TOP10VPN | OPEN RIGHTS GROUP

April 2019

Collateral Damage in the War Against Online Harms

How charities, schools, and social support websites are blocked by UK ISP adult content filters

Open Rights Group

Jim Killock
Pamela Cowburn
Alex Haydock
Ed Johnson-Williams

Top10VPN

Simon Migliano

Table of Contents

Key findings 1

- Scale of errors
- What gets blocked
- Evidence from errors reported to us
- Complaints made through Blocked.org.uk 2
- ISP responses
- Appeals and errors

Introduction: Why are websites being blocked in the UK? 3

PART ONE: The policy context 5

- What problem are content filters trying to solve?
- Assessing the harms of adult content 8
- Filters as a solution 9
  - Mobile Networks 10
  - Fixed-Line ISPs 11
  - Take up of ISP filters 12
- Do filters prevent children from seeing harmful content? 13
- Harms of overblocking 16
  - Young people and other household members
  - Harms of overblocking for businesses 17
  - Harms of overblocking for free speech 18
  - Other harms caused by filters 19
- The legal basis for content filtering 20
- Error correction 23

PART TWO: Understanding our Blocked.org.uk data 24

- Background to Blocked.org.uk
- Aims of this research 25
- Research methodology 26
  - User reports
  - Search 27
  - Interviews
  - ISP response statistics
- Reports submitted via Blocked.org.uk
  - Examples of Incorrectly Blocked Sites 28
    - Beam - Helping the Homeless
    - CARIS Islington - Bereavement Counselling and Cold Weather Night Shelter
    - Welcome Church

Error rates and numbers of likely mistakes 30

PART THREE: Research Findings 31

Problematic categories of blocks

Table A - Keyword list categories 33

Table A.2 Verified search results, UK sites only

Table A.3 Unverified search results 34

Table A.4 Unverified search results, .uk domains only

Content misclassification 35

Domestic violence and sexual abuse support networks

School websites 36

LGBTQ+ sites

Counselling, support, and mental health sites 37

Wedding sites 38

Drain unblocking services 39

Photographers

Builders, building supplies and concrete

Religious sites 40

Charities and non-profit organisations

Alcohol-related (non-sales) sites

The “Scunthorpe Problem” 41

Blocks which cause damage at a technical level 42

CDNs, APIs, and image hosting services

Technical back-end sites 43

Pre-launch site blocking 44

Overbroad blocking categories 45

Products already subject to age restrictions

Cannabidiol products blocked as drugs 47

Commercial VPN services

VPN and remote access software 48

Blocks are not being adequately maintained 49

Unblock request findings

Replies to unblock requests

Sources of unblock requests 54

Damage cited by Blocked.org.uk users 57

Mobile network inconsistencies 58

Complaints and appeals 59

BBFC appeals process

Site owners are not accessing the appeals process 60

Lack of appeals process for fixed-line ISPs 61

Unclear replies from ISPs

The future of web filters 62
Filters may get broader, less effective and less transparent
Filters can have low rates of error correction 63
Filters are poor products with little incentive to improve

Conclusion 65
Recommendations 66

Appendix A - Raw Data 69
Table A - Keyword list categories
Table A.1 Verified search results
Table A.2 Verified search results, UK sites only 70
Table A.3 Unverified search results
Table A.4 Unverified search results, .uk domains only 71
Table B - Unblock request categories
Table C - Unblock requests categorised by user affiliation 75
Table D - Breakdown of damage alleged by users submitting unblock requests
Table E - Unblock requests forwarded to each ISP 76
Table F - ISP reply statistics (aggregate) 77
Table G - ISP reply statistics (per-ISP)
Table H - Mobile network blocking inconsistencies 82

Appendix B - Methodology for reporting statistics 83
General
ISP reply information
ISP performance statistics
Categorisation of site, sender and damage types 84
Blocked versus unblocked sites
Filtering on ISP lines
What we have tested
What counts as a 'site' 85
Searches and lists of potential errors

Appendix C - Technical challenges from filtering products 86

Appendix D - Bibliography 88

Key findings

The research in this document looked at the 1881 unblock requests which have been made through our Blocked.org.uk tool since 2017[1]. The tool helps people ask Internet Service Providers (ISPs) to remove wrongfully-included websites from their adult content filters. As part of the Blocked project, since 2014 we have indexed over 35,000,000 websites, creating a database of over 760,000 blocked websites, allowing users of the site to search and check domains which they feel may be blocked[2].

Scale of errors

1. While ISPs and the Government have downplayed the significance of errors, we have seen over 1,300 successful complaints forwarded to ISPs about incorrectly blocked domains.[3]
2. Further analysis of the blocked domains in our database suggests that this is only a fraction of the errors present. For instance, while we have only received 122 requests to unblock counselling and mental health websites, a simple keyword search of the database shows over 112 more that may still be wrongfully blocked.[4]

What gets blocked

1. There is a great deal of useful and important material that is being blocked. Even on ISPs estimations, thousands of errors are made.
2. Some blocking is difficult to understand: over 1,700 wedding services' sites may be incorrectly blocked as of the time of writing, and over 730 sites relating to photography.[5]
3. Many local pubs' websites are blocked, yet other bars or restaurants do not necessarily get blocked.
4. A set of simple searches returns thousands of blocked sites that urgently need review. We believe many more errors can be found.

Evidence from errors reported to us

1. 98 reported sites for counselling, support, and mental health services have been unblocked.[6]

---

[1] *See: Table F*
[2] *See headline figures on https://www.blocked.org.uk ; see Appendix B for testing data sources.*
[3] *See: Table F*
[4] *See: Table A and Table B*
[5] *See: Table A*
[6] *See: Table B*

2. Over 55 charities or non-profit organisations have had their websites unblocked through our tool.[7]
3. At least 59 sites dedicated to domestic violence or sexual abuse support have been blocked over the lifetime of the Blocked tool. 14 of these are still blocked.[8]
4. LGBTQ+ community sites are often incorrectly blocked, with users having reported 40 though the Blocked site.[9]

Complaints made through Blocked.org.uk

1. An increasing number of complaints are made by site owners and users. In 2018, we saw more than 25% of unblock requests coming directly from site owners or users.[10]
2. Site owners often complain about wrongful blocks causing business damage and reputational issues.[11]

ISP responses

1. While some ISPs respond to complaints reasonably quickly, others are slow. The average was 8 days in 2018. Vodafone took 21 days on average to respond to our requests. Virgin Media and Three took 11 days.
2. A significant proportion of requests go missing. In 2018, 294 of 1,072 reports to networks went missing, or 27%, of which we believe 153 (15%) should have resulted in a URL being unblocked.[12]
3. ISPs often do not reply to complaints, even when they do remove the block.

Appeals and errors

1. Only mobile networks offer appeals. However these are seldom used.
2. Mobile networks do not properly apply policy changes from the British Board for Film Classification (BBFC) rulings. The BBFC made it clear the VPN providers should not be blocked, yet we have identified around 300 VPN-related websites that are blocked and need review, and requests from VPN providers are not usually resolved favourably without a further appeal to BBFC.[13]
3. For fixed networks, no appeal is possible. Within our complaints, we believe at least 39 reclassification errors were made by ISPs after unblock requests were submitted.

---

[7] *See: Table B*
[8] *See: Table A*
[9] *See: Table B*
[10] *See: Fig. 6*
[11] *See: Fig. 9*
[12] *See: Fig. 3*
[13] *See: Table A*

Introduction: Why are websites being blocked in the UK?

Since 2011, ISPs in the United Kingdom have applied filters to Internet connections in an effort to block children and young persons from accessing websites which host content considered inappropriate. This push was informally backed by the Government, who wanted to show that the UK was at the forefront of protecting children from online content. In 2013, the then Prime Minister David Cameron declared: "I want to talk about the Internet, the impact it's having on the innocence of our children, how online pornography is corroding childhood and how, in the darkest corners of the internet, there are things going on that are a direct danger to our children and that must be stamped out." [14]

In the same speech, Cameron announced that the four main ISPs in the UK; TalkTalk, Virgin Media, Sky and BT, had agreed to install 'family friendly' content filters and to promote them to their existing and new customers.

A previous report by Open Rights Group (ORG) had shown that there were serious problems with filtering by mobile phone companies, which were incorrectly blocking many websites.[15] We suspected, correctly, that there would be similar issues with network level filtering by broadband ISPs.

Overblocking has been dismissed as trivial, and ISPs cite low numbers of websites now reporting blocks. We would argue that this is not a sufficient measure of overblocking because the vast majority of website owners do not suspect that their site will be blocked. ORG's Blocked tool, created to identify blocked sites, gives a more accurate picture of the scale of the problem. UK websites are being incorrectly blocked in their thousands, and this includes sites that provide help and advice for young people and other household members. We have also found examples of significant under-blocking, where inappropriate content is not being blocked by filters.

There is no evidence that filters are preventing children from seeing adult content or keeping them safe online. They may be contributing to a lack of resilience that can increase risk to children.

Private companies are making questionable choices about what is and is not acceptable for under 18s, with no oversight or consideration of actual harms to young people.

Following the passing of an EU regulation on net neutrality, the position seems clear that Internet filtering by ISPs is prohibited. This is a regulation that was supported by the UK Government, in the full knowledge that it would have implications for ISP-level content restrictions, and the significant investments that the Government demanded from them.

---

[14] *UK Government. 'The Internet and Pornography: Prime Minister Calls for Action'. GOV.UK, 22 July 2013. https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action*

[15] *Open Rights Group. 'Mobile Internet Censorship: What's Happening and What We Can Do about It'. Open Rights Group, May 2012. https://www.openrightsgroup.org/about/reports/mobile-internet-censorship:-whats-happening-and-what-we-can-do-about-it*

In the short term, we would urge companies to ensure that customers are, at a minimum, being given the option to opt in to filtering, as well as sufficient information for this to be an informed choice. ISPs should move customers to independent, device level products that can be focused on a child's needs. Ofcom need to clarify the legal situation for UK network operators as the regulator responsible for the Internet access regulations.

As this report shows, filters are a flawed technical solution to a social problem. As with other areas of social policy, we would urge the Government to embrace a more long-term and holistic approach to promote lasting online safety.

This report looks at the impact of filters applied to prevent young people from seeing content that is believed to be unsuitable for under 18s. It looks at why filters were introduced, how they work and the kind of content they aim to block.

Using evidence from www.blocked.org.uk, a tool created by ORG and ORG supporters, we show evidence of over-blocking and under-blocking by filters. We look at the complaints process and error handling. In this report, we outline recommendations for greater transparency and consent with regard to filters, as well as other suggestions for keeping children safe online.

This report shows the dangers of poorly-designed policy, and of reliance on technology to police online content. The UK Government and the European Union continue to push technological solutions in this area, for instance in Article 13 of the Copyright Directive, the Terrorism Directive, and the UK's Internet Safety Strategy. However, technology has limits, and ultimately cannot substitute for human review. Furthermore, all systems cause errors. Error detection is often absent or limited, and it is left to individuals in these systems to report problems. Inevitably, mistakes are often not reported, and even when they are, they are not always resolved.

PART ONE: The policy context

What problem are content filters trying to solve?

The Internet has opened up new worlds to children, who now have unprecedented access to information and ideas, and the means to communicate them. While there are clearly huge benefits, using the Internet carries risks for children and young people, including accessing age inappropriate content. For a number of years, children and young people seeing pornography online has been a major concern for politicians, publications such as the Daily Mail and children's charities like the NSPCC.

Concerns around content range from young children being upset after accidentally being exposed to adult images, to worries that the excessive consumption of pornography is affecting how young people view sex and relationships. A 2016 report into sexual harassment and violence in schools by the House of Commons' Women and Equalities Committee said that, "Widespread access to pornography appears to be having a negative impact on children and young people's perceptions of sex, relationships and consent. There is evidence of a correlation between children's regular viewing of pornography and harmful behaviours."[16]

The media debate initially tended to focus on pornography[17], although there has been discussion about the harms caused by forums and websites that promote anorexia, self harm and, extremism. However, as we explain in more detail below, the adult content filters currently being applied in the UK by ISPs and mobile phone providers actually cover a much wider range of subjects, including alcohol, drugs, sex, religion, and politics. This is particularly problematic because filters are applied to adults as well as children, either as 'whole home' solutions provided by ISPs, or as 'default' filters on phones which require effort to remove.

Fears about the corrosive influence of certain types of content, whether music, film or games, have been discussed for years, both in the media and at a policy level. However, Internet saturation and the rise in the use of tablets and smartphones, means children can now access content to the exclusion of their parents or other adults in a way that was not previously possible. A Plymouth University report on peer education and online safety, notes: "Combine the feeling of exclusion with the Internet safety messages based on a risk-laden environment, and there surfaces an assumption that children are engaging in unsafe activities."[18]

According to the Internet Matters website: "Our … Pace of Change Research (2015) shows that 48% of parents

---

[16] *House of Commons Women and Equalities Committee. 'Sexual Harassment and Sexual Violence in Schools: Third Report of Session 2016-17'. House of Commons, 7 September 2016.* https://publications.parliament.uk/pa/cm201617/cmselect/cmwomeq/91/91.pdf, p.48, para.204

[17] *Sellgren, Katherine. 'Porn "Desensitising Young People"', 15 June 2016, sec. Education & Family.* https://www.bbc.com/news/education-36527681

[18] *Atkinson, Shirley, Steven Furnell, and Andy Phippen. Using Peer Education to Encourage Safe Online Behaviour, 2019.* https://www.researchgate.net/publication/237430450_Using_Peer_education_to_encourage_safe_online_behaviour

believe their children know more about the Internet than they do and, and 78% of children agree." This has undoubtedly contributed to sense of powerless and concern felt by parents, and to an extent MPs and the media. This has, in turn, shaped the debate and proposed solutions for keeping children safe online. A United Nations report into free expressions noted: "The limited understanding of children's use of the Internet frequently leads to the adoption of more restrictive approaches aimed at safeguarding children."[19] How we approach the issue of harmful content may change as digital natives become parents themselves.

Thanks in part to ORG's awareness raising, the Government accepted overblocking is a problem and initially set up a task force to deal with it. Originally an independent body, the task force was subsumed into the UK Council for Child Internet Safety (UKCCIS), which listed as one of its achievements "considering potential problems around overblocking". We observed little action, though, despite our attendance at most of their overblocking meetings.[20] The working group was specifically tasked with ensuring that:

> *ISPs develop and implement a single, centralised process for site owners to check the status of their site and report cases of suspected overblocking.*[21]

This resulted in a single email address being presented on Internet Matters, and made available only to website owners. The UKCCIS 'overblocking working group' reported at its conclusion in 2015 that:

> *To date, no webmasters have reported that the ISPs are overblocking their websites via Internet Matters, and a similar low level of activity is reflected in the data from the UK mobile operators (EE, O2, Three and Vodafone), which is published quarterly by the BBFC since September 2013 in conjunction with the Mobile Broadband Stakeholder Group.*[22]

This stands in contrast with the evidence in this report, of hundreds of complaints filed through our tools and thousands of likely misclassifications shown through our searches. We suspect the truth is that complaints via ISPs and Internet Matters are so low because:

- Many website owners do not know about filters and do not suspect that their sites are blocked. In our experience, charities are more aware of filters but many businesses, organisations and individuals have no idea that their website can be blocked.
- Many of the sites being blocked have low levels of traffic so the error may not be easily noticed.

---

[19] *United Nations General Assembly. 'Promotion and Protection of the Right to Freedom of Opinion and Expression', 21 August 2014. https://undocs.org/A/69/335., para.74*

[20] *UKCCIS has now been superseded by the UK Council for Internet Safety. Overblocking is not listed as among the Council's concerns.*

[21] *UKCCIS Overblocking Working Group. Final Report, 2015. https://www.whatdotheyknow.com/request/320569/response/791574/attach/3/280405%20Final%20Version%20UKCCIS%20Overblocking%20Working%20Group%20Final%20Report.pdf*

[22] *Ibid.*

- Many of the people who have got in touch with ORG found out by accident that their site was blocked.
- People do not understand the implications of being blocked – especially if their site is blocked on a network other than their own.
- Apart from the Blocked tool, there is no way of checking whether sites are blocked across all ISPs and mobile phone providers.
- If website owners discover their site is blocked, they may not know that they can challenge this decision or how they should go about it.

Harms resulting from blocks was also examined by the Group, particularly as content relevant to children such as advice sites might be blocked. The Overblocking Working Group agreed that "just … ChildLine and other emergency support for young people, including their individual forums" would be whitelisted to ensure children could find help. However, blocking of content relevant to children was not addressed, nor was the possible scale of blocking of help sites. We have found this to be a particular problem in our research.

Being blocked by adult content filters can also cause real problems for business owners or other people who make a living through the content on their sites. As we illustrate later in this report, overzealous web filtering can lead to businesses and website owners losing out on potential customers and revenue, as these potential customers find themselves unable to access the business website and instead take their business elsewhere.

Further, blocking sites belonging to legitimate businesses and groups has the knock-on effect of potentially causing lost sales, and may lead to potential site visitors trusting the judgment of the filtering systems and wrongly assuming that the site hosts unsavoury content.

The harm done to businesses and blocked sites by these filters is exacerbated by the fact that users are not always empowered to choose whether their filters are on or off. Filtering can always be toggled by users, however not all users are aware that filtering is enabled for them by default, or asked whether they want to enable it. This leads to a natural expansion of filtering to people who did not need or ask for it, such as those without children or who live only with children over 18.

These adult content filters can be disabled of course, but this does not counter the potential problems that they may cause. There are a multitude of reasons why Internet users may be unwilling or unable to disable adult content filtering:

- Users may not be the bill payer (shared household, public Wi-Fi, etc);
- Users with young children may wish to keep the filters enabled;
- Users of mobile networks may be unwilling to submit the required ID documents to disable the filters.

Wrongful blocks can be circumvented, but a business who is impacted by a block faces the loss of traffic to their site from people who do not have the time to work out how to bypass a block, turn off filtering, or simply from people who trust the filtering systems to be accurate who assume that if the filter blocks a site then it must be somehow problematic or malicious.

Assessing the harms of adult content

ORG campaigns to protect the right to privacy, free expression online and to challenge mass surveillance, it is not within our remit or expertise to assess the impact or potential harms of pornography or other adult content on children and young people. Our remit is to consider the impact of policies on the free speech and privacy of web users, including children, parents, and website owners.

However, we would urge that the policy debate around the harms caused by content:

- **Takes an evidence-based approach**

  Policies must be informed by independent research into the various strategies for keeping children safe online. Surveys of attitudes can reflect what parents and children think, or what they think society believes they ought to think, rather than being objective measures of harm. This does not mean that they are not of value, but their limits must be recognised and they should not be the sole driver of policy.

- **Is framed correctly**

  Filters do not just block pornography but a wide range of content, using broad categories such as alcohol, drugs, sex and extremism. It is important that this is recognised in any discussion of filters' impact on young people.

- **Includes young people's voices**

  While children are asked about their concerns and fears, they are rarely asked about the solutions. Dr Andy Phippen from Plymouth University told ORG,

  > *"I work a great deal with young people and what I am struck by is the majority of 'online safety' education is the prohibitive approach – don't do this, don't look at this, etc. What they tell me they need, rather than tools to stop them doing things (which they know don't work), are safe spaces and knowledgeable staff to allow them to discuss these issues in a sensible manner. We are never going to prevent access to pornography by determined teens, so they need to understand the impact of access and the wider cultural issues".*

- **Does not solely focus on risk**

  Many of the resources available to children, teachers and parents focus on the risks posed to children by the Internet and the exclusion of parents and other adults in being able to protect them from this.[23] Aside from the fact that it is impossible to wholly eliminate risk, technology-focused approaches to ensuring child safety online often fail to consider the potential risks they themselves may pose to children's rights. As part of a series of reports on "Children's Rights and Business in a Digital World", UNICEF highlighted that:

  > *"current public policy is increasingly driven by overemphasized, albeit real, risks faced by children online, with little consideration for potential negative impacts on children's rights to freedom of expression and access to information. The ICT sector, meanwhile, is regularly called on to reduce these risks, yet given little direction on how to ensure that children remain able to participate fully and actively in the digital world."* [24]

- **Does not focus solely on technology**

  We are supportive of the Government's 2017 commitment to introduce compulsory sex and relationships education (SRE) in schools. We feel that it is important for children to receive SRE which addresses topics such as pornography, relationships and online abuse. Children also need to be educated about how to stay safe online and what they can do if they encounter content that they might find disturbing or frightening.

