pluminsight

April 2023 | plumconsulting.co.uk

Trust and confidence in digital services

Chris Taylor Johnathan Charles

Digital services are already a central feature of our everyday lives. However, we may be just at the start of a journey on which more and more transactions and experiences will migrate from the physical to the digital world. Development of digital services in the coming decade has the potential to deliver innovative use cases of great benefit in important sectors like healthcare and education, as well as further transforming media and entertainment.

Adoption of new technology and engagement with digital services is not homogenous. Digital engagement can be constrained by a number of factors, including lack of infrastructure or poor quality connectivity, low digital skills, and low trust and confidence arising from concerns about online harms. In this paper, we look at the latter of these factors, and explain how new legislation and regulatory reforms present important opportunities to tackle barriers to confidence and trust.

Confidence to use digital services

Evidence shows that, whilst the digital economy continues to grow and deliver benefits, exposure to online harms, or fear of them, may affect trust and confidence in digital services, creating an impediment to engagement and take up.

It is important to give this the right context. Research has found that most people are generally comfortable online and confident that they can identify and navigate away from harmful material.[1] However, there is evidence that a significant proportion of users have been exposed to or experienced online harms,[2] and that people have reported high level of concerns about this.[3] A number of studies have identified areas on which people feel uneasy or distrust some digital services.[4] [5]

Risks to consumers and citizens in the digital world should not be seen as static. Just as the online ecosystem evolves and the benefits it brings change, so will risks of harm, and perceptions of this. Data from the UK Office of National Statistics (ONS) demonstrate this. These data show that, between 2009 and 2019 (the latest year for which data is available), the steepest rise in reasons for not being online in Great Britain was privacy or security concerns.

Figure 1: Percentage of households in Great Britain which do not have Internet access by reason given

	2010	2019
Don't need Internet	39	61
Lack of skills	21	34
Privacy or security concerns	4	33
Access costs too high	15	29
Equipment costs too high	18	28
Other reason	13	25
Have access to the Internet elsewhere	8	16

Source: ONS

What are online harms?

In the digital world, as in any setting where large numbers of people meet and transact, things can go wrong. Causes can be legal (e.g. exposure of individuals to content which they find distressing or addictive) or illegal (e.g. fraud, or misuse of personal data). Most of these harms are not unique to digital environments, but they have found new manifestations there.

[1] Ofcom research found that 69% of users are confident about their ability to stay safe online - https://www.ofcom.org.uk/__data/assets/pdf_file/0025/244168/online-experiences-tracker-waves-1-and-2-summary-report.pdf

[2] Ofcom's Online Nations Report 2022 reported that 63% of users have been exposed to at least one potential harm online in the last four weeks - https://www.ofcom.org.uk/__data/assets/pdf_file/0023/238361/online-nation-2022-report.pdf

[3] Doteveryone 2020 research included findings that 84% of people are concerned about children accessing inappropriate content, and 83% are concerned about online scams https://doteveryone.org.uk/wp-content/uploads/2020/05/PPT-2020_Soft-Copy.pdf.

[4] For example, research for the Aviva Fraud Report 2021 found that 53% of Internet users do not trust advertisements on search engines - https://static.aviva.io/content/dam/aviva-corporate/documents/newsroom/pdfs/reports/Aviva_Fraud_Report_2021.pdf

[5] For example, research by The Centre for International Governance Innovation (CIGI), UNCTAD and Internet Society reports a variety of factors which affect trust - https://unctad.org/press-material/jointly-released-cigi-ipsos-internet-society-and-unctad

Problems may arise which are particular to online experiences, both as a result of the ease with which individuals can access material from any location at any time, and the amount of time they spend online.[6] It follows that, as the reach and importance of the digital world grows, so does the potential for harm there. Harms may arise individually or cumulatively (e.g. increased exposure to other risks can be a consequence of online addiction).

Figure 2: Examples of online harms

Example 1: Harmful content
Harmful content encompasses a very broad scope of possible problems, including illegal material (e.g. incitement to violence), legal but harmful material (e.g. content which might give rise to eating disorders), targeting of individuals (e.g. cyber-bullying, trolling, cyber-stalking, harassment), and misinformation (e.g. "fake news").

Example 2: Risks to health
For some individuals, online services can risk exposure to material or behaviours which become addictive, or can exacerbate pre-existing health risks. For example, addictions to gambling or pornography where online channels also raise risks of age inappropriate behaviour. Excessive screentime can lead to addictive behaviour in relation to social media or other online facilities.

Example 3: Fraud and scams
Scammers have used online channels to target misleading or false information (e.g. fake reviews), including to particularly vulnerable groups. This can include investment or pensions fraud.

Example 4: Dark patterns
Presentation of information which manipulate consumers into making a choice which favours the content provider, e.g. messages telling consumers that there is limited stock of an item and/or it is in high demand.

Example 5: Unfair price discrimination
Data on individual preferences or behaviours can enable higher prices for goods and services to be targeted unfairly based on factors like location and browsing history.

Benefits of digital services and digital engagement

Overall, digital services deliver private benefits to individuals, and public benefits to us all. Some examples of this are presented in Figure 3.

