Australian adults' confidence and resilience online.

Ofqual (2020), Essential Digital Skills qualifications: progress so far. Guidance.

Older People's Commissioner for Wales (2020), Leave No-one Behind: Action for an age-friendly recovery.

One Digital (2019), Online Safety and Privacy.

ONS (2020), Internet access - households and individuals Great Britain.

ONS (2019), Internet access - households and individuals Great Britain.

Scottish Government (2020), Renewing Scotland's full potential in a digital world: consultation.

Smahel, D et al (2020), EU Kids Online 2020: Survey results from 19 countries.

Tambini, D (2019), Three ways the government can supercharge media literacy policy in the UK. London School of Economics.

Kelly, A (2020), Digital divide 'isolates and endangers millions of UK's poorest', The Guardian 28 April 2020.

UK Council for Internet Safety (2019), Digital Resilience Framework. Updated 2020.

UK Finance (2020a), Fraud: The Facts.

UK Finance (2020b), Eight in ten Brits would be embarrassed to admit they fell for a scam. Survey conducted by GingerComms with 1,510 British adults online between 2nd – 4th March 2020.

UK Finance (2019), Online Harms White Paper - UK Finance Response.

UKRN (2020a), The challenge of identifying vulnerability: a literature review. Research conducted by Britain Thinks for UK Regulators Network.

UKRN (2020b), Tips for identifying consumers in vulnerable circumstances. Britain Thinks for UKRN.

Understanding Patient Data (2017), Nicola Perrin: Understanding Patient Data. Video and transcript for The Kings' Fund Digital Health and Care Congress 2017.

Vidgen, B et al (2019), How much online abuse is there? A systematic review of evidence for the UK. The Alan Turing Institute.

Welsh Government (2020), Digital Strategy for Wales - Setting the context. Post by Lee Waters MS, Deputy Minister for Economy and Transport on 1 December 2020.

Woods, L & Perrin, W (2020), Online Harms - Interlocking Regulation. Carnegie UK Trust.

Woods, L & Perrin, W (2019), Online harm reduction: a statutory duty of care and regulator. Carnegie UK Trust.

World Wide Web Foundation (2020), Covid-19 Policy Brief: Misinformation & Freedom of Expression.

Yates, S et al (2020a), Who are the limited users of digital systems and media? A review of UK evidence. *First Monday*, **25** (7).

Yates, S et al (2020b), Understanding citizens' data literacies: thinking, doing and participating with our data. Me & My Big Data / University of Liverpool / Nuffield Foundation.

Annex: Initiatives and Resources

The following list is indicative of the practice landscape in relation to online safety, with a focus on resources for adults rather than children and young people.

Frameworks, for example:

- Essential Digital Skills framework (DfE and DCMS)
- Digital Resilience framework (UK Council for Internet Safety)
- Digital Understanding framework (Doteveryone)
- Data Citizenship model (University of Liverpool - Me and My Big Data)
- Digital Citizenship definition (Glitch)
- 5Rights framework (5Rights Foundation)

Research centres and forums

- Ada Lovelace Institute uses research and deliberation to ensure data and AI work for people and society, and to promote informed public understanding.
- Centre for Data Ethics and Innovation independent body set up by the government to advise on how to enable and ensure ethical, safe and innovative uses of data, including for AI.
- Joint Fraud Taskforce: Set up in 2016 to reduce the level of fraud, and the harm it causes.
- Living with Data: University of Sheffield with Nuffield Foundation to inform public sector stakeholders with a view to improving their data practices and policies.
- Making Sense of Media Network is convened by Ofcom to improve media literacy in the UK.
- Me and My Big Data: University of Liverpool with Nuffield Foundation to understand levels and variations in UK citizens' understanding of their personal data.
- National Cyber Security Centre: The UK's independent authority on cyber security. Also provides support and resources.
- National Research Centre on Privacy, Harm Reduction and Adversarial Influence online: To develop measures to empower individual citizens regarding their privacy and online safety.
- SafetyTech Network: A new UK innovation network dedicated to the promotion, collaboration and the industrial application of online safety technologies in the UK.
- UK Council for Internet Safety (UKCIS) - a forum bringing together government, regulators, industry, law enforcement, academia and charities to keep children safe online. UKRI funded research centres, including Centre for Digital Citizens and Horizon Institute.
- Understanding Patient Data uses research, public and stakeholder engagement to improve understanding and practice around health and care data.

Organisations focused on online safety

- 5Rights Foundation: Focused on children's and young people's rights online.
- Action Fraud: The UK's national reporting centre for fraud and cybercrime.
- Center for Countering Digital Hate: Targets hate groups, extremist sites, and fake news online and organises "analysis and active disruption" of hate groups
- Center for Humane Technology: A US nonprofit organisation aiming to realign technology with the best interests of humans.

- Cybersmile Foundation: A nonprofit organisation committed to digital wellbeing and tackling all forms of bullying and abuse online.
- Get Safe Online: A source of factual and easy-to-understand information on online safety.
- Glitch: A UK charity working towards ending online abuse through digital citizenship.
- Internet Matters: A not-for-profit organisation supported by major telecoms companies (BT, Sky, EE, Huawei, Virgin and TalkTalk) to work collaboratively across industry, government and with schools to reach UK families with tools, tips and resources.
- Internet Watch Foundation: A UK charity working to minimise online sexual abuse content.
- NewsGuard: Launched in the US by journalists to tackle the problem of disinformation on the site's ownership, financing, content, credibility, transparency and history.
- Web Foundation: A US-based international non-profit organisation advocating for a free and open web for everyone, responsible for Contract for the Web - a global plan of action to make the online world safe and empowering for everyone.