- **Encourages active parenting**

  This may mean actively monitoring the use of young children and talking to older children about the dangers they might encounter online. Parents already do this on a daily basis – whether it is discussing the news in age-appropriate terms or educating their children about alcohol, drugs and sex. Promoting device-level filters rather than ISP-level filters may also help parents to take a more active role in their child's Internet use, and can assist parents to have more granular control over what their children are able to see online, rather than outsourcing such decisions to Internet Service Providers.

Filters as a solution

The 2010 coalition Government identified tackling 'the commercialisation and sexualisation of childhood' as one of its commitments.[25] The subsequent 2011 Bailey Review into the commercialisation and sexualisation

[23] *Phippen, Andy, and Henry Phippen. 'The UK Government Internet Safety Strategy – Time to Listen to the Youth Voice?' Entertainment Law Review 29, no. 8 (2018): 237–44.*

[24] *UNICEF. 'Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information, and Participation', June 2017. https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_EXPRESSION.pdf*

of childhood recommended that parents should be given an 'active choice' about applying filters when they bought a device or entered into a contract.[26] Bailey recommended that companies offer parental controls voluntarily, or if they failed to comply within a timescale, through regulation. In 2013, the coalition Government persuaded the UK's four largest Internet Service Providers (BT, TalkTalk, Sky, and Virgin Media) to fulfil this recommendation and make network-level filters available to their customers.

Network-level filters have been promoted as a simple way of preventing children from seeing adult content. Parents do not need any technical expertise to activate them. Former Prime Minister David Cameron said filters were intended to provide "One click to protect your whole home and to keep your children safe."[27] As this report will show, this simplistic view is misleading and potentially counterproductive.

Filters – whether applied at home or in schools – have now become central to government policies for children's safety online.

Mobile Networks

Mobile networks introduced 'opt-out' or 'default on' filters much earlier than fixed-line ISPs on the basis that it was hard to know who a mobile account was being used by. An industry Code of Practice in 2004 first established the general approach.[28] Mobile ISPs started to introduce opt-out filters from around 2011.[29]

One immediate limitation of filtering Internet access for children in this manner is that network-level filtering applied by a user's mobile ISP will only work when a user is using mobile data. If the user is connected to a WiFi network, any filtering will be done through that WiFi network rather than the mobile ISP.

Mobile phone filters are switched on by default by a number of providers, including EE, Telefonica (O2), Three and Vodafone. Mobile phone customers generally have to prove they are over 18 if they want to switch filters off. Some networks require the submission of identification documents, such as a passport, in order to allow the filters to be disabled.

Mobile phone providers use a framework from the BBFC to identify content that should be filtered. This means that all mobile phone providers should in theory be using the same criteria to decide whether sites are blocked, although data from the research we have conducted through our Blocked tool suggests that there

---

[25] *UK Government. 'The Coalition: Our Programme for Government', May 2010.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78977/coalition_programme_for_government.pdf

[26] *Bailey, Reg. 'Letting Children Be Children'. UK Government Department for Education, June 2011.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/175418/Bailey_Review.pdf, *p.38*

[27] *UK Government. 'The Internet and Pornography: Prime Minister Calls for Action'. GOV.UK, 22 July 2013.* https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action

[28] *Ofcom. 'UK Code of Practice for the Self-Regulation of New Forms of Content on Mobiles', 11 August 2008.* https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/ukcode

[29] *Geere, Duncan. 'O2 Installs 18+ Filter on the Mobile Web'. Wired UK, 4 March 2011.* https://www.wired.co.uk/article/o2-mobile-web-filtering

are is still some variation from provider to provider.

Site owners who think or realise that their site has been blocked incorrectly can appeal to the BBFC, who publish quarterly reports on the outcomes. There is a unified appeals process for websites filtered by mobile ISPs, and transparency about decisions. While it is not perfect, and is not a legal process, it is better than the previous arrangement which lacked independent means to deal with errors.

Fixed-Line ISPs

ISPs agreed to install filters on home broadband connections following private meetings with MPs and policy makers. Initially, the proposals were for ISPs to offer their customers an 'unavoidable choice'. ISPs would ask customers if they wanted filters, often blocking all other Internet access until a choice had been made.

Filtering on fixed-line ISPs began to roll out in 2014. Despite some concerns being raised that customers were not being given an informed choice, they did initially have an opportunity to decide whether to enable the filters. However, in December 2015, Sky announced that it would turn on filters by default for new customers.[30] TalkTalk also announced in a blog that they would be activating filters by default until customers made a choice about whether to opt out (the blog is no longer available on TalkTalk's site).[31] However, when ORG met with TalkTalk in July 2017, they confirmed to us their customers are forced to make a choice when setting up. We believe there is a similar arrangement at Virgin Media.[32]

Network-level blocking means ISPs enable filters that apply to every device connected to a household network. They can only be switched on or off by the account holder. Most ISPs offer different levels of filtering and some allow customers to customise the categories they would like to be blocked.

Most ISPs offer different levels of network-level filtering for different age groups, but only one level can be active at any time. Some offer the ability for timed filters, which can be switched on or off automatically, depending on the time of day.[33] Device-level filtering is also achievable without the use of ISP filters by using filtering software on individual devices, such as Net Nanny, McAfee Family Protection, or OpenDNS FamilyShield.

Each ISP outsourced the development of their filters to third party suppliers such as Symantec and there is no consistency or transparency about the criteria that these suppliers are using. Depending on where suppliers

---

[30] *Sky Broadband. (2015, December 21). Sky to automatically turn on parental controls for all new broadband customers. Retrieved 7 March 2019, from https://web.archive.org/web/20161219184644/https://corporate.sky.com/media-centre/news-page/2015/sky-to-automatically-turn-on-parental-controls-for-all-new-broadband-customers*

[31] *Birtles, Alex. 'How HomeSafe Is Keeping TalkTalk Homes Safer | TalkTalk BlogBlog', 23 January 2015. https://web.archive.org/web/20150130140151/http://blog.talktalk.co.uk/newsroom/how-homesafe-is-keeping-talktalk-homes-safer/*

[32] *Virgin Media's system is sometimes described as 'default on' but we have been assured that customers are asked whether they want filters or not at set up.*

[33] *'BT Parental Controls: How to Keep Your Children Safe Online'. BT.com. Accessed 13 March 2019. http://home.bt.com/tech-gadgets/internet/broadband/stay-safe-with-bt-parental-controls-11363887238413*

are located, there may be an inherent cultural bias about what is viewed as inappropriate for under 18s. There is a large discrepancy over which websites or categories of content each ISP filters. What is blocked by one ISP is not necessarily blocked by another.[34] There is no definitive list of sites that are considered harmful for children nor it would seem are there any consistent criteria.

Each ISP also has its own complaints process. Some ISPs have indicated that their supplier decides what should be blocked and they have no control over it. For example, when contacted to request review of a site that is inappropriately blocked, we find that BT's automated system issues a response that says:

> *"BT Parental Controls is conducted by our expert 3rd party supplier and BT is not involved in this process. ... BT or its third party supplier will not enter into correspondence regarding this investigation."*

Staff do not always appear to be appropriately trained to deal with overblocking queries over the phone. One website owner we spoke to found that when she called Virgin Media to report the incorrect block, the customer services operative she spoke to refused at first to believe that there was no pornographic or violent content on her site. She was told to speak to her own ISP even though they were not blocking her site, and even advised to tell all her customers to disable the filters.[35]

Take up of ISP filters

When ISP filters were launched in late 2013, they were first offered to new customers. An Ofcom report showed that, six months later, the take up among new customers was relatively low: [36]

- BT: 5%
- Sky: 8%
- TalkTalk: 36% [37]
- Virgin Media: 4%

Ofcom published a second report in December 2015, one year after ISPs' existing customers were given an 'unavoidable choice' about filters. In January 2015, Sky changed its process so that if existing customers did not make a choice about filters, they were switched on automatically whether or not there were children in the household. Customers had to opt out if they did not want them.

---

[34] *See: https://www.blocked.org.uk/stats*

[35] *See: https://www.blocked.org.uk/personal-stories*

[36] *Ofcom. 'Internet Service Providers: Network Level Filtering Measures', 22 July 2014. https://www.ofcom.org.uk/__data/assets/pdf_file/0019/27172/Internet-safety-measures-second-report.pdf, p.17*

[37] *According to the above-referenced Ofcom report, one potential explanation for filter uptake being notably higher for TalkTalk customers is the fact that TalkTalk provided customers with a pre-ticked box when asking them to whether they wanted to enable filters. (See 3.26)*

ORG contacted each of these ISPs in 2015 for the actual numbers of households using filters. TalkTalk were the only ISP to provide figures. Using a combination of figures relating to broadband customers and the take up figures from Ofcom, we created rough estimations for the number of households that have active filters in the UK.

ISP	Percentage of customers using filters[38]	Number of households using filters[39]
BT	6%	550,000 (estimate)
Sky	30-40%	2 million households (estimate)
TalkTalk	14%	450,000 (confirmed by TalkTalk in July 17)
Virgin Media	12.4%	650,000 (estimate)

We welcome corrections to these figures from ISPs. We would encourage ISPs to regularly publish up-to-date figures of how many households have adult content filters enabled. Website owners can get a better understanding of the impact of web blocking if they can see how many households will not be able to see their site if it is blocked.

More recent evidence from Ofcom states that around half of parents do not use filters, even when they are aware of them.[40]

Do filters prevent children from seeing harmful content?

We are not aware of research demonstrating that filters are effective in preventing children and young people from seeing harmful content. Researchers from Oxford University's Oxford Internet Institute published a 2017 paper in the Journal of Pediatrics noting they had "failed to find convincing evidence that Internet filters were effective at shielding early adolescents from aversive experiences online" and, within their sample, found "convincing evidence they were not effective".[41]

[38] *Ofcom. 'Strategies of Parental Protection for Children Online', 16 December 2015. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/31754/Fourth-internet-safety-report.pdf p.5*

[39] *These figures were calculated using figures for Q4 2016 from https://www.choose.co.uk/guide/home-broadband-market-overview.html and take-up percentages from http://stakeholders.ofcom.org.uk/binaries/internet/fourth_internet_safety_report.pdf*

[40] *Ofcom. 'Children and Parents: Media Use and Attitudes Report 2018', 29 January 2019. https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf. [This report does not include more up to date figures on takeup, unfortunately.]*

[41] *Przybylski, Andrew K., and Victoria Nash. 'Internet Filtering Technology and Aversive Online Experiences in Adolescents'. The Journal of Pediatrics 184 (1 May 2017): 215-219.e1. https://doi.org/10.1016/j.jpeds.2017.01.063*

It can be assumed that filters will limit very young children's ability to see pornography – whether searched for intentionally or deliberately – unless particularly adept at using technology. Filters do not block all pornography, there is still a risk that a young child could come across unsuitable content even if ISP filters are activated. This could be through mainstream social media platforms, such as Twitter[42], or by actual pornographic sites that are not blocked by filters.[43]

Our research shows filters may block many pornographic sites and many sites that children are unlikely to be interested in anyway, such as wine merchants and breweries, but they are unable to protect children from individual pieces of content on sites like Twitter, Facebook and YouTube. In the modern encrypted era of the Internet, filters are an increasingly blunt instrument which can only restrict access to unsuitable content on the aforementioned platforms by blocking access to the entire platform.[44] This renders ISP-level web filters ineffective as gatekeepers for what content children are able to view online.

YouTube in particular has been the focus of recent media attention concerning content children can view. While content on YouTube may not be pornographic by site policy, parents have raised concerns about children still being able to access "disturbing videos" on the platform, including on the YouTube Kids section of the platform which is designed to exclude content which is unsuitable for children.[45] ISP-level filters are unable to take any effective steps to stem the flow of potentially unsuitable content on these platforms aside from, as already discussed, blocking entire platforms indiscriminately.

If technically adept children wish to view pornography filters are unlikely to stop them. Ofcom's report into the strategies parents use to keep their children safe noted "there is broad agreement that all content filtering solutions are liable to circumvention by a dedicated and technically competent user, supported by a range of advice available online."[46]

Parents are also aware of this. According to Ofcom's 2018 Children and Parents: Media Use and Attitudes report, 15% of parents of children aged 5-15 said they thought their child would be able to bypass home network-level filters. This figure raises to one in five among parents of children aged 12-15.[47]

Professor Andy Phippen, professor of social responsibility in information technology at the University of Plymouth, argues that this is why young people appear to tolerate filtering and monitoring technology:

> *"they know [filters] don't work and they know how to get around them. Filtering*

[42] *White, Geoff. 'One in Every Thousand Tweets Is Porn'. Channel 4 News, 17 February 2015. https://www.channel4.com/news/one-in-every-thousand-tweets-is-porn*

[43] *We are not considering the impacts of partial requirements for age verification systems in this repov rt, but they too will only partially reduce certain opportunities for under 18s to access pornographic content*

[44] *This technical limitation is discussed further in later sections of this report.*

[45] *Matsakis, Louise. 'Parents, Here's How to Make YouTube Kids Safer'. Wired, 28 February 2019. https://www.wired.com/story/youtube-kids-parental-settings-safer/*

[46] *Ofcom. 'Strategies of Parental Protection for Children Online', 16 December 2015. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/31754/Fourth-internet-safety-report.pdf, p.16*

can be bypassed through proxies and personal hotspots, monitoring doesn't work with encrypted communication, and location tracking can be disabled if you switch off your device or leave it with a friend!"[48]

Some of the ways that older children may be able to see pornography or other banned content include:

- **Friends**

  They may access content through WiFi at friends' houses where filters are not activated. Friends may also send pornographic content via WhatsApp or similar messaging apps that are not affected by filters. A Parent Zone report noted: "each child - however diligent their parents have been about filtering and monitoring on home broadband – is only as safe as their least-protected friend".[49]

- **Virtual private networks (VPNs)**

  VPNs allow users to access websites securely and anonymously. Devices contact websites through the VPN, bypassing filters or geo-blocking. These can be free or paid for. The VPN market is growing rapidly. The global mobile VPN market is expected to grow to $1.5 billion by 2023.[50]

- **Proxy sites**

  Proxy sites act as intermediaries between computers and websites and files they want to connect with. They are often free and easy to use. Crucially, proxy sites are often encrypted, which means that ISP-level adult content filters are unable to block sites which users access via a proxy.

- **Tor**

  Tor is free software that allows people to use the Internet anonymously, without filters being able to see what sites are being visited, or block traffic to sites which are on the block list. Internet traffic from Tor users is routed through a series of nodes run by volunteers.

- **File sharing services**

  While file sharing sites may be blocked, it is harder to stop file sharing services with filters.

- **Data storage**

  Young people may use CDs or other offline media, to circulate pornography or other material such as shared music or films, much as was commonly done before streaming video and large images became easy to download due to increased Internet bandwidth.

---

[48] *Open Rights Group. 10 x 10: Digital Rights for the Next Decade, 2016. p.57*

[49] *Rosen, R. (2017, January). Ordinary magic for the digital age: understanding children's digital resilience. Parent Zone. Retrieved from https://parentzone.org.uk/system/files/attachments/Parent%20Zone%20Ordinary%20Magic%20online%20resilience%20report.pdf*

[50] *P&S Intelligence. 'Mobile VPN Market to Reach $1,560.7 Million by 2023', June 2018. https://www.psmarketresearch.com/press-release/mobile-virtual-private-network-products-market*

- **Sexting**

  Young people may also create their own pornographic images and share them, commonly known as sexting.

There are multiple ways children may come to view inappropriate content using technology, web filters are unable to act as a panacea to protects children completely. This should be kept in mind and should inform discourse and decisions around content filtering. Applying wide-ranging content filters on the basis of a "precautionary principle" approach may seem like a good idea even if there were some risk of overblocking, but the potential harm caused by overblocking is much harder to defend where it is clear that content filtering does not have as much of an impact on the ability of children to access inappropriate material as some may claim.

Harms of overblocking

Young people and other household members

A 2014 UN report on free speech noted that:

> *"The result of vague and broad definitions of harmful information, for example in determining how to set Internet filters, can prevent children from gaining access to information that can support them to make informed choices, including honest, objective and age-appropriate information about issues such as sex education and drug use. This may exacerbate rather than diminish children's vulnerability to risks"* [51]

Even if only a small proportion of websites are incorrectly blocked, there can still be significant consequences. For example, we tested around 9,000 Scottish charity websites and discovered that around 50 of them were blocked by one or more ISPs.[52] This was a small proportion, but a number of these sites were designed to reach out specifically to young people in a crisis, including the Different Visions Celebrate project in Dundee that works with under 25's who have questions about their sexuality, and Glasgow's Say Women project, which offers services to young women who have survived rape, abuse and sexual assault.

Adults can also be affected by erroneous Internet filtering – for example people attempting to access domestic abuse, rape counselling or other crisis services. Websites are often the first point of contact for such

[51] *United Nations General Assembly. 'Promotion and Protection of the Right to Freedom of Opinion and Expression', 21 August 2014. https://undocs.org/A/69/335., para 49*

[52] *"Scottish NGO Results." Open Rights Group. Accessed March 13, 2019. https://www.openrightsgroup.org/blog/2014/scottish-ngo-results*

services. If people are prevented from using them, it may prevent them from getting help.

Brian Cowie, Manager and Senior Recovery Support Practitioner at Aberdeen-based Alcohol Support told STV:

> *"These filters are ridiculous. How are we supposed to get people help and into therapy when they need it if they can't get through to us?*
>
> *"There's no way that I'd want anyone to be unable to reach us. The most important thing nowadays is not just for people seeking help with their alcohol problems to be able to seek help - it's also for their families and their children to be able to access support as well."* [53]

These are genuine harms that cannot be dismissed by the fact that erroneous blocking may only lead to a small number of organisations being filtered.

Harms of overblocking for businesses

Websites are essential to modern businesses and overblocking can have a serious impact. This is especially true for small businesses, who our research shows appear to be more likely to be blocked than larger ones. Small businesses are also less likely to have the kind of wide customer base that would enable them to discover very rapidly from customer feedback whether particular service providers were filtering their sites. Larger businesses are more likely to be empowered to discover erroneous blocks more rapidly and work to get them corrected.

A number of specialised wine merchants have experienced their sites being blocked by the filtering systems. We do not see the same outcome for supermarkets selling alcohol and stocking the same products. This is despite the fact that both arguably pose the same potential harm to minors.

Many of the small businesses that have contacted us note that they cannot rely on their potential customers having awareness of their brand. If their site is blocked, customers will assume that there is something dubious about it. A number of business owners who have submitted reports via the Blocked tool have indicated that their site being blocked impacts the credibility of their business.