Figure 3: Examples of private and public benefits of digital services

Service type	Type of benefit	Examples of benefits
Digital healthcare	Private	Easier and quicker access to services, including 24/7
	Public	Improved outcomes for public health, education, and employment Lower cost of delivery
Digital education	Private	Distance learning Learn at your own pace Learn when you like, 24/7 access
	Public	Improved outcomes for public health, education, and employment Lower cost of delivery
AI	Private	Faster and cheaper access to some services and facilities More reliable results for some interactions
	Public	Improving reliability and accuracy for some public services, e.g. road traffic management Lower cost of delivery

Factors that reduce engagement dilute benefits. Improving engagement through proportionate and targeted interventions can therefore benefit everyone.[7]

The opportunity to address harms and build trust and confidence

It is in the interests of all stakeholders to improve the digital landscape by addressing online harms.

2023 and 2024 will be landmark years for regulation of digital services. Globally, the United Nations has a programme of work on digital development, and is preparing for its Summit of the Future in 2024 which includes digital engagement as an area of potential action.[8]

Meanwhile, reform is underway or in plan in a number of jurisdictions, including:

[6] Ofcom's Online Nations Report 2022 reported that UK adults spent on average 4 hours a day online - https://www.ofcom.org.uk/__data/assets/pdf_file/0023/238361/online-nation-2022-report.pdf

[7] To illustrate, in an article for the IIC, Sam Wood of Plum carried out analysis that indicated the benefits of online harms regulation could significantly outweigh the costs - https://www.iicom.org/wp-content/uploads/IM-June-2021-Vol-49-Issue-2-Economics-Of-Online-Harms-Regs.pdf

[8] https://www.un.org/en/common-agenda/summit-of-the-future

- Across the EU through the Digital Services Act,[9] Digital Markets Act,[10] and Artificial Intelligence Act.[11]
- In the UK, the Online Safety Bill[12] is progressing through Parliament, and the Government has said it will introduce the Digital Markets Consumer and Competition Bill in 2023.[13] The Competition and Markets Authority (CMA) has established a Digital Markets Unit to expand its capability and capacity to regulate digital markets, and in July 2022, issued a joint statement with Ofcom on the approach to regulation of online safety and competition.[14]
- The Australian Competition and Consumer Commission (ACCC) is undertaking a major review of markets for digital services and platforms.[15]

Developing regulation to address online harms is breaking new ground in an environment where regulation has been light up until now (for example, compared to regulation of broadcast content or telecommunications services). Hence, there is a need for innovative thinking by policy makers to strike an appropriate balance between effective safeguarding of consumers and competition, and the benefits of innovation in the provision of online services which regulatory failure could constrain. Simple transference of regulatory methods from other regulatory sectors to the digital economy is unlikely to be effective, and may be damaging.

Policy makers will find it helpful to consider the following points as they build regulatory frameworks for digital services:

- Common measures and approaches to effectively and proportionately address harms. This might include:
  - clear identification and codification of harmful content giving examples of material which is illegal, and that which is legal but may be harmful to groups or individuals;
  - measures for effective prevention, detection and enforcement against harms;
  - effective, transparent, and navigable systems for consumer redress when things go wrong and/or consumers are dissatisfied,[16] including independent sources of help and advice where there are disputes between a consumer and their provider;
  - clear and straightforward measures to ensure children are not exposed to age-inappropriate content;
  - information and support for consumer self-help in protecting themselves and their families from harmful content; and
  - targeted measures to reach and support individuals with low digital skills, particularly those who are isolated without access to help.
- Consumer protection in digital markets should be coordinated with other aspects of regulation, e.g. measures to safeguard fair competition, and the prevention of harmful advertising, so that the regulatory framework is coherent and holistic.
- Measuring and tracking of outcomes, identifying risks of harm as well as benefits.
- Future proofing through analysis of changes to the consumer experience as digital markets evolve and new services emerge, and flexibility for protections to adapt to new sources of harm.

A need for international coordination

Digital markets are rarely constrained geographically, and online harms do not stop at national borders. Therefore there is a need for national authorities to cooperate between jurisdictions to address international or global harms.

Inter-agency dialogue and sharing of information between jurisdictions can help in developing effective regulatory measures. Regulation is not consistent between countries, and regulatory capacity is uneven. For example, the United Nations reports that 80% of developed countries in Europe have laws for online consumer protection, compared to 41% of least developed countries (LDCs).[17] This does not mean that regulation should be identical in all countries, especially in the area of content which may have unique characteristics in a country, or be culturally significant in some countries whilst not in others. However, benefit can be gained from learning from each-other, including sharing of research and analysis, knowledge transfer, and capacity building between countries.

[9] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

[10] https://competition-policy.ec.europa.eu/dma_en

[11] https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

[12] https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill#types-of-content-that-will-be-tackled

[13] https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets/outcome/a-new-pro-competition-regime-for-digital-markets-government-response-to-consultation

[14] https://www.gov.uk/government/publications/cma-ofcom-joint-statement-on-online-safety-and-competition/online-safety-and-competition-in-digital-markets-a-joint-statement-between-the-cma-and-ofcom#foreword

[15] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25

[16] Research by doteveryone found that people do not have access to adequate redress, and doteveryone have made recommendations to rectify this - https://doteveryone.org.uk/wp-content/uploads/2020/05/Better-Redress-for-the-Digital-Age.pdf

[17] https://unctad.org/news/least-developed-countries-still-lag-behind-cyberlaw-reforms