Campaigns

- Don't be fooled Campaign: A Cifas and UK Finance campaign aimed at informing students and young people about the risks of giving out their bank details, and deter them from becoming money mules.
- Friends Against Scams (National Trading Standards) A National Trading Standards Scams Team initiative which aims to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams.
- Get Online Week Annual campaign week for digital inclusion run by Good Things Foundation each October.
- Nobody in the Dark: A coalition campaign and landing page led by Mastercard, Good Things Foundation, CleanSlate, APLE Collective and JRF on digital financial inclusion, signposting to online safety courses and money support.
- Safer Internet Day Safer Internet Day takes place in February every year, and it's mission is 'Together for a better internet'. The campaign began in the UK, but now takes place across Europe, and works with a broad range of partners including Facebook, Twitter. The campaign mainly focussed on safety for children of school age, and works extensively with schools to promote safer internet use.
- Scams Awareness: A yearly campaign run by Citizens Advice which aims to create a network of confident, alert consumers who know what to do when they see a scam. Citizens Advice runs the Scams Awareness campaign in close collaboration with the Consumer Protection Partnership. This brings together key partners in the consumer landscape to identify, prioritise and coordinate collective action to tackle detriment. Partners include BEIS.
- Take Five Stop Fraud: A national campaign that offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud, led by UK Finance. Their online quiz is based on a range of current scams: https://quiz.takefive-stopfraud.org.uk/

Online resources and advice

Regulators and public sector, for example:

- National Cyber Security Centre is the UK's independent authority and provides support and resources for individuals and families, as well as for businesses, public sector and others.
- Ofcom's advice for consumers contains information on a range of topics concerning online safety and security, from managing broadband security to parental controls. The website also has content on recognising scams related to telecommunications, and a Covid-19 resource section to help people navigate news and information on Covid-19.

- The Information Commissioner's Office has a range of online resources, such as Your data matters, to inform and protect individuals and organisations and businesses with regard to personal data privacy and protection.
- The Financial Conduct Authority provides online resources and advice on how to protect yourself from scams.
- Government Communications Service provides a toolkit - RESIST - for government and public sector communications professionals to limit the spread of disinformation.
- Welsh Government: HWB is an online one-stop shop which includes dedicated resources on children's online safety for parents, governors, teachers and other professionals.

Private sector, for example:

- Accenture's Futurelearn website has courses on fact checking in the media, fraud, digital citizenship, data literacy, cybersecurity; many courses require a higher level of literacy.
- BT Skills for Tomorrow is a dedicated initiative to build digital skills and confidence. BT also has webpages on specific topics such as email security/scams in relation to their consumer products, and through their subsidiaries and divisions: EE, Openreach, and PlusNet.
- Barclays has an interactive quiz on digital safety and their Digital Eagles programme which includes e-learning content on "Staying Safe Online"
- Lloyds Bank has a dedicated web page on How to Protect Yourself from fraud and includes analysis around online safety in its annual Consumer Digital Index reports.
- Which? has a variety of advice guidance resources in the area of scams and online safety including: a sign-up to scam alerts, rating banks on online banking safety, and a guide on scams and older people.

Voluntary sector, for example:

- Ability.Net has a range of online safety resources for those with disability and/or impairments. Including: Internet Scams and how to avoid them.
- Age UK has a range of online safety resources for older people and those supporting them, including: Making the most of the internet; Staying safe online tips; and Avoiding scams.
- Alzheimer's Society has online safety resources for people with dementia and carers including: Advice on coronavirus and scams and dementia friendly postcards.
- CHANGE has developed a keeping safe online resource for people with learning disabilities.
- Full Fact is a charity that campaigns for and undertakes independent fact-checking.
- Good Things Foundation is a digital inclusion charity which supports a free-to-join UK-wide network of community organisations (online centres network). Online safety resources include content on Learn My Way for people with no or low digital skills and Make it Click for people with limited digital skills. Also resources to support digital inclusion practice, such as online safety with people with learning disabilities; low income families; and older people.
- Internet Matters has a range of resources for adults to support and protect children's online safety in their online safety and resources section.
- Mind has a dedicated section on staying safe online in the context of the benefits and challenges of being online for mental health.
- NSPCC has a range of resources aimed at parents, carers, teachers and other professionals around children's internet safety and more resources on their NSPCC learning site.

- One Digital programme - a partnership of Age UK, Citizens Online, Clarion Futures (part of Clarion Housing Group), Digital Unite and Scottish Council of Voluntary Organisations (SCVO) - has a range of resources on their website's online safety and privacy section.

- ParentZone provides online support and learning resources for parents as well as children and schools around online safety, including a series of parent-focused guides.

- SCVO - the Scottish Council for Voluntary Organisations - has resources and initiatives around digital, including guides for charities to think through digital safety responsibilities.

- Wales Cooperative Centre's Digital Communities Wales website includes a padlet of resources relevant to online safety during Covid-19.

For more information about the project, contact Good Things Foundation on:

e: research@goodthingsfoundation.org
t: 0114 3491619

Good Things Foundation