As Rebecca Struthers, whose watchmaking business was blocked by Virgin Media, puts it:

> *"As a small watchmaking business, we don't have 200-300 years of reputation that a more established company has. If customers can't get onto the site, it*

[51] *"Anger as ISP Web Filters Block Access to Fifty Scottish Charity Websites | STV Edinburgh | Edinburgh," July 15, 2014.* https://web.archive.org/web/20140715071104/http://edinburgh.stv.tv/articles/282356-anger-as-isp-web-filters-block-access-to-fifty-scottish-charity-websites/

> *flags up that there is something fraudulent, which reflects badly on us. They will assume there is something wrong with our website not the filters – they are more likely to trust BT or Virgin [Media] than a small business like ours."* [54]

The small businesses that have contacted ORG have understandably been very concerned about the financial damage caused by blocking. As Amy Leatherbarrow who ran a ladies' dressmaking agency that was blocked by Sky and O2 told us:

> *"Who knows how many customers have encountered this and potential sales we have lost? We also offer a re-selling service for our clients which will have been affected. Our website is so important in our advertising and marketing and this issue is devastating as a business owner.*

Philip Raby who runs a Porsche consultancy told us,

> *"we must have lost some business and, of course, it doesn't look great telling people the site is not suitable for under 18s!"* [55]

Most of the small businesses that contacted us discovered that their site was blocked by accident. Why would dressmakers, watchmakers or Porsche dealers suspect their sites were blocked? We think that the overblocking of small businesses is a significant problem. ISPs and mobile phone providers need to be more proactive in raising awareness of this.

Harms of overblocking for free speech

Plans to stop children from seeing pornography online have been extended to a much wider range of content deemed 'adult'. As well as leading to overblocking, this also results in companies being required to make decisions about what is, and is not, suitable for children. It is unclear that they are in a position to do this. As examples given in the case study on alcohol below show, companies are making dubious decisions about content that is unlikely to be harmful to minors. This is problematic for free speech in the UK.

As the UN Special Rapporteur's 2014 free speech report put it:

> *"The Internet has dramatically improved the ability of children and adults in all regions of the world to communicate quickly and cheaply. It is therefore an important vehicle for children to exercise their right to freedom of expression*

[54] https://www.blocked.org.uk/personal-stories

[55] https://www.blocked.org.uk/personal-stories

> *and can serve as a tool to help children claim their other rights, including the right to education, freedom of association and full participation in social, cultural and political life. It is also essential for the evolution of an open and democratic society, which requires the engagement of all citizens, including children. The potential risks associated with children accessing the Internet, however, also feature prominently in debates about its regulation, with protection policies tending to focus exclusively on the risks posed by the Internet and neglecting its potential to empower children."* [56]

Children aged 16-18 are already considered mature for some legal purposes. At this age, they can legally have sex, work, or join the army. It is therefore clear that it is reasonable to treat members of this under 18 age group differently, rather than to subject them to a one-size-fits-all approach to filtering which imposes the same level of content blocking on all who fall into the wide "under 18" age group.

Other harms caused by filters

Filters contribute to an increasing set of restrictions on communications and access to information for children - both at home and in school. There are also other factors in this, from the rise of technologies that tag children, to government programmes like Prevent. As a result, we are seeing the unprecedented monitoring of the UK's young population. This has implications for the free speech and privacy rights of the next generation. We do not yet know the full extent of the effects of this, which could see a rise in self-censorship or the increased use of circumvention tools.

In the debate about harmful content online, children's voices are not being heard. As a report by the Child Rights International Network noted: "given the gulf that exists between adults' and children's experience of and the ways they use technology, it is all the more important that children are involved in developing any age-labelling systems." [57]

Of course, impacts such of those we have illustrated here can be argued to be anecdotal and unrepresentative. Individual problems can be fixed and dismissed. For this reason, we have tried to quantify the harms in the research we present in Part 2 and 3.

---

[56] *United Nations General Assembly. "Promotion and Protection of the Right to Freedom of Opinion and Expression," August 21, 2014. https://undocs.org/A/69/335, para 65*

[57] *Child Rights International Network. "Access Denied: Protect Rights - Unblock Children's Access to Information," June 2014. https://archive.crin.org/sites/default/files/access_to_information_final_layout.pdf*

The legal basis for content filtering

There has never been a legal obligation for companies to provide filters. In the case of ISPs, the companies voluntarily agreed to create parental controls after private meetings with government officials and policy makers. Parliament did not pass any legislation.

In November 2015, the European Union agreed the final version of a regulation on net neutrality, known as the Open Internet Regulations, which state that providers of Internet services: "should treat all traffic equally, without discrimination, restriction or interference, independently of its sender or receiver, content, application or service, or terminal equipment".[58]

The regulation aims to stop ISPs from acting in an uncompetitive way, and intervening against particular parties or companies, to keep the economy as innovative as possible. Filters have clear impacts here. By blocking small alcohol providers such as corner shops or wine merchants, but not others, such as large supermarkets. The UK's filtering arrangements may be unlawful because they do not treat all traffic equally; the regulation stipulates that only illegal content can be lawfully blocked.

The Regulation also attempts to provide legal balance around blocking, allowing a member state to put in place laws that require ISPs to block sites, as an exemption to the general prohibition on blocking. Such legislation would need to show respect for proportionality and the rights of the blocked site and its users. These requirements are not spelled out in the regulation, but might for instance include the right to be notified and to be able to stop an incorrect block.

The current blocking arrangements, which are opaque, could not be justified as proportionate, clearly codified or respecting legal process for all parties.

After the regulation was agreed by the European Parliament, the then Prime Minister, David Cameron told the House of Commons that the Government would legislate to allow filtering to continue in the UK. The following clause in the Digital Economy Act 2017 was included for this purpose:

> *"A provider of an Internet access service to an end-user may prevent or restrict access on the service to information, content, applications or services, for child protection or other purposes, if the action is in accordance with the terms on which the end-user uses the service."* [60]

---

[58] *Regulation (EU) 2015/2120, § 8 (2015).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120

[59] *For instance, to comply with the Charter of Fundamental Rights, European Convention on Human Rights, and the Human Rights Act 1998.*

[60] *Digital Economy Act 2017, s.105 (2019).* https://www.legislation.gov.uk/ukpga/2017/30/part/6/crossheading/internet-filters/enacted

In a debate on the Digital Economy Act (DEA) 2017 amendment, Baroness Jones appeared to question the efficacy of this amendment:

> *"To some extent we are taking all of this on trust. While it would be easy to demand more evidence, I accept that it would not help the case of those committed to family-friendly filters—I suspect that the more we probe, the more the robustness of the proposals before us could unravel. We support the intent behind these amendments and it is certainly not our intention to bring them into question in any way."* [61]

As we understand it, the amendment to the DEA 2017 is not sufficient to make ISP filtering legal. In a written question from Julia Reda MEP on the topic of the legality of ISP filters, European Commissioner Andrus Ansip, who leads the project team for the Digital Single Market[62], responded that:

> *"the provision of an Internet access service whose terms of service restrict access to specific information, content, applications or services, or categories thereof, result in limited access to the Internet and as such would be contrary to Article 3 of the Regulation. This is further explained in paragraph 17 of the BEREC (Body of European Regulators for Electronic Communications) guidelines. Whether the end-user has the ability to disable that restriction would not affect the above assessment."* [63]

The BEREC Guidelines state:

> *"BEREC understands a sub-Internet service to be a service which restricts access to services or applications (e.g. banning the use of VoIP or video streaming) or enables access to only a pre-defined part of the Internet (e.g. access only to particular websites). NRAs should take into account the fact that an ISP could easily circumvent the Regulation by providing such sub-Internet offers. These*

---

[61] *House of Commons. 8 February Debate (Vol 778, Col 1786), 2017.* https://hansard.parliament.uk/Lords/2017-02-08/debates/6EFC892A-F1A8-4156-B838-E8952E0908BA/DigitalEconomyBill#contribution-DBD7F39C-6A3F-4BDC-8759-E97AF7F26B59

[62] *European Commission. 'Andrus Ansip'. European Commission, 7 March 2019.* https://ec.europa.eu/commission/commissioners/2014-2019/ansip_en

[63] *'Parliamentary Questions: Net Neutrality and Restriction of Access', 29 August 2017.* http://www.europarl.europa.eu/doceo/document/E-8-2017-005328_EN.html

[64] *Body of European Regulators for Electronic Commissions. "BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules," August 2016.* http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf

> *services should therefore be considered to be in the scope of the Regulation and the fact that they provide a limited access to the Internet should constitute an infringement of Articles 3(1), 3(2) and 3(3) of the Regulation."* [64]

The Regulation will apply until the UK leaves the European Union, but may continue have legal effect beyond this departure depending on the terms of deals or agreements which are negotiated with regard to the UK's future relationship with the Union.

We would like Ofcom to clarify the legal status and basis for adult content filtering, and provide guidance to companies who might be in breach of the law.

Filtering by ISPs is problematic for many reasons including:

1. Network level filters are 'one size fits all' and will never be suitable for everyone in a household. Adults may dislike the intrusion of a filter, while small children may need a lot of content to be restricted. As we discussed above, older teens in the 16-18 age bracket have different needs with regard to being protected from particular content than younger children.
2. Network level filters may give a false sense of security to families who mistakenly believe ISP claims that they provide peace of mind.
3. Several ISPs have trouble operating network filters. We have observed filters disabling themselves for an ongoing period of months at the test line we use at TalkTalk. At Plusnet we were unable to get filters to work at all on at two lines we tried. The technical difficulty of operating content filters at network level should not be underestimated.
4. Filters depend on the misuse of the Domain Name System (DNS) by 'forging' DNS results, sometimes including interfering with DNS results from third-party services. The interaction between filters and DNS systems may cause reluctance at ISPs to adopt DNS security technologies, which would improve Internet safety including protection against man in the middle attacks.[65]
5. Filtering offers a means of interfering with competitors' markets, while claiming that this is done by user choice.
6. Filtering prevents access to legitimate content in an arbitrary manner.
7. In general, mass adoption of filters will be contributing to a trend towards use of VPNs, proxies and other technologies to enhance users' privacy and access to content. Over time, this reduces the effectiveness of targeted blocking measures imposed by law, such as court orders to block copyright infringing websites,

[65] *"Man-in-the-Middle Attack." Wikipedia, March 6, 2019.* https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack

or sites that do not provide age verification for adult content.

These issues will have been in the minds of European Union legislators when drafting the Open Internet Regulations. ISPs should ideally point customers to third party tools, rather than operating network-level filters which are in conflict with their basic business of providing Internet access.

Error correction

Correcting errors in filtering systems is not necessarily easy, and was not prioritised by the Government alongside introduction of filters. Some MPs such as Claire Perry initially denied that there would be a problem with errors at all. [66]

O2 are the only provider to have a URL checker.[67] This tool ended up being disabled for over a year, beginning in late 2013, following its use by journalists.[68] Each ISP provides an email address for reports of overblocking, but ISPs do not accept bulk or automated enquiries.

Internet Matters is a not-for-profit organisation, backed by BT, Sky, TalkTalk and Virgin Media, which promotes online safety for children. Website owners can email report@internetmatters.org to find out if their site is blocked by the four ISPs. It should also be noted that this is only available to website owners, not the wider public. Owners can ask whether a particular site might be blocked.

ORG feels these solutions inadequate so we run our own system, Blocked. It allows end users to test to see whether sites are blocked by filters on all the major broadband and mobile ISPs. ORG would like to work with providers, Internet Matters and the BBFC to help reduce the censorship caused by filters. We hope that Internet Matters will promote the Blocked tool to help people find out instantly whether a site is blocked and if they need to contact an ISP.

[66] *'UPDATE MP Claire Perry Claims UK ISP Internet Filters Will Not Overblock - ISPreview UK', 29 January 2014.* https://www.ispreview.co.uk/index.php/2014/01/government-mp-claire-perry-claims-uk-isp-internet-filters-will-overblock.html

[67] *"O2 Site Checker." Accessed March 13, 2019.* http://urlchecker18plus.o2.co.uk/

[68] *'O2 Pulls Blocked URL Checker as Wave of New Customers Activate Their Phones'. Open Rights Group, 24 December 2013.* https://www.openrightsgroup.org/blog/2013/o2-pulls-blocked-url-checker-as-wave-of-new-customers-activate-their-phones

PART TWO: Understanding our Blocked.org.uk data

Background to Blocked.org.uk

ORG has collaborated with volunteers to develop a tool that tests whether sites are blocked by UK ISPs. The tool is located at Blocked.org.uk, and was first launched in July 2014. The system allows anyone to check whether a website is being blocked by the filters of major home and mobile ISPs in the UK. Through this we have gained valuable insight about the extent of incorrect content decisions based on filtering. The data we have collected is examined in Part 3 of this report, and laid out in summary tables in Appendix A.

Site owners and users can visit the Blocked tool and enter a domain or URL to check. The system then passes this to a series of probes, some of which are connected to fixed broadband lines, and others to mobile data connections. We have an unfiltered and a filtered line for each ISP. The probes request the URL via the ISP to which they are connected and report the results. The results of the tests appear to the user of the Blocked tool.

The tool also allow users to search blocked sites by category and keyword, and to make it easier to report these errors to ISPs and mobile providers. In 2018, we began to route ISP replies to users' reports through the tool, allowing us track the responses that ISPs sent back to Blocked users. This makes it possible to view an ISP's stated reasoning when they refuse to unblock a particular site, and also view how long it takes for a user to receive a reply, if at all.

When we first launched Blocked, ORG discovered that around 10% of the Alexa top 100,000 websites were blocked by the default settings of at least one filtering system. This rose to 20%, or one in five, websites when strict settings were applied. We found lots of websites are erroneously blocked, and that different sites appear to be blocked by different ISPs, demonstrating a lack of common consensus regarding what material should be blocked.

We have run tests on over 35 million unique domains across 15 ISPs and mobile providers and found over 760,000 currently blocked domains. We have added real-time updates on the Blocked tool's results page, and expanded the tool to also detect court-ordered blocks for sites which host copyright infringing material.[69]

Blocked has helped website owners find out their websites are blocked. Many did not suspect that this was happening because the websites they run pose no harm to children at all. As Amy Leatherbarrow, who ran a women's clothing company said:

[69] *See: https://www.blocked.org.uk and https://www.blocked.org.uk/stats*

> *"Without www.blocked.org and your help, I would not have known how to go about getting this problem resolved".*[70]

Keyword search has been particularly helpful for us to discover wrongfully blocked sites in certain categories, such as LGBT, counselling and business websites. We are able to use keywords to create automatically-populated lists of blocked domains which are likely to be mistakenly blocked, helping volunteers to focus their efforts to report these sites specifically.[71]

The reports filed and the responses given, as well as the search facility, have given us the ability to present more detailed information to show how filters restrict content and make mistakes.

Aims of this research

This research seeks to understand the nature of the errors with Internet filters, and the potential damage they may cause. We believe filtering is demonstrably error prone. It should be clear that it is important to limit filtering to where necessary, for instance to help a particular child manage their Internet access. If it is the case that filters necessarily cause some damage by unavoidably overblocking, then this damage from filters can at least be limited if the use of filters is encouraged only in more targeted contexts, for instance on devices belonging to individual children, and by ensuring that adults agree to the use of filters before they are applied. It is also important to know what kinds of mistakes are made, and how these are handled.

We chose to take a closer look at the problems arising from filters on mobile networks and fixed-line ISPs. The former are 'default on', while ISP filters are targeted at the whole home network. Both are in our view encouraging far more filtering than is ideal, as they are targeting adults who are able to manage their content choices.

The research has attempted to understand, from our data:

1. What kind of sites are reported as blocked?
2. Who reports sites?
3. What damage is cited by users making reports?
4. How mobile and fixed ISPs respond to reports?

Our dataset reflects reports we have handled. We are unable to examine what happens when people choose not to report mistakes, or report them directly to ISPs. For a report to reach us, the following steps typically

[70] *See Designer Dressing Room at: https://www.blocked.org.uk/personal-stories*

[71] *See: https://www.blocked.org.uk/lists*

take place occur:

1. A block is noticed by a site owner or user or is reported to them;
2. They would need to investigate how to remove the block; and
3. They would need to find our website for instance via search and choose to use it rather than an ISP's own systems.

It is reasonable to assume that Blocked.org.uk would be used mostly by non-customers of ISPs who decide not to rely on reporting directly to a network, nor by using the reporting facility offered to site owners by Internet Matters. This may well be a small fraction of such reports.

Research methodology

We have attempted to understand what sites are blocked by examining our indexing data through searches and classifying reports made through the Blocked tool. Additionally, some interviews with affected website owners have been conducted.

User reports

The unblock requests which users submit via the Blocked tool are a rich source of information about filtering blocks and their direct impacts. For reports, we have:

1. Classified each report according to the reporter's affiliation to the site in question (owner, user, web developer, etc).
2. Checked whether reports appear to be violations of the ISP's blocking policy.
3. Categorised the damage cited by users who have reported blocked sites.
4. Categorised the site against our own typology.

It should be noted that users fall broadly into four types:

1. People with a specific complaint, wishing to report a wrongful block they are already aware of.
2. People worried that a site may be blocked, and checking if it is.
3. People loosely affiliated with ORG, who are aware of issues around content filtering, and wish to make reports to ISPs about particularly problematic blocks. The main Blocked.org.uk site presents a selection of blocked sites for users in this category to check and report if necessary.

4. People affiliated with a particular campaign or industry that are aware of a specific impact being caused by filters. This has included some local branches of the Campaign for Real Ale, companies selling fireworks, and shooting ranges.

Our dataset reflects the mistakes and harm suspected and uncovered by people motivated to get them rectified. We would not characterise it as a completely 'objective' measure of harm, nor necessarily an indication of where filters are causing the most harm, although it may provide us with a strong indication. It can how show that harms exist and highlight examples of these. Reports from website owners also give us an indication of who is finding out about filtering and is most concerned to rectify wrongful blocks.

Search

During the lifetime of the project, Blocked.org.uk has tested over 35 million unique domains for potential blocks. Where blocks are detected, information including title and metadata description are stored in the Blocked database. This data is made searchable on Blocked.org.uk site, to find possible erroneous blocks. We compile lists of search results which are particularly revealing, and some of these of results are prioritised for users to report. For instance, we prioritised local city results, charities, advice lines and counselling websites for users to review. However, our search is limited by the fact that we cannot regularly re-index all sites, so will not catch all blocks even for the URLs we have tested at least once.

Interviews

ORG and Top10VPN have spoken where possible to site owners about their experiences. These have been identified through their reports via Blocked.org.uk, so we are able to show when and where their site was blocked.

ISP response statistics

We evaluate the performance of ISPs by checking how rapidly and effectively they respond to user requests submitted via the Blocked tool.

Reports submitted via Blocked.org.uk

If filters work as intended, only sites clearly unsuitable for children would be blocked. We have found this is not the case. Many of the blocked sites under these filters do not contain adult content and in fact belong to charities, churches, counselling services, and mental health support organisations.

A small selection of sites which we feel have been inappropriately blocked can be found below. The rest of this report will focus on some of the specific issues we have found during our research.

Examples of Incorrectly Blocked Sites

Beam - Helping the Homeless

Beam.org is a site belonging to the Beam organisation.[72] Beam is a service that raises funds to help support homeless people into training and work. The service has been featured as a success story in many national newspapers, and also receives financial support from the Mayor of London.

CARIS Islington - Bereavement Counselling and Cold Weather Night Shelter

CARIS is an Islington-based charity which runs two projects - a Bereavement Counselling Service for children and adults, and a cold weather night shelter for the homeless. CARIS is a site which we found to be inexplicably blocked by some Internet Service Providers under the filtering system.[73]

Welcome Church

The Welcome Church is a church based in Woking, UK.[74] It describes itself as a "diverse community with activities and groups for all ages" and notes that it has "a vibrant youth and children's work, so your whole family can feel welcome".

Filters blocking the sites listed is problematic, and not just for Internet users unable to access Internet content Groups like these, as well as businesses who rely on their websites for income might find a large segment of the population blocked from accessing their sites. Some site owners and business owners may be unaware this is happening.

Using the tool, many businesses were able to discover or confirm that their site is blocked for certain users. The tool allows site owners or potential site users to submit an "Unblock Request", which asks an ISP to review a blocked site in accordance with their policy and ensure that their categorisation of it is correct. We find that most ISPs will take action to unblock a wrongfully-blocked site when they are alerted to it. However, it is unacceptable that, without our tool, many site owners may have been losing out on potential site visitors and

[72] *See: https://www.blocked.org.uk/site/http://beam.org*

[73] *See: https://www.blocked.org.uk/site/http://www.carisislington.org/*

[74] *See: https://www.blocked.org.uk/site/http://allwelcome.uk*

customers while being completely unaware of the fact.

Manually reviewing every site on the Internet would be time consuming and expensive, so adult content filtering makes heavy use of automated systems. These automated systems may look for particular keywords or content found on web pages and use a set of rules to decide whether a site should be blocked or allowed. Using an automated approach like this can lead to false positives and unfair or unreasonable blocks. This is because the automated systems do not have as much information as human reviewers with regard to the context or importance of content on webpages.

When considering what to block, automated systems need to decide whether they prefer to block too little or too much. By making the criteria for blocking tighter and forcing stricter matches, they can reduce overblocking. This increases the likelihood that they will 'underblock' and leave sites available which are unsuitable for children. As the products are aimed at preventing children's access to such sites, they are likely to prefer to match against loose criteria, meaning more 'overblocking' mistakes are made. This decreases the likelihood of children encountering material that has been chosen for blocking, but has detrimental effects elsewhere.

Even if a site is discovered to be wrongfully blocked and is reported to ISPs using our Blocked tool, some bias may still remain. At this point, a human reviewer is expected to assess the site in accordance with the ISP's blocking policies and determine whether to lift the block.

We have found that blocks are often lifted where they are clearly in error, but some blocks remain even after a review. The opinions of individual reviewers can differ, and may influence the re-categorisation process. For example, we examined the case of a site belonging to Feeld - a dating app for polyamorous couples.[75] The main webpage for this app had been filtered, and after receiving a request via our Blocked tool to review the site, one ISP continued to insist that it should be categorised as "pornography" because of the fact it targeted "alternative sexual preferences". The site or app in question did not contain any pornographic content. In any case, doing so would violated the app marketplace terms of service for both the Apple App Store and Google Play Store.

We experienced issues with some ISPs replying unreliably to reports of sites which are inappropriately blocked. Blocked.org.uk allows users to request ISPs unblock particular sites if a user feels they have been blocked in error. Some ISPs respond to this process by unblocking sites within a reasonable timeframe. But we have experienced issues with multiple providers being slow to reply, or not replying at all. Some providers send automated responses back to our tool, indicating that they will be in touch about a particular unblock request within a few days, and then we never hear from them again.

We have attempted to quantify these issues in our research, presented in Part 3.

[75] *See: https://www.blocked.org.uk/site/http://feeld.co*

Error rates and numbers of likely mistakes

It is hard to calculate the number of erroneous blocks and the number of vendors making mistakes compounds the problem for website owners. They may be blocked by an error at multiple opaque blocking systems, which they often cannot check.

In meetings with us, ISPs have asserted a 0.01% error rate in classifying whether sites should be blocked. Using this assumption, we can make an estimate of the total number of mistakes made, for instance on the four major fixed-line networks:[76]

	Sites Tested	Number of blocks	Percentage of sites tested which are blocked	Estimate of erroneous site classifications using ISP figure
BT	23,315,636	284,242	1.22%	2332
Sky	23,213,914	233,248	1%	2321
TalkTalk	22,573,610	311,238	1.38%	2257
Virgin Media	23,252,676	206,116	0.89%	2325

From our dataset we have also made a comparison of consistency based on sites which have been tested on all four mobile networks:

Number of mobile networks blocking a URL	Domains or URLs
1	25,492
2	33,042
3	43,055
4	72,335

More than half of the blocks implemented by mobile filters are not present on all networks. This is despite the fact that mobile networks have agreed on the BBFC's unified Classification Framework drafted, which defines what types of content should be blocked. By this measure, over half of the blocks on mobile networks may regarded as reflecting some kind of error, which may be either underblocking or overblocking content.

[76] *Figures correct as of 1 Mar 2019*

PART THREE: Research Findings

Problematic categories of blocks

Automated filters are blunt tools. The automation is required because it would be a huge task to manually classify every website on the Internet. But automated filters are based on sets of rules and often wrongly classify content as they lack a human understanding of context or nuance. In the course of our research with the Blocked tool, we have encountered a number of recurring themes among sites which have been wrongfully blocked, which we will explore in this section.

Problematic blocks largely fall into one or more of three main categories:

- Content which has been misclassified;
- Blocks which break the Internet at a technical level (for instance, blocking content distribution sites, application programming interfaces (APIs), or servers used by mobile apps); or
- Blocks which are based on categories which are overbroad and therefore end up applying to material which is not likely to be harmful to children.

For the purposes of analysing some of the most frequently recurring themes we have seen among blocked sites, this section will isolate some examples of content which fall into the categories identified above. It is important to note that there are limitations to our analysis, as we are unable to reverse-engineer the inner workings of web filtering systems. Our methodology is focused mainly on identifying common patterns or shared characteristics among sites which we have identified as being filtered. At the time of writing, the range of domains which we have proactively analysed using the Blocked tool is slightly UK-centric, and we expect to see further patterns emerge as more domains are processed and added to the database.[77]

The table below identifies some of the commonly recurring categories of domain which have been submitted to ISPs on behalf of users of the Blocked tool, and the number of domains which fall into each category. We have compiled this data by manually reviewing and applying a category which describes the main content of each submitted for unblocking via the Blocked tool. We analysed a total of 857 unique domains submitted by Blocked.org.uk users since July 2017. An expanded version of this table with the full range of categories we have manually assigned to reports is available in Appendix A of this document.

[77] *In addition to sites which have been specifically submitted for checking by users of Blocked.org.uk, we have proactively processed all sites registered under the .uk and .org top level domains. Sites registered with a .com top level domain are currently being processed and added to the database.*

Category for Submitted Reports	Number of reported domains
Advice sites (drugs, alcohol, abuse)	52
Alcohol-related (non-sales) sites	36
Building and building supplies	32
CBD oils, CBD-related, and hemp products	21
Charities and non-profit organisations	68
Counselling, support, and mental health	122
LGBTQ+ sites	40
Religious sites	21
Weddings and wedding photographers	44

To further analyse some of the recurring themes which we have encountered among blocked domains, we also expanded the scope of our analysis to include blocked domains which were in the Blocked.org.uk database but which had not necessarily yet been reported by users of the site. To quantify this data, we used keyword searches of Blocked.org.uk's database of blocked domains to identify sites which matched keywords relating to the various categories of frequent block we had seen. Through this process, we produced lists of sites in those categories which we feel are likely to be wrongfully blocked. While the number of user-reported URLs in particular categories is often relatively small, the lists of sites produced by keyword searches of our database offers a view of the scale and unpredictability of the level of overblocking which may be happening for specific types of site. A version of this table with footnote sources for the lists used to compile the data is available in Appendix A of this report.

Table A - Keyword list categories

Sites relating to keywords related to	Number of blocked domains identified through search[78]	Number of domains still blocked	Current ISP blocks[79]
Addiction, substance abuse support sites	185	91	287
Charities and non-profit organisations	98	17	24
Counselling, support, and mental health	112	77	191
Domestic violence and sexual abuse support	59	14	42
LGBTQ+ sites	114	39	121
School websites	161	23	52

Table A.2 Verified search results, UK sites only

Sites relating to keywords related to	Number of blocked domains identified through search[78]	Number of domains still blocked	Current ISP blocks[79]
Addiction, substance abuse support sites	35	14	48
Charities and non-profit organisations	91	17	24
Counselling, support, and mental health	104	70	177
Domestic violence and sexual abuse support	7	3	11
LGBTQ+ sites	27	7	25
School websites	143	13	28

Table A.3 Unverified search results

Sites relating to keywords related to	Number of blocked domains identified through search[78]	Number of domains still blocked	Current ISP blocks[79]
Building and building supplies	67	26	64
CBD oils, CBD-related, and hemp products	307	220	1081
Drainage and drain unblocking services	107	3	3
Photography sites	1858	732	2109
Religious (Christian) sites	137	54	147
Weddings and wedding photographers	4506	1718	3739
VPN sites	404	345	1719

Table A.4 Unverified search results, .uk domains only

Sites relating to keywords related to	Number of blocked domains identified through search[78]	Number of domains still blocked	Current ISP blocks[79]
Building and building supplies	59	23	48
CBD oils, CBD-related, and hemp products	112	91	510
Drainage and drain unblocking services	99	2	2
Photography sites	1372	514	1348
Religious (Christian) sites	37	9	20
Weddings and wedding photographers	4012	1480	3154
VPN sites	23	15	55

These tables are intended to illustrate how easy it is to find likely or actual errors in blocking systems. The data used in the tables above are intended to display particular patterns we have observed among blocked sites. They cannot be said to be inclusive of "all websites" as the Blocked tool is limited to testing only domains which have been submitted by users, or indexed for search. Figures based on user-submitted reports cannot perfectly reflect the entire landscape of wrongful or overzealous blocking by content filters, as users submitting reports are likely to proactively search for and report sites in categories which they already data is a reliable illustration of some of the issues that are arising commonly with the misclassification of particular categories of website.

The work that would be required to remove errors from ISPs' filtering systems would be very considerable, even for those areas we have been able to identify. The search terms we have used are not exhaustive and will not catch all relevant content, as the Blocked project's site indexing is limited. Our keyword searches are further limited by the fact that we have to run exclusion terms to filter out the most likely adult content in order to identify just those domains that are most likely to be mistakenly blocked.

Content misclassification

As filters misclassify content so regularly, we have logged a large number of examples of misclassification over the lifetime of the Blocked project. Due to the automated nature of these filters, there are a number of repeated misclassifications we have seen which are common and recur on a regular basis. This section will explore some of the more common misclassifications we encountered.

In many cases, misclassification does not have an obvious reason. It may be that filters classify some sites according to their hosting provider, for instance, assuming that all sites sharing a particular IP address are likely to be pornography, even when the sites are in fact radically different.

Domestic violence and sexual abuse support networks

One of the most obvious and egregious misclassification errors is the blocking of sites which offer information and support to survivors of rape and sexual assault.[78] Such sites, understandably, contain frequent uses of words and terminology which could be interpreted as sexual or pornographic in nature by a blunt filter which does not have an appropriate understanding of the context in which language is used.

The filtering of such sites is extremely problematic, as it may lead to vulnerable or at-risk people being restricted from accessing vital safety information or emotional support resources. The damage caused by this type of filtering is potentially very large, and ISPs should therefore take proactive steps to ensure that their filtering systems are free of examples of sites which fit into these categories.

[78] *See non-exhaustive list at: https://www.blocked.org.uk/list/Domestic%20and%20Sexual%20Violence%20Support*

School websites

Despite being demonstrably appropriate for children, school websites do not escape being caught up by overzealous adult content filters. Our research produced a non-exhaustive list of schools and school-related websites which were blocked, with at least 13 URLs in this category blocked by at least one ISP at the time of writing.[79]

Even more surprisingly, we detected at least 34 unique sites with a .sch.uk top level domain that had been filtered during the lifetime of the Blocked project. 24 of these were still blocked by at least one ISP as of March 2019, 12 on general filters, and 12 using BT's 'Strict' filter.[80] Domains ending in .sch.uk were allocated to schools beginning in 1999, "on behalf of the Department for Education and Skills (DfES), the Scottish Executive Education Department (SEED), the Welsh Assembly Education Department and the local education authorities of England, Scotland and Wales".[81] These domains cannot be registered privately and are only available to schools in the United Kingdom.

Some filters may misclassify content so poorly that they actively block school websites with an audience of children and families with children reliably demonstrates the fallibility of blunt network-level content filters. It is not only parents who may have an interest in visiting school websites; children may actively need to use such sites to view class schedules or information, or to submit homework.

As a caveat, we note that many of the school domains which we have found to be blocked are blocked by filters such as BT Strict, or TalkTalk Kidsafe, which are more intensive filtering options intended particularly for users with younger children. However, we do not believe that this affects the conclusion which can be drawn from the over-filtering of sites in this category - namely that filters often make errors that leave many sites filtered as 'collateral damage'. In particular, we highlight the fact that specific care is not being taken by supposedly child-friendly filter levels to avoid filtering resources specifically targeting children, or special-use domains which may only be registered by schools.

LGBTQ+ sites

We have seen a lot of sites which relate to LGBTQ+ issues and communities getting caught up in adult content filters.[82] This is potentially due to filtering systems drawing connections between sites specialising in pornographic content targeting LGBTQ+ demographics and sites which act as community resources or discussion forums.

---

[79] *See non-exhaustive list at: https://www.blocked.org.uk/list/Schools*

[80] *See: https://www.blocked.org.uk/list/sch.uk*

[81] *'UK Schools Get .Sch.Uk Domain', 23 September 2004. https://web.archive.org/web/20130528081325/http://www.netimperative.com/news/2004/09/23/UK_schools_domain*

[82] *See non-exhaustive list at: https://www.blocked.org.uk/list/LGBT*

Again, it is not only adults who are inconvenienced by the overzealous blocking of sites in this category. The filtering of sites which cater to LGBTQ+ identities is particularly problematic, as they are often a valuable and important resource for children and teenagers who may be seeking advice and support about their own identities or experiences. Being able to access such support networks may be particularly vital for children or teens who have unsupportive parents or families, or limited support resources outside of the Internet.

As Simon Mallison, who runs a network of services for the LGBT community, says, "If they're blocking my site they should be blocking Amazon too." Among those services is an online bookshop which sells a variety of books on gay history, politics and philosophy but at the time of writing was blocked by BT and Plusnet.

"All the stuff we sell is readily available on Amazon or in Waterstone's. All these shops now have LGBT books, there's nothing that's unavailable from the high street," Mr Mallinson continues.

> *"Over the years the blocking's increased - there's always been a catchup from ISPs and government because the internet moves so quickly. The ISPs have over the years increased their restrictions, which is frustrating - especially when it affects sites and books which talk about health issues as those really shouldn't be blocked.*
>
> *"The thing about Gay Bookshop, Gay Travel and so on is that they deliberately have nothing offensive on there. It's just travel information, guest houses and so on."*

Counselling, support, and mental health sites

Sites which deal with counselling, support and mental health are also frequently misclassified by adult content filtering systems.

In the case of sites specialising in relationship counselling, this is likely because many sites in this category make use of sexualised language to describe common relationship difficulties. Even in such cases, however, the sites are not sexually explicit and are unlikely to be of interest to children.

But as we have identified, it is not just relationship counselling sites which are being affected by filtering. There are many different types of counselling site we have identified using our non-exhaustive keyword searches, including sites which provide support for anxiety, stress, and narcotics use.[83]

[83] *See non-exhaustive list at: https://www.blocked.org.uk/list/Counselling*

Case Study

ADUS Healthcare is a private supplier of specialist care for people affected by addiction, however two of their sites were being blocked by BT and TalkTalk at the time of writing.

"It's been like this ever since we started." said ADUS director Mark Rich. "We help people get off heroin and cannabis and cocaine and alcohol and everything else - if they can't access the sites then they don't know we're there, and they can't get the help.

"There are people who need help with cocaine and can't access our rehab centres because of this."

Michael Stock is a sex and relationship therapist who is used to dealing with sensitive subject matter. "The research evidence suggests that people can struggle to seek help," he says. "It can take someone up to three years on average to get to the point of contacting someone like me."

Mr Stock's sexual and couple therapy site is currently being blocked by Sky, Three and EE.

"It's a difficult area, so if someone gets that far and then finds that they couldn't access my website then that could put them off for a long time again.

Mr Stock said he found the prospect of being blocked by ISPs worrying for his line of work.

> *"One group of people I work with are people who are worried that they will commit a sexual offence.*
>
> *"They're encouraged to seek help before they do, and of course if they're not able to get help then that could make the difference between them getting the help they need and going on to commit a serious sexual offence."*

Wedding sites

One recurring theme with regard to misclassified content that we have processed as part of our research is sites which belong to businesses that deal with weddings.[84] These may be venue hire, decoration hire, caterers or, in particular, wedding photographers. We have discovered the filtering of wedding sites to be a recurring theme, and one which potentially damages small and even large-scale businesses by blocking potential clients from accessing their websites.

[84] *See non-exhaustive list at: https://www.blocked.org.uk/list/Weddings*

We have not been able to identify common patterns among the webpages of wedding businesses which explains why they may be so frequently miscategorised, although the consequences of this filtering for the small businesses and sole traders involved is a real risk of damage through the loss of potential customers or contracts.

Drain unblocking services

Another recurring content misclassification relates to sites that offer services in drain cleaning, or otherwise maintaining drains and drainage equipment.[85] These sites show up in our logs of filtered sites repeatedly, however they do not contain any content which ought to be filtered under the ISPs' own filtering policies.

We are unsure why there is a theme emerging around the repeated misclassification of drainage-related sites. One possible reason could be the blunt automated filtering of terminology such as "unblock" and "unblocking". Many of the sites in question provide support, advice, and paid services that deal with removing blockages from drains, but the "unblock" and "unblocking" terminology is also associated with web pages that offer VPN and proxy services to "unblock" blocked websites as a means of evading content filters.

It is notable that over time we have observed that sites relating to drains and drainage have gradually become unblocked by ISPs, even where unblock requests have not been filed through the Blocked service. This is interesting to us, as it suggests that ISPs, or third-party filter providers, are capable of resolving some misclassification errors in their filtering systems themselves, and they may be reviewing and adjusting their processes accordingly.

Photographers

We have already mentioned the overzealous blocking of sites which belong to wedding photographers, but we have seen a pattern more generally that sees the personal sites of many small or independent photographers filtered. Keyword searches based on photography terms have identified a large number of photography sites which have been blocked over the lifetime of the Blocked project.[86]

Photographers are often sole traders who rely heavily on their website to act as a portfolio to demonstrate their work and style to potential future clients. It is not unreasonable to conclude that the filtering of photography sites in this manner could lead to a loss of business for the photographers involved.

Builders, building supplies and concrete

A number of sites which specialise in concrete and cement mixers are targeted for filtering with no obvious

[85] *See non-exhaustive list at: https://www.blocked.org.uk/list/Drains*

[86] *See non-exhaustive list at: https://www.blocked.org.uk/list/Photography*

common link between them which might cause filters to act to block them. Other building supplies firms are also blocked.

Religious sites

Churches, religious charities, and other religious sites also seem to feature prominently in our database of filtered sites. It is not immediately obvious why this is the case based on the content generally featured on sites of this type. In some cases, they may discuss relationships and sex, or problems like drugs and alcohol.

For the purposes of generating a list of religious sites, we focused on keywords related to various denominations of Christianity. This is because such sites are often presented in English and therefore easy to identify in our database using keywords. Sites relating to other religions which more commonly use non-English languages or non-Latin script may be more, or less, likely to be affected by overzealous filtering. This may make for fruitful future investigation. Despite this, keyword searches still uncovered a large number of filtered sites.[87]

Charities and non-profit organisations

Charities and non-profit organisations also frequently appear to get caught up in overzealous filtering systems.[88] This happens for reasons which we cannot exactly pinpoint, though it is illustrated by the numbers of reports seen for sites which are charities, charitable foundations, or non-profit organisations.

Alcohol-related (non-sales) sites

While we have encountered a number of sites online which sell alcohol directly to customers, and these are dealt with in the later section of this report Products already subject to age restrictions - there are also a number of sites which deal with alcohol as a topic but do not directly offer it for sale online. Examples of this include the sites for bars, pubs, breweries, and vineyards.

We separate these categories of site because the potential 'harms' presented to children by such sites are different. In the case of sites which directly sell alcohol, it is conceivable that sites may poorly implement age verification for purchases, and determined children may be able to acquire alcohol from the site. However, in the case of sites which do not offer alcohol for sale online, it appears far less likely that harm could be caused.

Pubs and restaurants listing their menus frequently include lists of alcoholic drinks which are available for sale on-site at the venue itself, are frequently blocked. It is hard to see any justification for the blocking of such sites, however. Children are unable to purchase alcohol using the site directly, and the information available on

[87] *See non-exhaustive list at: https://www.blocked.org.uk/list/Christianity*

[88] *See non-exhaustive list at: https://www.blocked.org.uk/list/Charities*

the sites about the alcohol which is available at the venue is unlikely to be different to that which is available inside the pub or restaurant itself.

Other sites in this category include nearly all websites run by the Campaign for Real Ale. There are also sites for beer bottle top collectors that have been classified as inappropriate for children.[89] Others are businesses related to the industry but not direct sales sites, such as pub management companies.[90]

Additionally, many breweries and vineyards use their websites as advertising tools for family-oriented events such as tours. For example, the Black Sheep Brewery in North Yorkshire, which offers brewery tour tickets for both 'kids' and 'family' was blocked.[91] While such sites inevitably also discuss the alcohol which the business produces, such events can be educational and alcohol is not being made available to children in the process. For businesses like these which generate revenue from family visits. Having their site blocked for users who have adult content filters enabled could conceivably lead to a direct loss of revenue, as some potential customers are unable or dissuaded from visiting the site.

We have also discovered inconsistencies with regard to how ISPs treat unblock requests for sites in this category. For example, BT and TalkTalk accepted a request to reclassify and unblock the website for *The George* pub in Wraysbury,[92] but rejected a similar request for a similar website owned by a pub less than 30 miles away, *The Greenwich Union*.[93]

The "Scunthorpe Problem"

Historically, early Internet filters were even more blunt and less aware of context than modern ISP-managed adult content filters. A particular class of content misclassification came to be known as the Scunthorpe Problem,[94] named after an incident in which AOL's filters prevented residents of Scunthorpe from creating accounts on the AOL service due to the presence of a certain sequence of letters within the word Scunthorpe which would be considered a profanity if they stood alone.

Over 20 years have passed since AOL's unfortunate incident, however through our research we are still uncovering examples of adult content filters which appear to be misclassifying sites based on certain strings of characters used inside a site's URL. Often these characters form part of personal surnames or forenames, or are unfortunately created when two words are joined together without spaces, as is common within web

[89] *For example, https://www.blocked.org.uk/site/http://www.vintagecans.com*

[90] *For example, https://www.blocked.org.uk/site/http://www.hopinnspubmanagement.co.uk*

[91] *See: https://www.blocked.org.uk/site/http://www.blacksheepbrewery.com*

[92] *See: https://www.blocked.org.uk/site/http://www.thegeorgewraysbury.co.uk*

[93] *See: https://www.blocked.org.uk/site/http://www.greenwichunion.com*

[94] *"Scunthorpe Problem." Wikipedia, March 12, 2019. https://en.wikipedia.org/w/index.php?title=Scunthorpe_problem*

addresses.[95]

After more than two decades of the problem being a known issue that may arise with adult content filters, we find it surprising that the issue still appears to be present with the modern systems employed by current ISPs.

Blocks which cause damage at a technical level

There are a number of blocks we have observed in which filters restrict access to domains which are not intended to be directly accessed by the general public, but instead form part of wider technical systems or sites. Blocking domains used this way can cause problems for other sites which make use of content hosted on these domains, or can prevent otherwise-authorised users from logging into domains which use login pages to restrict access. We have also encountered issues in which filters have blocked sites and products which are in the process of launching. We refer to these as 'pre-launch blocks'.

CDNs, APIs, and image hosting services

Some of the inappropriately blocked domains we have reviewed fall into a subset of domains which are not necessarily intended to serve content on the main domain as a regular webpage would, but act as domains which distribute content behind the scenes, such as images and code for other websites or mobile apps. Broadly, we have categorised these as content delivery networks (CDNs), APIs, and image hosting services. Collectively, we will refer to these as "backend services".

Sometimes, depending on the content which might be served by a publicly-facing website or application, a content delivery network or image host which hosts some of the content for the main site may find itself hosting content which would fall into the categories considered for blocking as adult content by ISPs.

At this point, an ISP's filter may opt to block the address of the backend service by its domain, though this does not necessarily lead to the blocking of the main domains for the site or app itself that the backend service hosts content for. Blocking just one of potentially many backend services which host content for a website or app can lead to a situation in which some content on that site or app simply fails to load for users on connections with filters active. This could cause breakage of the site or app in different ways, from a mild inconvenience of some images or content not loading through to total malfunction of the service.

Inaccurate blocks of backend services are particularly problematic, because there is no transparency to

[95] *See potential examples at:*
https://www.blocked.org.uk/site/http://www.pennyhancock.com;
https://www.blocked.org.uk/site/http://www.thepawtraitsexhibition.co.uk;
https://www.blocked.org.uk/site/http://www.trixiehiscockphotography.co.uk;
https://www.blocked.org.uk/site/http://www.kingsexotica.co.uk;
https://www.blocked.org.uk/site/http://www.bighornbasinpaleontologicalinstitute.org

the end user that the reason some of the content on a particular service may not be loading is down to an overzealous adult content filter. Additionally, the addresses of backend services are not often exposed to end users in an obvious manner, so a user who experiences some services failing to load and suspects adult content filters may be to blame is not necessarily empowered to even test the relevant domains with a service like our Blocked.org.uk tool.

We received one particular report privately via the Blocked tool which came from the developers of a mobile app who indicated that some of the URLs used by their backend services were being been filtered in this way. The app developers suggested that the filtering was causing them a loss of business. This led them to have to rapidly establish new domains and shift their content and services there so that their services began to work again and they were able to minimise the potential damage to the business that might otherwise have been caused by the blocks.

Technical back-end sites

Automated filtering systems also seem to struggle with the accurate categorisation of domains which are used to host technical infrastructure rather than more conventional public-facing webpage content. We have encountered examples of blocked domains which host administration panels for websites, log-ins for email services, and other generally non-public services.

For example, Automattic, a software company most notable for developing the WordPress.com blogging service, use an internal-only short domain for employees. For users external to the company, the domain redirects to the main company homepage, but for employees it allows access to company resources. Through the Blocked tool, this domain was discovered to be blocked by multiple ISPs and, at the time of writing, was still blocked by Three.[96] Ensuring employees are not blocked from accessing internal resources is particularly important for a company such as Automattic, whose employees primarily work remotely and may need to routinely make use of home or mobile Internet connections in the course of their work.

We have also encountered users who are facing issues due to the filtering of domains hosting multiplayer video games. One domain used by a server for a small game called Space Station 13 was reported by a user who noted that, due to the block, administrators of the server were having to re-route Virgin Media users in the UK through alternative servers. According to the user, this caused “lag” and a degraded game experience for those players.[97]

One potential explanation for the overzealous filtering of domains of this type is that such technical access sites often make use of technical language as they are not intended as public webpages. It is possible that filters may mistake this as being language which relates to VPN services or “hacking tools” - two commonly filtered categories of website. It is also possible that the filtering of pages of this type may be intentional, as

[96] *See: https://www.blocked.org.uk/site/http://a8c.com*

[97] *See: https://www.blocked.org.uk/site/http://geo.byond.nsscyberiad.net*

login pages by their nature suggest that other content is held on the domain that the ISP is unable to see or classify.

Regardless of the reason why such sites are filtered, the filtering of technical backend sites in this manner clearly leads to issues for users such as those who need to make use of administration panels for websites, remote workers who need to be able to log into company-hosted remote access interfaces, or those who wish to play multiplayer video games.

Pre-launch site blocking

Another recurring theme we have seen from these content filters is the blocking of pre-launch websites which do not yet have any content, or are noted as being under construction.[98] While parked or inactive domains are not usually mentioned specifically by ISPs as being a category of site which they block, we have found that it is common for such sites to be filtered. In some cases this may be due to the fact that a domain may have been used for some other purpose in the past, or it may be because the filtering provider is unsure how parked domains may be used in the future and chooses to block them as a result.

This filtering of inactive domains can cause problems for site and business owners who have obtained a domain and intend to use it to launch a site, only to find that their domain is already blocked and inaccessible to potential users or customers. Even worse is the fact that most ISPs do not make the blocking of parked or inactive domains clear in their policies, so a site owner may be unable to understand why the block is in place.

We should worry that the large scale presence of filters may cause a 'chilling effect' by creating an incentive for business owners to avoid certain domain names and branding that they suspect might be more likely to trigger the overzealous filtering of their websites.

We are also concerned that businesses and others who are in the course of launching new products or services may not wish, or may not be able, to disclose information about new products or services which may make use of new domains. Although reports to the Blocked tool can be submitted anonymously, businesses in such situations may still be unwilling to use the tool to identify whether their chosen domain is filtered, or to submit unblock requests, as doing so involves allowing the Blocked system to check the domain.

[98] *See for example the report for: https://www.blocked.org.uk/site/http://a1taxiservice.co.uk*

Overbroad blocking categories

Products already subject to age restrictions

As we mentioned in the introduction to this report, adult content filters were originally put into place for the purpose of protecting children from content which may be harmful to them. Although it is generally accepted that this includes pornographic content, some other categories of content are less clear and lead to inconsistencies in blocking.

For instance, alcohol and tobacco might be harmful to children physically, but they are also included in the categories of site which are blocked by most service providers. Many websites host content that deals with alcohol in some capacity. Often these sites belong to businesses such as pubs and breweries, or sometimes they are discussion sites or sites belonging to groups such as the Campaign for Real Ale[99] or the Leeds Beer Festival.[100] Many of these sites find themselves inaccessible for a large portion of UK users, as they deal with a topic which has been deemed to be potentially harmful to children. This means that the pages for pubs, breweries, and even beer bottle collecting enthusiasts[101] are amongst those which find their sites inaccessible in millions of homes around the UK.

Below is a table which displays the number of search results for sites in the Blocked database which use the following terms related to products which are already subject to age-restrictions: [102]

Keyword	Number of blocked results
airsoft	487
brewery	1638
casino	10,086
firearms	834
fireworks	103
vineyard	1063
whisky	1304

[99] *See: https://www.blocked.org.uk/site/http://www.camra.org.uk*

[100] *See: https://www.blocked.org.uk/site/http://www.leedsbeerfestival.co.uk*

[101] *See: https://www.blocked.org.uk/site/http://www.brewpalace.com*

[102] *These search results were gathered using the Blocked.org.uk search engine at the following link: https://www.blocked.org.uk/sites and are accurate as of the time of writing in March 2019.*

The above searches were carried out using the Blocked.org.uk search engine using single keywords only and were not manually filtered, so there may be some room for over, or under, inclusion of related URLs in the results above, but we feel that the keywords used are not terms which appear to return a large number of false positives.

The Blocked project has not been able to categorise every domain available on the Internet, so the results returned for each keyword are not exhaustive. They do, however, show that the filtering of sites dealing with goods already subject to age restrictions appears to be commonplace.

Do such filters really achieve their aim of protecting children? As discussed above, the potential result of being blocked is lost business for filtered sites, and yet it is difficult to see how filtering sites as a result of any minor relationship to alcohol, tobacco, or firearms can actively protect children. Children are unable to buy such products directly, as age verification measures are in place, and sites dedicated to the topics also generally contain useful and potentially relevant safety information which does not make sense to block.

If such blocks must exist, they should be limited in scope to avoid causing damage by overblocking. It may be possible to restrict alcohol blocks, for example, by limiting it to major alcohol brands and marketing sites, rather than using a wide 'alcohol' definition that includes village pubs, restaurants, and French vineyards. A list of major UK alcohol brands of potential interest to under 18s could be compiled quite easily, and might be restricted to a few hundred websites at most.

Some ISPs note in their filtering policies that they block sites relating to general categories of content such as "Alcohol and Tobacco". Although it may not make sense to filter sites which deal with goods for which age restriction is already in place, it may still be within an ISP's policy to filter wide categories such as the above, and we cannot therefore conclusively say that such filtering is overzealous. However, this raises an important divide between fixed ISPs who implement such policies, and mobile ISPs.

Filtering by mobile ISPs is overseen by the BBFC. In their Classification Framework for use in filtering mobile data networks, the BBFC specifically note that their guidance does not endorse filtering "sites which supply age restricted goods or services such as knives, fireworks, tobacco, legal highs, alcohol, gambling or adult entertainment", and that it is the retailer's responsibility to enforce effective age verification for such products.[103] As the BBFC note, this is something which is overseen by Trading Standards. This divergence of policy leads to a significant divide between mobile networks and fixed-line broadband services, who tend to operate under their own policies and frequently decide that such sites ought to be blocked. In order to take a consistent approach, it would make sense that content which is deemed as potentially harmful to children is not treated differently depending on which Internet service provider the user is attempting to access the site through.

[103] *"Framework | British Board of Film Classification." Accessed March 13, 2019.* http://www.bbfc.co.uk/what-classification/mobile-content/framework

Cannabidiol products blocked as drugs

Another frequently recurring issue that appears to highlight inconsistent filtering policies between service providers revolves around sites which sell Cannabidiol (CBD) oil and CBD-related products. Producing a list of sites which only sell CBD products is challenging, as many also distribute drug paraphernalia more commonly associated with illicit substances, which is likely to be the reason for the overblocking of sites in this category.[104] Nevertheless, businesses which only sell CBD products do exist, and we have received at least 21 reports from owners and users of sites of this type via the Blocked project over its lifetime. Cannabidiol is a food supplement derived from the cannabis plant. CBD does not contain any of the psychoactive compounds from the cannabis plant and it is therefore legal to buy and sell in the UK. CBD products are said to provide potential health benefits,[105] especially amongst sufferers of anxiety, epilepsy, and those who suffer chronic pain, and are sold in high street stores such as Holland & Barrett, and Boots.

Due to the relation between CBD products and the cannabis plant, many online retailers who advertise the product for sale have found their sites categorised as dealing with "drugs" and subsequently filtered. The filtering of such sites as "drugs" may lead business owners to lose sales, or lead potential site visitors to believe that the retailer is not trustworthy, despite the fact that the products are legal to sell in the UK. Meanwhile, ISPs have not blocked Holland & Barrett's website.

There appears to be a significant divide between service providers when it comes to how they treat CBD products. Some service providers classify CBD sites as "health" and choose not to block them, or unblock them upon request, and some providers insist even after a blocked site is reported to them that the "drugs" classification is correct and that the site should therefore remain blocked. This inconsistency between ISPs still seems to be present even when ISPs outsource their filtering services to the same third-party provider. We have found instances of Symantec categorising the same site differently between different ISPs: as either just "CBD", which does not lead to the site being blocked, or both "CBD" and "drugs", which leads to the site being blocked.

This inconsistent approach across ISPs, and even amongst ISPs who subscribe to the same third-party services, demonstrates the fallibility of this approach to content filtering. It is possible that reports for the same site are reaching Symantec via multiple ISPs, and the sites are being reviewed multiple times by different human reviewers, who are reaching decisions which are not necessarily the same as each other.

Commercial VPN services

Among the categories of frequently blocked site that we have encountered, we find commercial VPN services

[104] *With the above caveats in mind, a list of sites in the Blocked database which match the keyword "CBD" may be viewed at: https://www.blocked.org.uk/list/CBD*

[105] *Halperin, Alex. "What Is CBD? The 'miracle' Cannabis Compound That Doesn't Get You High." The Guardian, May 28, 2018, sec. Society. https://www.theguardian.com/society/2018/may/28/what-is-cbd-cannabidiol-cannabis-medical-uses*

are very frequently blocked.[106] Commercial VPN services are usually paid services which allow users to encrypt their Internet traffic and route it through servers in different locations. This is typically done for privacy and security reasons, or to access resources which are blocked on the basis of a user's IP address.[107] VPN services could, however, be used to circumvent adult content filters by allowing users to encrypt their Internet traffic. This leaves filters unable to determine which sites are being visited, and therefore unable to block sites which would normally be filtered.

Commercial VPN services raise particular issues for content filters and fairness. For the purposes of protecting children from accessing adult content, blocking paid commercial VPNs can be said to do very little. As most services require payment to access, the likelihood of children being able to utilise them to circumvent content filters is low. Additionally, any child with enough determination to acquire access to paid VPN services will be able to circumvent filters in a number of different ways.

The BBFC appear to recognise this, as they will instruct mobile operators to unblock commercial VPN services when they receive reports that operators have refused to unblock them. This highlights some further issues. Firstly, this suggests that, as mobile operators do frequently block such services, they are not actually currently blocking to the BBFC's standards. It also shows that even when the BBFC have repeatedly adjudicated upon blocking decisions and instructed mobile operators not to block commercial VPN services, the mobile operators have not adjusted their filters accordingly to ensure that other services of the same type are also unblocked. They appear to be waiting for adjudications from the BBFC and unblocking sites on a case-by-case basis rather than taking sensible proactive action.

Secondly, this highlights a failing in the communication of the BBFC appeals process to business and website owners in the UK. We feel it is fair to conclude that many commercial VPN operators are not aware of the BBFC appeals process or the fact that they have the right of appeal, otherwise we would not expect to see so many of these services still being filtered by mobile networks. We explore appeals processes in more detail below.

VPN and remote access software

While content filters often block access to sites which offer a commercial VPN or proxy service, as already discussed in this report, we have also found evidence that many filters also block sites that use similar keywords but do not directly belong to VPN or proxy services themselves. Examples of this include:

- WonderProxy[108] - a paid service which allows website owners and administrators to view how their site looks from different countries around the world: and

[106] *Our research showed that nine of the "top 10" ranked commercial VPN services tested by Top10VPN were blocked by one or more ISPs at the time of writing in March 2019.*

[107] *Resources are typically blocked by checking whether a users' IP Address belongs to a particular geolocation. Security considerations can be as simple as reducing risks from using public wifi, including viruses and malware attacks from other users.*

[108] *See: https://www.blocked.org.uk/site/http://wonderproxy.com*

- PiVPN[109] - which provides software for a user to set up their own VPN server and is not providing any VPN or proxy service of its own.

We have found evidence of some ISP content filters blocking sites offering remote access services such as TeamViewer[110] and join.me[111]. Remote access services are widely used by companies to facilitate remote working for employees, or to enable remote access to their computers for IT purposes.

Mobile operators are not meant to block commercial VPN providers according to BBFC guidelines, however they frequently do. This is discussed below.

Blocks are not being adequately maintained

In an earlier section, we discussed the prevalence of pre-launch blocks or, in other words, sites which are blocked before they become operational. This is often as a result of the domain previously holding content which would fall into an ISP's blocking policy, or parked domain pages.

ISPs often block parked or inactive domains, domains sometimes change hands and function. This raises an important concern around ongoing maintenance of blocks and filtering lists. Unless blocked sites are periodically reviewed and filter lists actively maintained, blocks can remain active for a long time, even after a domain has changed ownership or changed the type of content it displays.

For ISPs to ensure that they remain responsible, they should ensure that blocking and filter lists are reviewed continually and that sites are periodically assessed to ensure that it is appropriate for them to remain filtered.

Unblock request findings

We allow users of the Blocked.org.uk site to submit requests to ISPs for sites which they have blocked to be reconsidered and potentially reclassified. We have assigned categories to these reports to show who has requested the unblock, and whether their report directly references any damage which they feel has been caused by the site being filtered.

Replies to unblock requests

Blocked tracks the unblock requests sent to individual ISPs, and their response rate. For this, we were interested in graphing two primary things: the number of unblock requests which ISPs replied to, and how quickly they replied.

---

[109] *See: https://www.blocked.org.uk/site/http://pivpn.io*

[110] *See: https://www.blocked.org.uk/site/http://www.teamviewer.com*

[111] *See: https://www.blocked.org.uk/site/http://join.me*

We measured the time taken for an ISP to reply to requests rather the time taken for an ISP to "unblock" a site, as a site becoming unblocked is is not always the result of the ISP's own actions. Many ISPs subscribe to the same third-party filter list providers and when one ISP refers a site to the filter provider for re-categorisation, it often results in the site being unblocked on all ISPs who subscribe to the provider's filtering lists. We believe that the time taken for an ISP to reply is roughly equivalent to the time it takes for an ISP to remove a block, or to refuse to remove it.

The below graph demonstrates the time it takes ISPs to reply. ISPs do reply to unblock requests, they generally reply within 2 weeks.[112] We can see this is fairly consistent between 2018 and 2019, although we acknowledge that we do not have enough data from 2019 to begin establishing trends. In addition, two ISPs (Virgin Media, Vodafone) have not yet replied in 2019.

How long do ISPs take to reply to unblock requests? (days)

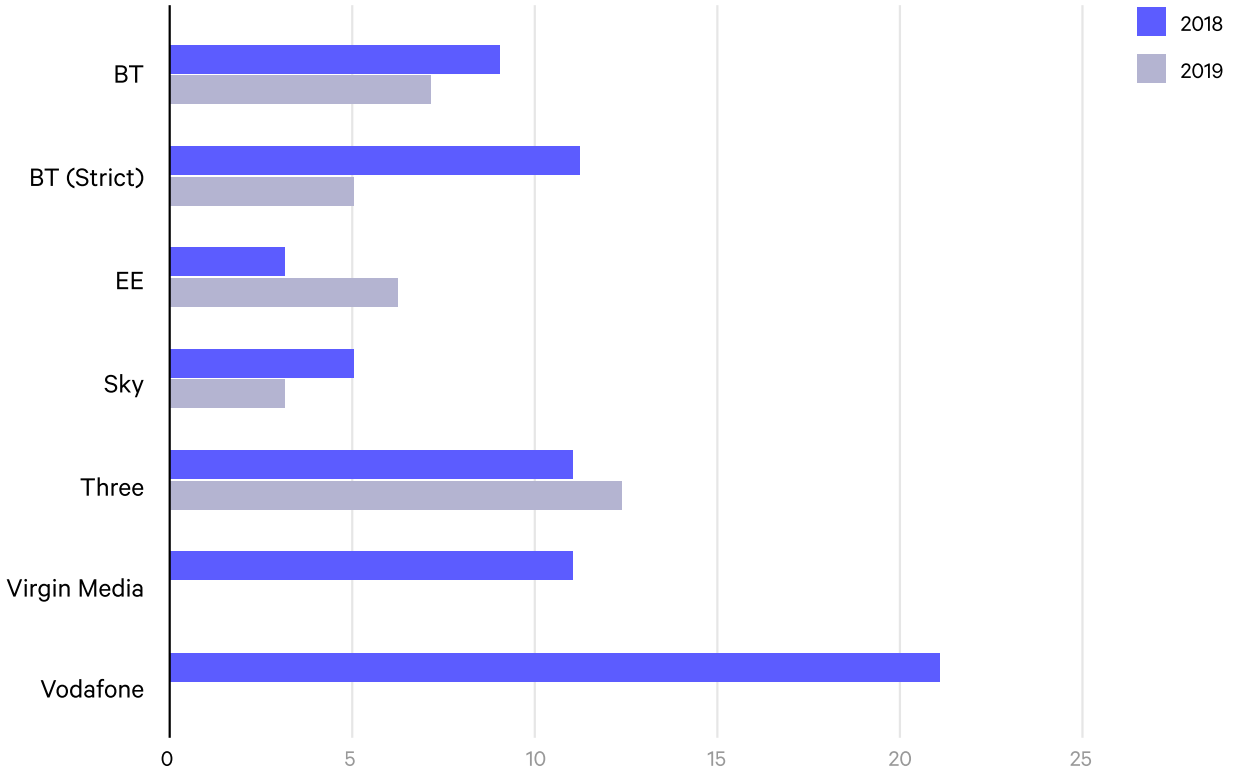

Fig 1: Time taken for ISPs to reply to unblock requests, measured in days.

The above graph does not contain data from some ISPs in an effort to avoid misrepresenting their response times. We have found that TalkTalk and Plusnet have not responded to unblock requests sent via the Blocked tool. TalkTalk are currently investigating this. We discovered O2 were using the email addresses of users

[112] *For more information about the calculation of ISP reply interval statistics, please see Appendix B of this report which provides further detail on our methodology.*

submitting unblock requests to reply to them directly, rather than replying via our Blocked tool. This means that we have been unable to capture O2 responses to unblock requests. We have discussed this with O2 and have subsequently removed the feature that displays the email address of the user submitting the original unblock request, to ensure that future ISP responses are sent directly via the Blocked tool for us to record.

We can see from the above data that in 2018, ISPs took an average of 8 days to reply to unblock requests submitted through the Blocked tool.[113]

As we have demonstrated above, the overblocking of sites can cause harm to owners and users of those sites. Because of this, it is vital that service providers promptly acknowledge and reply to unblock requests. We would suggest that users reporting wrongful blocks should expect to receive a reply within a fixed time frame - ideally no more than 48 hours. The data above demonstrates that ISPs have room to improve the rate at which they reply.

Despite the average ISP reply time being around 8 days, we found that even as we compile this report in March 2019, a large segment (3 out of 10) of the total unblock requests submitted to ISPs during 2018 are still awaiting a resolution:

What proportion of unblock requests from 2018 are still unresolved?

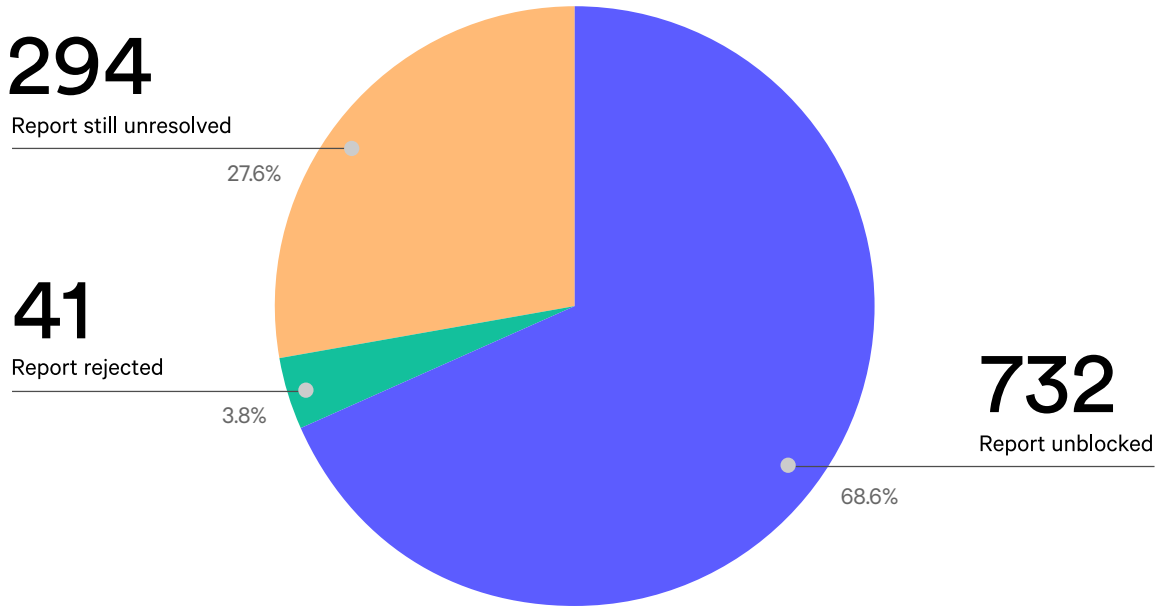

Fig 2: Unresolved report status for unblock requests forwarded to ISPs during 2018.

For the purposes of compiling the above graph, we treated reports as “unblocked” where the ISP did not reply but did still unblock the domain as requested. This was in an effort to avoid unfairly treating ISPs who did

[113] *This figure is calculated using the response time for responsive ISPs (BT, BT Strict, EE, Sky, Three, Virgin Media, Vodafone) and uses reply-time data from 2018.*

unblock sites as requested, but did not confirm the fact by email for any particular reason. Therefore, reports which we consider as “still unresolved” are those for which an ISP both did not respond and where we also did not detect that the site has been silently unblocked.

The majority of unblock requests do receive replies, but we have identified a number of issues preventing the submission of unblock requests from being a reliable method of recourse for those affected by blocks. In particular, the system is fragile. ISPs do not always reply to unblock requests reliably, and reply rates differ by ISP. We find that this occurs despite all ISPs involved having an awareness of our Blocked project and how it functions.

After graphing the above, we considered that it was possible that the unblock requests which were still awaiting resolution by ISPs months later were for domains which were clearly pornographic or otherwise spam or misuse of the Blocked tool to submit unblock requests for obviously correctly-filtered domains. However, when we graph the proportion of domains which had not received a reply as of March 2019 based on whether the domain is filtered in-line with ISP policy or against ISP policy, we find that this is not the case:

What proportion of unresolved blocks are not within ISP policy?

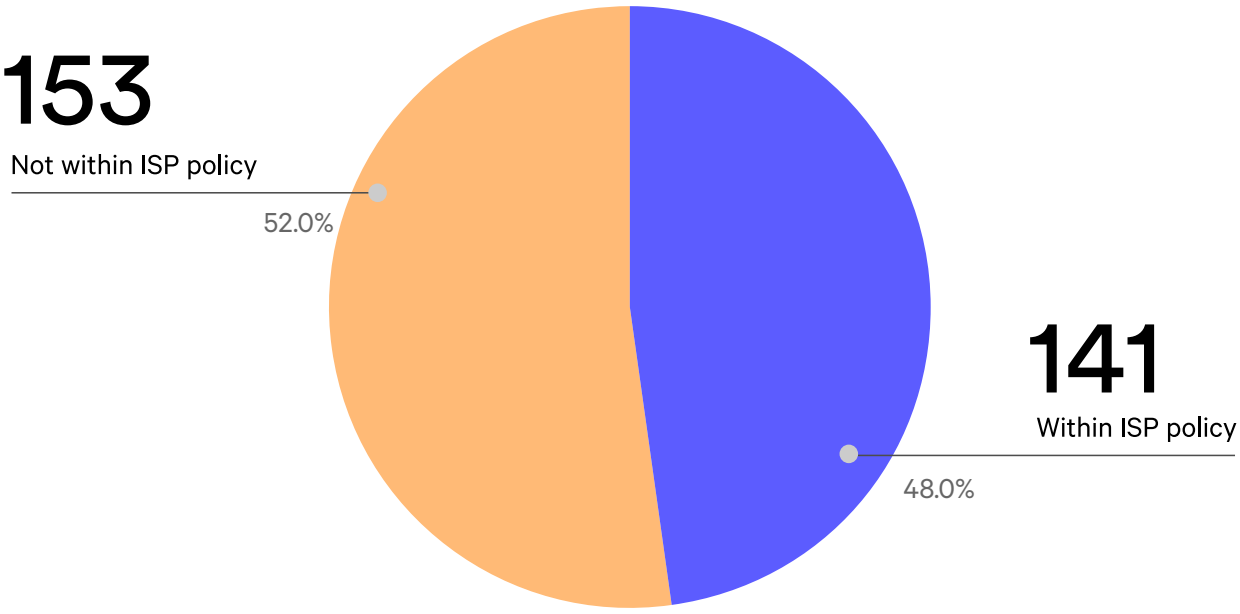

Fig 3: Unresolved reports for 2018 which are/are not within ISP policy to block.

Of the 294 unblock requests from 2018 which were still left unresolved as of March 2019, we discovered that more than half (153) of these requests were for domains which did not fall into any of the categories of content that the ISP blocked by policy, and should have been unblocked upon request. This suggests that some reports are simply not dealt with at all.

We are able to further break-down this data and analyse per-ISP the proportion of unblock requests submitted

in 2018 which still remained unresolved as of March 2019:

What proportion of unblock request is each ISP leaving unresolved?

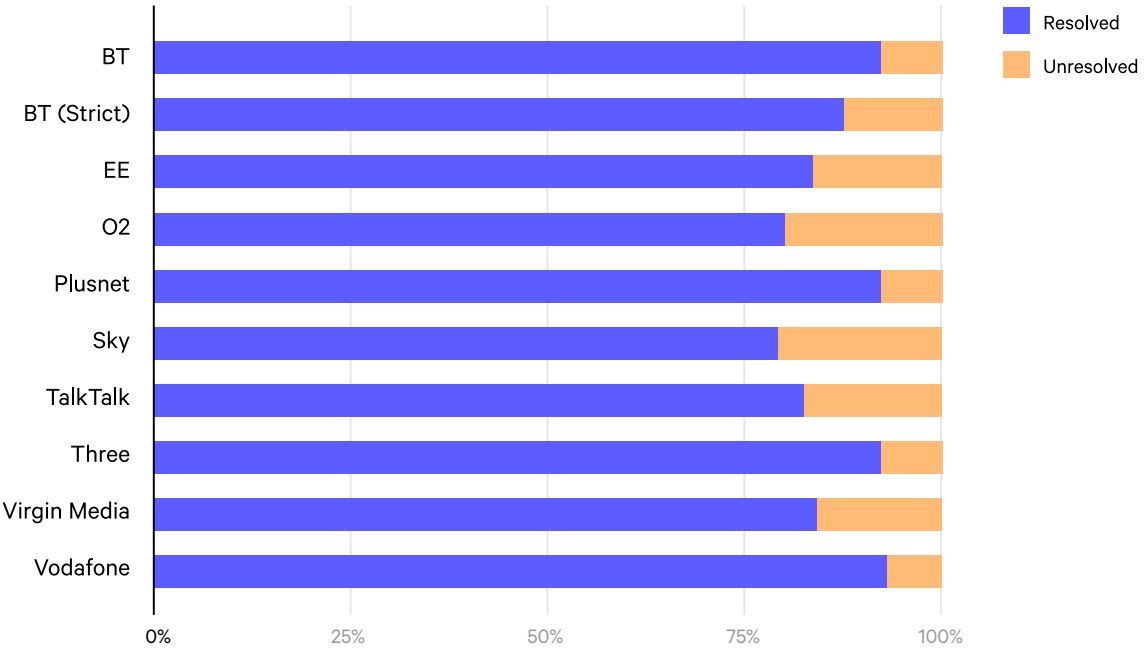

Fig 4: Status of unblock requests forwarded to ISPs in 2018, as of March 2019.

For the purposes of the above graph, the figure used for "unresolved" unblock requests is the number of domains which not only have not received replies, but are also not within ISP policy to block. As the graph shows, all ISPs are resolving the majority of unblock requests forwarded to them via the Blocked tool.[114] Despite this, no ISP is free from leaving some number of reports unresolved. We feel this is an inevitable consequence of ISPs relying on an email-based system for users to report erroneous blocks. Email-based systems can result in requests getting lost or misplaced and are often hard to track accurately, as we feel this data shows.

Some ISPs leave some unblock requests without reply in situations where the site is clearly pornographic or otherwise within the scope of their filtering policy. However, it remains concerning that some of our forwarded unblock requests are still finding themselves lost or left without reply despite not falling within the ISP's policy. With the Blocked project we have, in effect, built the missing ticketing system for users and site owners who are interested in ensuring that overzealous blocks are reviewed and lifted where appropriate. However,

[114] *Since we consider sites to be unblocked where it appears they have been 'silently' unblocked without the ISP actively sending back any reply to the Blocked tool, some ISPs may 'overperform' in our statistics as a result of outsourcing their filtering processes to third-party providers. For example, if more than one ISP subscribes to the same third-party filtering service, then an unblock request forwarded to the third-party service by just one subscribing ISP could lead to the site in question being unblocked across all of the ISPs who subscribe to that service. This is a limitation of our data collection process, though we do not believe it meaningfully impacts the quality of our data. The unblock requests which are left "unresolved" are of most consequence to us.*

since the Blocked project is forced to rely upon email as a means of forwarding unblock requests to service providers, we are still finding a lower rate of issue resolution than would be desirable.

We would ask that ISPs engage openly with the Blocked project and work to ensure tighter integration with our system to allow it to operate like an efficient ticket-based issue resolution process, ensuring that unblock requests are not being lost or forgotten about. ISPs could also take steps to create their own ticket-based systems for submitting requests to unblock wrongfully-blocked sites, although we would caution that it is desirable for a user or owner to be able to check a site's status across multiple ISPs at the same time, rather than needing to test their site individually across many ISP systems.

Sources of unblock requests

The use of the Blocked tool by site owners looking to unblock their own sites has increased over time. Site owners are becoming increasingly aware of the issues with adult content filters and are turning to our tool to try and resolve them. We processed a total of 1,880 requests to unblock sites between 2017 and the publication of this report.

Among the reporters in 2017 and 2018, we can see in the graphs below that a majority did not state whether they had an affiliation with the site in question. As we have initially popularised and promoted the tool within our own membership, we can assume that the majority of Blocked users in this category are digital rights activists or ORG members. But we can see that between 2017 and 2018, the proportion of reporters who fall into this category fell, as the number of site owners reporting their own sites for unblocking rose notably.

Who submitted unblock requests using Blocked.org.uk in 2017?

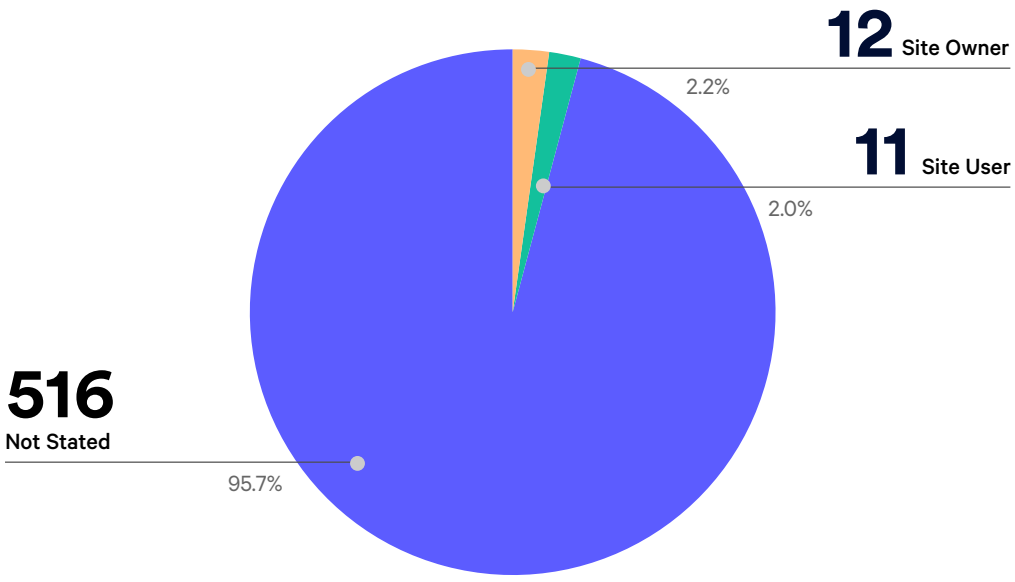

Fig 5: Blocked.org.uk unblock requests categorised by reporter affiliation (2017).

Who submitted unblock requests using Blocked.org.uk in 2018?

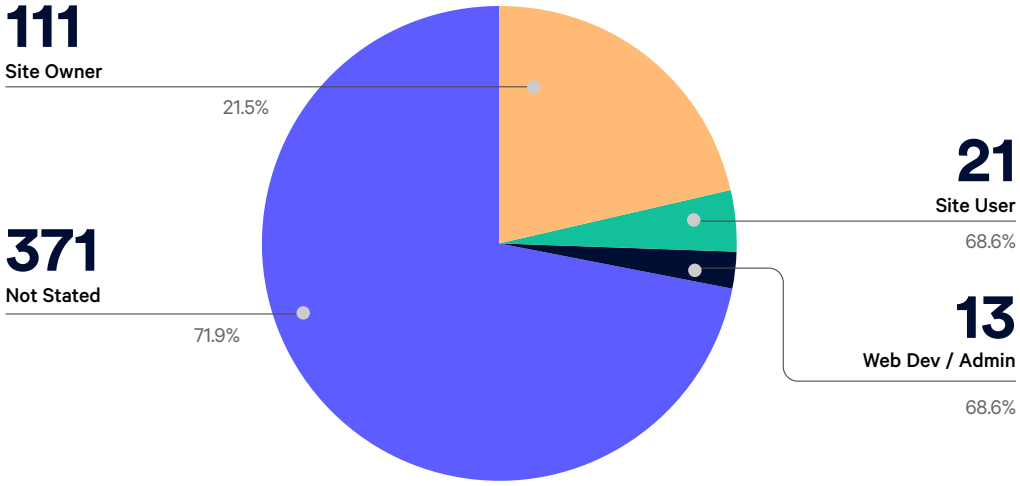

Fig 6: Blocked.org.uk unblock requests categorised by reporter affiliation (2018).

As the Blocked tool grows in popularity, we can see our user profile for the site is shifting. More site owners, site users, and web developers and designers who manage sites for clients are turning to it to submit unblock requests. This means that more users of the tool are identifying themselves as being directly affected by content filtering.

When we specifically break down reporters who did identify themselves when submitting reports, we find that a vast majority (75%) of users of the Blocked tool now identify themselves as the owner of the site in question. Combining this with the figure for reporters who identified themselves as web developers or managers working on a blocked site on behalf of a client, we see that 8 out of 10 of those who identified themselves to us when submitting unblock requests had a direct affiliation to the site in question. This is detailed in the graph below:

Among people who identified themselves, who is submitting unblock requests via Blocked.org.uk? (Data from all-time)

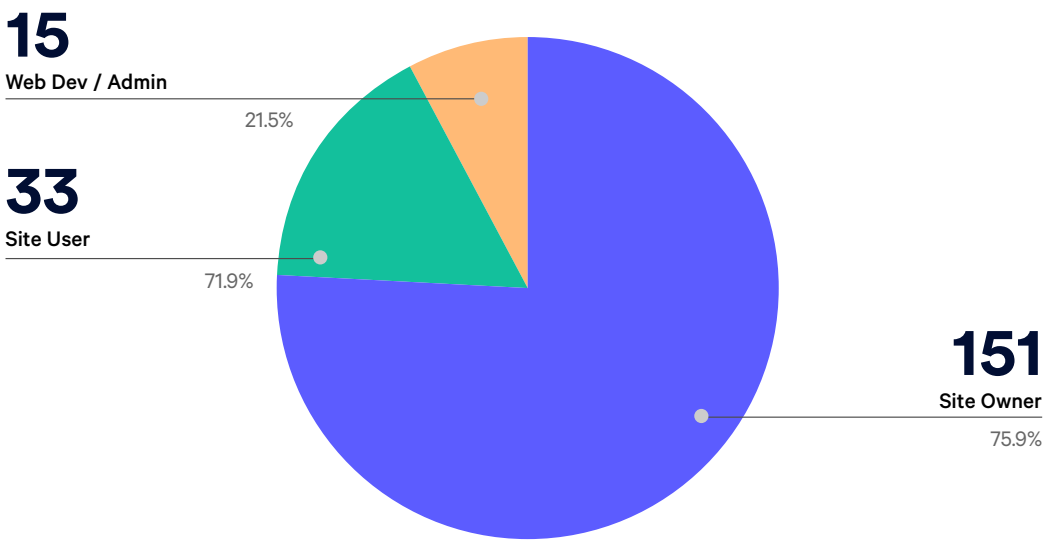

Fig 7: Blocked.org.uk reports divided by reporter (known reporters only, data from all-time).

The high proportion of reports being submitted by those directly affiliated with blocked websites suggests that site owners and maintainers are increasingly concerned with web filters and with ensuring that their site remains visible to as many people as possible.

When we further break down the reports submitted directly by site owners, we begin to notice an interesting trend. Nearly 70% of unblock requests sent by owners of blocked sites were related to sites which were part of a business. A further 16% belonged to groups like charities and campaigns. The smallest category belonged to owners of personal sites, with less than 16% of reports coming from a personal site which had been filtered. This data can be seen in the graph below:

Among reports from site owners, what type of site do they own?

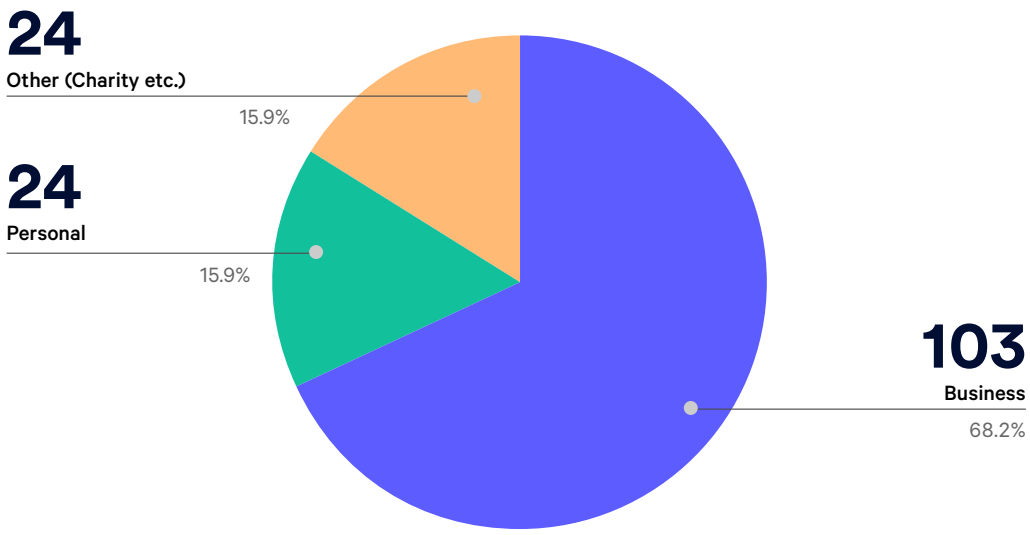

Fig 8: Blocked.org.uk reports by site owners - broken down into type of site.

One thing we may conclude from this is that the owners of non-business sites are possibly at risk of being more frequently subject to erroneous blocks which remain in place long-term. It is possible that the lower proportion of personal sites being reported for unblocking indicates that the owners of small personal sites and blogs are less aware of the fact that their site may be filtered by some ISPs than business owners may be. Business owners are likely to have customers who they are in personal or face to face contact with. Those customers will use many different ISPs so businesses are more likely to be notified by their own customers about erroneous blocks if they arise. Business owners also have a financial incentive to proactively check that their sites are not being unfairly caught up in adult content filters, for instance through the Blocked tool. Personal site owners are not as likely to have this kind of insight about potential issues with adult content filters.

Similarly, the owners of small personal sites may not feel as empowered to take action and have their site reviewed by ISPs. They may feel that judgments taken by the ISPs filters are not open to challenge and as a consequence may not actively seek out methods of recourse for wrongful blocks, which may otherwise have led them to the Blocked.org.uk reporting tool.

Damage cited by Blocked.org.uk users

We have found that when business owners file reports using the Blocked tool, many include content in the text of their reports which indicates that they feel damage is being done to their business by the filters. We analysed these reports and categorised them based on the most common reports we received. That data can be seen in the graph below for reports that were submitted in 2018.

What damage are Blocked.org.uk users indicating in reports?

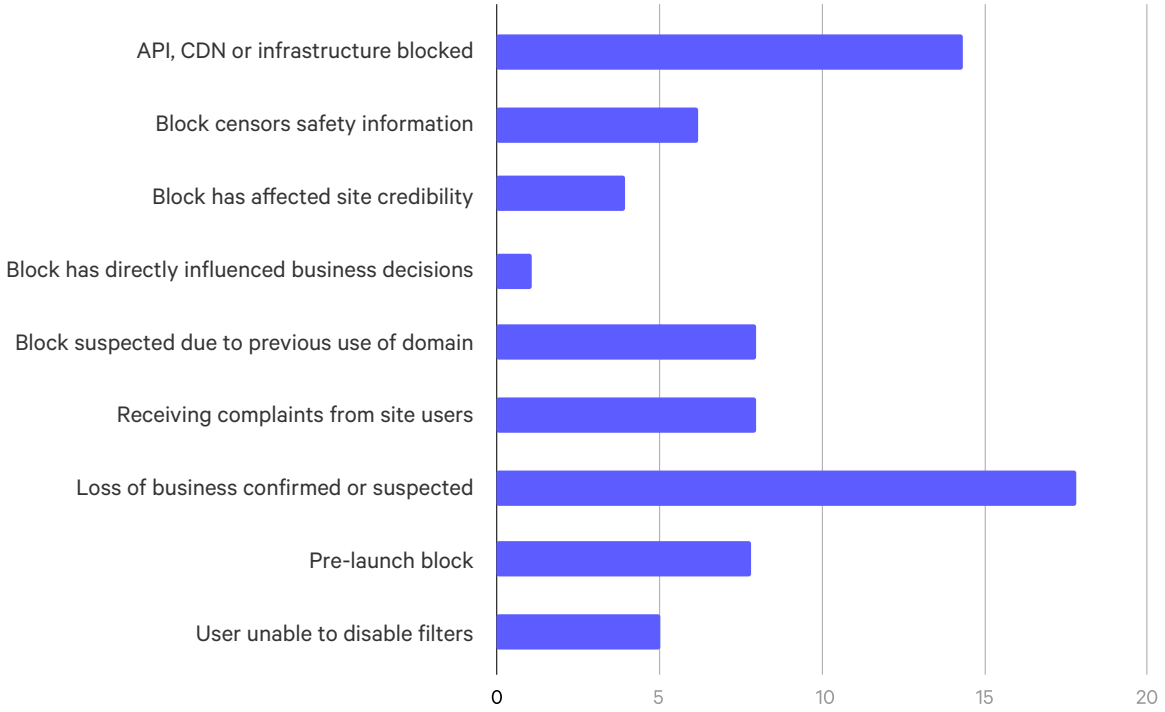

Fig 9: Damage as indicated by those submitting unblock requests via Blocked.org.uk in 2018.

The above shows it is quite common for site owners to reference the fact that they suspect business is being affected by the blocking of their site. This can be either referenced directly - which we found to be the most common recurring theme in reports from site owners - or it can be indirect, for instance the site owner noting that they suspect the block has negatively affected the credibility of the site, or that users of the site have been complaining they are unable to access it.

We also see reports that sites are being filtered before they have been officially launched, or before the site holds all of the content. Blocks of this type can be particularly disruptive to the launch of new sites or products and could have a direct impact on businesses if they have to wait for unblock requests to be resolved by ISPs before publicising the launch of a new domain.

Finally, we discovered one particular instance of a blocked online shopping retailer referencing in their unblock request that they had directly taken the business decision to stop selling adult toys on their site as a result of the adult content filters. For the retailer, they felt the block was negatively impacting business so it directly

influenced their business decision to discontinue the sale of such products.[115] Similar products to those which were discontinued by the retailer are available from Amazon, which is not currently filtered by any ISP.[116]

One limitation of our current approach is that our categorisation of reports in this fashion is limited to situations in which the reporter has specifically referenced damage within the text of their report. For this reason, it is a minority of overall reports which we are able to categorise specifically by what damage has been reported.[117]

Mobile network inconsistencies

Among the domains categorised by the Blocked tool, we identified that there was a significant level of inconsistency in the filtering being applied among the mobile network providers we tested. This is notable since mobile operators are voluntarily subject to a classification framework for Internet content filtering which is administered and overseen by the BBFC. The mobile networks do not decide directly on the categories of site which should be blocked as unsuitable for children, but instead follow the BBFC's framework when deciding whether sites should be filtered for mobile users who have adult content filtering enabled. In theory, this therefore means that all mobile networks should be filtering based on the same standards, and the list of sites blocked on any mobile network should be mostly comparable to the sites blocked on the other mobile networks.

However, what we see when processing the blocked sites in our database is a high level of inconsistency between providers. This is detailed in the graph below:

How many mobile networks are filtering each blocked domain in our database?

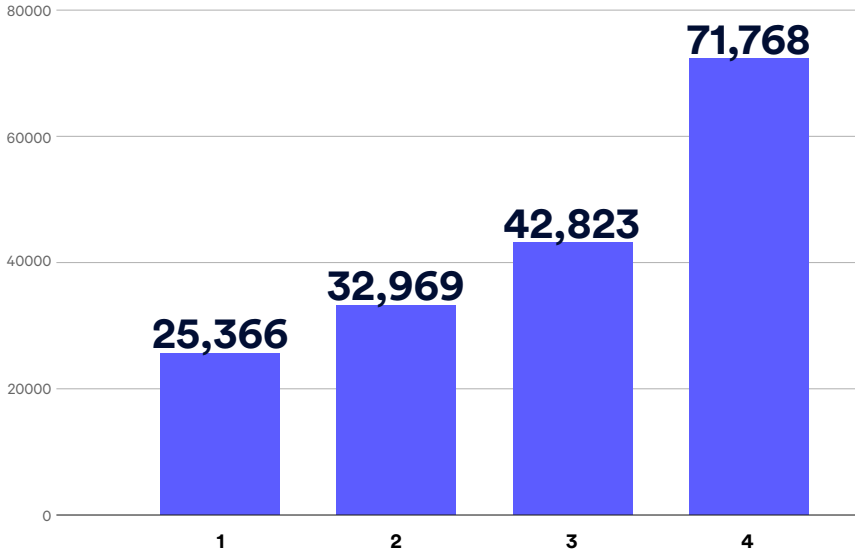

Fig 10: Number of mobile networks blocking each filtered domain in our database.

[115] See: https://www.blocked.org.uk/site/http://britishcondoms.uk

[116] See: https://www.blocked.org.uk/site/http://amazon.co.uk

[117] *In the future we may wish to explore options that would allow users to select from a list of possible categories of damage to report. We would, however, need to ensure that this did not unduly skew results by prompting users to report certain things, or by making users less likely to include details about other categories of damage which we did not already have in our list.*

What we would expect to see from the graph above, if the mobile network operators were consistently applying BBFC Classification Framework standards, is that almost all filtered sites would be filtered by all four of the mobile networks we tested, and that the number of sites filtered by fewer than all four networks would be within a reasonable margin of error. Instead, what we actually see is that - while the largest number of filtered sites are indeed filtered by all four mobile providers - there is a large number of sites which are filtered by only three, only two, or only one of the four networks we tested.

When totaled up, the number of domains which are blocked on fewer than all four mobile networks reaches 101,158 - compared to the 71,768 domains which are filtered by all four providers. When it comes to mobile network filtering, inconsistency is the norm rather than the exception.

Complaints and appeals

BBFC appeals process

Where a mobile operator has been informed of the fact that a site has been blocked in error, but has not taken any action to unblock the site in question, a user or site owner can appeal directly to the BBFC, who will consider the merit of the unblock request.

Upon appeal, the BBFC will review the content and decide whether the block is justifiable, or whether the site should be recategorised and unblocked. The BBFC aims then communicate its decision to the appellant, and the mobile operator(s) involved within 5 working days.

As part of the analysis we have conducted, we have noticed that in their replies to users who have reported sites via the Blocked.org.uk tool, mobile service providers do not always provide information about the user's rights with regard to appeals via the BBFC. We have found that mobile operators sometimes mention that a user may wish to contact the BBFC directly if they are dissatisfied, but the operators do not appear to include specific contact information, or sufficient detail about the BBFC appeal process.

We would call upon these operators to ensure that this information is included in the body text of their reply emails in a transparent and easy to understand manner. We have included some example body text for this below, which is largely based on the text available on the BBFC's appeals page:[118]

> *If you are unsatisfied with the outcome of this unblock request, you have the right to contact the BBFC for an adjudication. You can do so at:*
>
> *https://www.bbfc.co.uk/mobile-complaint*

[118] *"Appeals and Complaints | British Board of Film Classification." Accessed March 13, 2019. https://www.bbfc.co.uk/what-classification/mobile-content/appeals*

*Disallowed categories include: Suicide and self-harm promotion; Discriminatory language; Promotion, glamorisation or encouragement of drug use; Repeated / aggressive use of 'c**t'; Sex works; Fetish material; Adult Sex education and advice; Violence and Horror. Full details of what is allowed and disallowed on filtered mobile networks can be found here:*

http://www.bbfc.co.uk/what-classification/mobile-content/framework

On receipt of a valid written appeal request, the BBFC will ensure that the site, or the relevant parts of the site, is viewed by the BBFC Mobile Content Appeals Committee, made up of senior members of the BBFC.

The BBFC will consider any written representations made by you or any other interested party.

The BBFC will communicate the outcome of the appeal to the you, the mobile network operator and such other interested parties as the BBFC considers appropriate within 5 Working Days, provided there is no need to seek views from legal and / or other external advisers, in which case such views will be sought and considered as soon as is reasonably practicable.

Site owners are not accessing the appeals process

We identified a number of complaints made through our system where an ISP responded with a decision which did not appear to be in line with the BBFC's Classification Framework. As site users and owners are not being empowered to make use of the BBFC's appeals process, the end result is a large number of sites that could be unblocked on mobile networks will remain blocked. This is in part because the system is cumbersome, and in part because the mobile operators are, as discussed, not clearly communicating the existence of the BBFC appeals procedure to complainants.

From the complaints we have seen, it is clear that mobile network operators are not applying BBFC standards accurately and do not adjust their policies to reflect BBFC guidance. The same kinds of mistakes repeatedly made. For instance, upon appeal, the BBFC will suggest that commercial VPN sites should not be blocked, and will instruct mobile operators accordingly to unblock them. However, mobile networks do not appear to be taking this feedback from the BBFC on board in a broader sense by acknowledging the BBFC policy and proactively unblocking all VPN sites in their filter, and instead are treating such adjudications on a case-by-case basis and only unblocking single domains. As a result, we have a mix of VPN sites that are sometimes blocked on mobile networks, and sometimes unblocked.

In some cases this is because filters are incapable of contextual judgements. BBFC's guidance in these cases may be hard to apply, although effort could be made. In other cases, classification is entirely technically possible, but possibly commercially undesirable. For instance a search for "VPN" on Blocked.org.uk would give mobile operators a list of 3-400 VPN sites they could review and remove from their blocking lists.[119]

[119] *See non-exhaustive list at: https://www.blocked.org.uk/list/VPN*

Lack of appeals process for fixed-line ISPs

Virgin Media, TalkTalk, Sky and BT do not offer an appeals process. Their processes refer a complaint to their content review company, but the decision of the third party is viewed as final. The ISPs will not engage in further dialogue with a site owner or user.

We identified at least 197 sites that appear to have remained blocked after unblock requests have been submitted to fixed-line ISPs, despite their content seemingly not falling within the categories of content which the ISP blocks as per their filtering policy. However, the lack of an appeal process for fixed-line ISPs means that these sites will remain blocked.

This approach stems from the fact that there is no clear standard for the blocking, but rather it is a product bought from a third party. Even despite their specialism in the area, however, we have identified a number of complaints where the external suppliers appear to make categorisation errors.

For instance, The Suicide Project, which identifies itself as a site where people struggling with suicide-related feelings can share stories of desperation, depression and hope and "find a reason to live, a reason to survive another minute. Another hour. Another day". In response to an unblock request for the domain in question, one ISP replied that their third party filtering provider had analysed the site, and subsequently recategorised it as "Leisure & Recreation". Whilst this did lead to the site being unblocked, the apparent short-sightedness of the site's new classification leads us to question just how much time third-party providers spend reviewing each site.

We believe that it would make sense for the 'recommended' blocking option to be a matter of clear policy, such as that of the mobile networks 'under 18' standard operated by BBFC. The standard could then be seen to have some kind of objective test, for which an appeals process could handle complaints.

Unclear replies from ISPs

While processing replies from ISPs to unblock requests submitted via the Blocked tool, we have encountered some patterns with ISP responses which lead us to be concerned about a lack of transparency around the decisions ISPs make when sites are referred to them as wrongfully blocked.

For example, during our testing we encountered one report for a questionable URL, for which BT returned an email with only the following body text:

> *"Thank you for your email and feedback regarding [reported URL].*
> *The URL is currently correctly categorised as entertainment."*

This provides the reporting user or site owner a very unclear picture about the action an ISP has taken with regard to their complaint. It indicates how the ISP or third-party filter list supplier has categorised the site, but

does not indicate what, if any, action has been taken in response to the user's report.

In contrast, the same report garnered a more comprehensive and understandable response from EE, who replied:

> *"I have checked the classification of [reported URL] with Symantec who classify websites on EE's behalf and they say that the site is correctly classed as 'Pornography' category website which means it can only be seen by adult EE users who have turned their parental controls off.*
>
> *"Symantec added that the site allows users to hire Male Strippers and this falls under our Pornography category."*

The above text makes much more clear that the user's request to unblock the site was rejected, and indicates the third-party provider's reasoning why the site will retain its current classification and remain blocked for users with filters enabled.

ISPs should ensure that they provide clear communication of any decisions taken, and an explanation of why they, or a third-party provider, has determined that a site falls into a specific category.

The future of web filters

Filters may get broader, less effective and less transparent

As sites on the Internet increasingly make use of encrypted HTTPS traffic, filters are becoming more indiscriminate. For instance, while it's possible to block sections of a website which serves content over plain HTTP, a filter must decide to block the whole of an HTTPS website. This means that filters will begin to increasingly over-filter, blocking more material than is necessary as a result of needing to filter entire domains. This is already apparent in the fact that only BT's 'Strict' filter blocks the primary domains for Twitter[120] or Reddit[121], and no ISP appears to restrict access to Imgur.[122]

Users are shown security warnings by web browsers when pages are served at HTTPS links that are not from the original site in question. This means that ISPs are unable to place block pages on filtered domains which use HTTPS. For a project like Blocked.org.uk this means we may have less information about website blocks over time, and may need to infer blocks for instance from non-responses at website URLs. For website

[120] *See: https://www.blocked.org.uk/site/http://twitter.com*

[121] *See: https://www.blocked.org.uk/site/http://www.reddit.com*

[122] *See: https://www.blocked.org.uk/site/http://imgur.com*

owners, this will also make it harder for their visitors and customers to understand why a website is not responding; they may assume the website is broken, rather than that it is filtered incorrectly. This means that transparency measures such as discovery through Blocked.org.uk or ISP databases of blocked sites are even more important.[123]

Implementing network-level filtering may become harder for ISPs over time, depending how DNS evolves. Most ISP filtering is currently carried out by ensuring that DNS servers operated by the ISP do not return accurate results when a user with filters enabled attempts to visit a blocked domain. Some ISP filters also make use of methods to stop savvy users from using alternative DNS servers to bypass filtering. This is likely to become harder to sustain, as it relies on the fact that DNS responses are unencrypted, and DNS servers which supply results over encrypted links are beginning to increase in popularity.[124]

The technical challenges above will continue to make network-level filtering increasingly difficult, and suggest that shifting a focus towards device-level controls is likely to be sensible, as these allow more granular control than network-level blocks.

Filters can have low rates of error correction

Across the blocks we have detected and curated as lists of likely errors.[125] The rates of error correction vary. Sometimes, most blocks seem to be removed over time, while elsewhere, they are not. While we do not know how errors are corrected, it may be that products rely on user reports to remove blocks. People may be more keen to report some kinds of error than others. This is suggested by the kinds of reports made through our own tool, which shows that business users are keen to report, and that instinctively 'unfair' blocks applied to charitable websites are more likely to be reported than for more special interest sites. Many websites may only be published for a few years, meaning a categorisation error may persist for most or all of its lifespan.

Filters are poor products with little incentive to improve

The aim of this research was to understand how filters cause damage, and who suffers that damage. However, we can also make some observations about what filtering is at this point in time.

1. Filters are inaccurate and error-prone across many kinds of content, rather than just a few. Many mistakes seem simply inexplicable.
2. Seemingly, a small amount of inappropriate content may trigger a filter.
3. Some categories of error, such as the blocking of wedding and photography sites, seem both hard to

[123] *This issue is discussed in more detail in Appendix C.*

[124] *Encrypted DNS services are already provided by companies such as Cloudflare and Google, and support for these is available natively in the Mozillla Firefox web browser and recent versions of Android.*

[125] *See: https://www.blocked.org.uk/lists*

explain and persistent. This implies that there is little interest in improving the technology.

4. The commercial imperative would seem to be to limit children's access to inappropriate material, rather than accuracy.

5. Filters will be more prone to correction when sites are seen by many people. For smaller websites, however, the chances that errors are not corrected except by the owners themselves is much greater.

6. Human intervention in filters is expensive, so this is avoided, shifting the burden of error correction onto filter users and site operators. Site operators are not in most cases given easy tools to check when they are being blocked, except in O2's case and through ORG's efforts.[126]

7. The Internet is a moving target. Sites often have short lifespans, and domains are recycled. Automatic indexing and re-checking of sites is likely to be the main task for filter providers.

The incentives seem to give little reason for filtering technologies to improve. The assumption appears to be that mistakes are both inevitable and somewhat unimportant: a reasonable assumption if the use of filters is restricted to children whose parents can resolve errors.

[126] *Some large filter companies do allow URL checking, for instance OpenDNS.*

Conclusion

Filters are an attempt to use technology as a quick fix for a complex social problem. This approach was always going to be flawed and it is time that the Government reviewed it objectively.

Keeping children safe, both online and off, should be a priority for the Government. But there is no evidence that filters are succeeding in their objective of preventing children from seeing adult content, or keeping them safe online. Parents are being misled, children are being encouraged to circumvent technology, and a whole range of businesses and organisations are being harmed.

Using filters is the prerogative of any parent, but ISPs have a duty to make their customers aware of the limitations of filters and promote other ways of keeping children safe online. This includes explaining that device-level filters aimed at individual needs are more likely to be suitable than whole-home products.

It is clear from our research that blocking errors are widespread and affect many kinds of content. It is also clear that trying to categorise all content on the Internet cannot be done accurately within current technology, not least because content is constantly changing. The only practical way to limit the harm of filters is to restrict their use. Indeed, the breadth of restriction they impose is cited as a factor that prevents parents from using them.

We also need rigorous research into whether filters are meeting their stated policy goals. We cannot continue to pursue a policy of blocking more and more without genuinely investing in other solutions, particularly education.

ORG will continue to gather evidence of overblocking through the Blocked tool. We have developed the tool to allow the analysis of blocked sites by category and keywords. We are calling on our supporters and any interested parties to analyse this data and report over-blocked sites to ISPs. We will continue to use the evidence gathered to identify the scale of blocking and any patterns that show cultural bias against particular types of content. Our goal is to improve transparency and ensure censorship in the UK is documented and limited.

Both fixed and mobile ISPs can vastly improve the way they deal with complaints about overblocking. They should commit to a minimum response time for complaints. They should address problems with missing reports, including by checking Blocked.org.uk for unresolved requests. Appeal processes should be introduced by fixed line ISPs, preferably to review against a fixed standard such as the BBFC provide for mobile, as reclassification errors are made. ISPs should work directly with groups that feel their websites are being unfairly restricted, such as regulated gun clubs and fireworks resellers, so that they are able to agree a fair path forward.

Fixed-line ISPs can reduce the problems they are creating by recommending more narrowly-tailored filters to their customers, which exclude typically over-broad categories such as alcohol from filter lists.

Third-party filtering companies should examine the categories of damage we have observed - from technical sites through to counselling, wedding services, and advice websites - to understand how they can limit the harms from filters. UK ISPs, as their customers, can also play a role in this. Filtering companies need to make their own lists much more open to public inspection and correction. In the long term, databases should be open to non-manual checking.

Recommendations

We would like to see child-safeguarding solutions that balance the fundamental rights of children and adults. So long as filters are enabled, they particularly adversely affect freedom of expression for people who are unable to choose whether they use filters, such as children, or adults who do not control the account settings, for instance in shared houses.

1. Opt-in

Filters must be opt-in so that customers can make an informed choice about whether or not they want filters. We urge all ISPs who enable filtering by default to reverse their policy and provide filters on an opt-in basis. For mobile phone contracts, it should be easy to verify age at set-up. For pay-as-you-go mobile phones, we would note that data usage is less common, which makes both the need for age checks less important, and the harm from imposing filters less significant.

2. Harm-based evaluation of content

Greater transparency is needed about how ISPs are blocking sites. While we understand that different ISPs may want to offer different categories for blocking, it would be helpful if there was some convergence of standards over what is considered 'harmful'. Additionally, some top-level domains which have restricted uses should always be excluded from filtering, such as .sch.uk, .nhs.uk, .gov.uk, and .ac.uk. We would recommend that ISPs follow a similar framework to that established by the BBFC for their basic, or 'default', level of opt-in filtering.

3. Inform websites

We believe that website owners should be informed if their website is blocked and given an opportunity to appeal this decision. This is particularly important for small businesses, who may not be aware of filters but for whom the impact of blocking could be serious. It should not be left to customers or website owners themselves to discover and resolve erroneous filtering. Website owners could be informed using standard emails such as webmaster@example.com.

4. Better processes

Internet users need to be provided with better processes for identifying and requesting unblocks of wrongfully-blocked sites. We urge mobile providers, fixed-line ISPs, Internet Matters, and the BBFC to promote the Blocked tool as a means for all website owners and web users to be able to discover immediately whether a website is blocked. Due to the potential negative impact of wrongful blocks on business, complaints should receive responses within a fixed timeframe - ideally no more than 48 hours.

We hope ISPs will engage with the Blocked project, to ensure that the process for reporting sites is streamlined and acts more like a reliable ticketing system, without reports getting "lost". ISPs could ensure that they make APIs available to the Blocked project which allow instant and accurate information to be retrieved from each ISP about whether a domain is currently filtered.

5. Appeals

None of the fixed-line ISPs currently allow direct appeals once a site has been reviewed and deemed correctly classified. Providers should ensure that they have processes in place for users to request further review of sites where they are dissatisfied with an ISP's providers' decision.

Mobile ISPs should also ensure that they remind those who report wrongful blocks that they have the right to appeal to the BBFC if they are unsatisfied with the decision that the mobile operator takes with regard to the unblock request. We have produced draft text for this purposes which we have included earlier in this report and which ISPs may wish to make use of.

6. Providing filters should continue to be voluntary

The Government should not force all ISPs to provide network level filters. If major ISPs find better ways to deliver filters via third parties, this should be encouraged.

7. Move towards device-level filters

Network-level filters are a blunt instrument. They are "one size fits all". In practice, children need differing levels of intervention, while most adults do not need them at all. Network level filters are likely to be switched off due to the inconvenience they impose. Device level filters are more likely to be able to deal with https content effectively and can be tailored to the needs of a particular child.

8. Ofcom should seek and publish advice from BEREC and the Commission about the legal status of ISP filters

As the regulator, Ofcom is responsible for ensuring the Open Internet regulations are complied with.

9. Further research is needed

The Government should fund rigorous, independent research into the risks to children of viewing different types of content. It should also fund research into the success of different strategies for keeping children

safe, including strategies for building resilience as well as those around removing risks. We encourage academics to work with our data and testing environment to understand filtering technology better.

Appendix A - Raw Data

Table A - Keyword list categories

All results in Table A 1-4 relate to the results at default filtering levels, so do not include sites blocked at BT Strict filter settings, except in number initially identified.[127]

Table A.1 Verified search results

These results have been produced by search and then hand checked.

Sites relating to keywords related to	Number of blocked domains identified through search[78]	Number of domains still blocked	Current ISP blocks[79]
Addiction, substance abuse support sites	185	91	287
Charities and non-profit organisations	98	17	24
Counselling, support, and mental health	112	77	191
Domestic violence and sexual abuse support	59	14	42
LGBTQ+ sites	114	39	121
School websites	161	23	52

[127] *See results at https://www.blocked.org.uk/lists?network=BT&network=Plusnet&network=Sky&network=VirginMedia&network=TalkTalk&network=EE&network=Three&network=Vodafone*

Table A.2 Verified search results, UK sites only

These results are produced by the same results as above, but exclude non-UK results.

Sites relating to keywords related to	Number of blocked domains identified through search	Number of domains still blocked	Current ISP blocks
Addiction, substance abuse support sites	35	14	48
Charities and non-profit organisations	91	17	24
Counselling, support, and mental health	104	70	177
Domestic violence and sexual abuse support	7	3	11
LGBTQ+ sites	27	7	25
School websites	143	13	28

Table A.3 Unverified search results

Sites relating to keywords related to	Number of blocked domains identified through search	Number of domains still blocked	Current ISP blocks
Building and building supplies	67	26	64
CBD oils, CBD-related, and hemp products	307	220	1081
Drainage and drain unblocking services	107	3	3
Photography sites	1858	732	2109
Religious (Christian) sites	137	54	147
Weddings and wedding photographers	4506	1718	3739

Sites relating to keywords related to	Number of blocked domains identified through search	Number of domains still blocked	Current ISP blocks
VPN sites	404	345	1719

Table A.4 Unverified search results, .uk domains only

Sites relating to keywords related to	Number of blocked domains identified through search	Number of domains still blocked	Current ISP blocks
Building and building supplies	59	23	48
CBD oils, CBD-related, and hemp products	112	91	510
Drainage and drain unblocking services	99	2	2
Photography sites	1372	514	1348
Religious (Christian) sites	37	9	20
Weddings and wedding photographers	4012	1480	3154
VPN sites	23	15	55

Table B - Unblock request categories

The table below shows the number of user-reported domains fitting into each primary category which we manually assigned.

Category for Submitted Reports	Number of reported domains	Number of domains unblocked after reporting
Adult, Pornography, and Escort Services	40	1

Category for Submitted Reports	Number of reported domains	Number of domains unblocked after reporting
Advertising, Branding, and Communications Agencies	11	9
Advice Sites (Drugs, Alcohol, Abuse)	52	44
Agriculture, horticulture and agricultural supplies	10	8
Alcohol	23	4
Alcohol-related (non-sales) sites	36	8
Antiques and Collectibles	2	2
APIs, CDNs, and Network Endpoints	9	3
Architecture and Design	3	2
Arts, Crafts, and Sculpture	32	24
Bars, Clubs, and Restaurants	18	8
Beauty and cosmetics	14	7
Body piercing and tattoos	3	2
Books, Writing, and Literature	22	18
Builders and Building Supplies	32	27
Business and Services	16	15
Care homes	1	1
CBD Oils, CBD-Related, and Hemp Products	21	8
Celebrity related	5	5
Charity and non-profit	68	55
Child-related business	8	7
Clothing and Fashion	8	5
Community and social media	19	6
Cooking and food	7	7
Counselling, Support, and Mental Health	122	98
Dating	5	0

Category for Submitted Reports	Number of reported domains	Number of domains unblocked after reporting
Directory Services and Advertisements	3	3
Drug Paraphernalia	2	0
E-cigarettes	1	0
Education and Academic Reference	19	14
Energy and environment	1	0
Events and events companies	18	16
Fashion	12	7
File Sharing and BitTorrent Trackers	7	0
Financial	3	3
Fireworks	4	1
Flower shops	3	2
Gardening	1	1
Guns and Weapons	4	0
Health	25	19
History and heritage	11	8
Household, household repairs and DIY	32	32
Humour, Comics and Entertainment	4	1
Industry and manufacturing	14	12
Kitchens and Interior Design	3	2
Languages and language learning	4	4
LGBTQ+	40	27
Lotteries and gambling	3	1
Media Streaming	12	4
Movies and TV	2	2
Music	50	41
Parked or Inactive Domain	1	1

Category for Submitted Reports	Number of reported domains	Number of domains unblocked after reporting
Personal	15	11
Photography, Graphic Design, and Filmmaking	21	14
Political	17	6
Real Estate and Property	9	9
Regulated shooting ranges and associations	14	5
Regulated UK gunshops	3	1
Religious	21	19
Science and medical science	12	11
Shopping	22	13
Spam or Hijacked	3	2
Spirituality and non-conventional beliefs	2	2
Sport and leisure	35	30
Takeaway businesses	5	3
Tech, IT and Software	41	21
Tobacco paraphernalia and collectibles	1	0
Tobacco sales	1	1
Transport and vehicles	21	18
Travel and Tourism	14	13
Video and Online Games	17	5
Vineyards	2	0
VPN or security tool	12	2
Web designers	3	3
Weddings and Wedding Photographers	44	40
Wellbeing	5	4

Table C - Unblock requests categorised by user affiliation

Reporter	2018	2019	Total
Not Stated	516	371	**36**
Site Owner (Total)	12	111	**28**
Site Owner (Business)	9	78	**16**
Site Owner (Other)	2	21	**1**
Site Owner (Personal)	1	12	**11**
Site User	11	21	**1**
Web Developer / Administrator	-	13	**2**
Totals:	**539**	**516**	**67**

Table D - Breakdown of damage alleged by users submitting unblock requests

Damage	2018	2019	Total
API, CDN or infrastructure blocked	-	14	**14**
Block censors safety information	2	6	**8**
Block has affected site credibility	-	4	**4**
Block has directly influenced business decisions	-	1	**1**
Block suspected due to previous use of domain	-	8	**8**
Complaints from users[128]	1	8	**9**
Loss of business (confirmed)[129]	-	11	**11**
Loss of business (suspected)[130]	-	7	**7**

[128] *Situations in which a site owner reports in the text of their unblock request that they have been receiving complaints about the block from the users of their site.*

[129] *Situations in which a site owner references with certainty in the text of their unblock request that a loss of business is being caused to the block. As we are unable to verify the legitimacy of this kind of claim, we present this data for statistical interest only and opt not to draw conclusions directly from it.*

[130] *As above, but where the site owner has referenced their suspicion that a block may lead to a loss of business.*

Damage	2018	2019	Total
Pre-launch block	1	8	**9**
User unable to disable filters[130]	11	5	**16**

Table E - Unblock requests forwarded to each ISP

ISP	2017	2018	2019	Total
BT	170	223	48	**441**
BT-Strict	12	116	36	**164**
Plusnet		21	14	**35**
Sky	146	152	37	**335**
TalkTalk	34	232	50	**316**
Virgin Media	27	100	20	**147**
FIXED TOTAL	**389**	**844**	**205**	**1438**
EE	38	106	22	**166**
O2	58	99	21	**178**
Three	27	80	24	**131**
Vodafone	45	59	28	**132**
MOBILE TOTAL	**168**	**344**	**95**	**607**
GRAND TOTAL	**557**	**1188**	**300**	**2045**

[131] *Situations in which a user of a particular site has submitted an unblock request via the Blocked tool and their report confirms or suggests that the user is unable, or unaware of how, to disable the adult content filters on their connection.*

Table F - ISP reply statistics (aggregate)

	2017	2018	2019	Total
Sites reported	350	414	93	**857**
Reports logged	545	1072	264	**1881**
Reports sent	545	1072	264	**1881**
Reports answered	0	139	155	**294**
Reports unblocked	465	732	170	**1367**
Reports rejected	0	41	20	**61**
Reports unresolved	80	294	33	**407**
Reports unresolved where site is blocked against ISP policy	29	153	15	**197**

Table G - ISP reply statistics (per-ISP)

BT

	2017	2018	2019
Reports Sent	170	223	48
Auto-replies logged	0	55	48
Total replies logged	0	106	84
Avg reply interval	-	9 days	7 days
Unresolved count	33	45	0
Unresolved non-policy block count	9	18	0
Unresolved policy block count	24	27	0
Resolved & blocked against policy	0	7	0
Open report count	33	48	9

BT-Strict

	2017	2018	2019
Reports Sent	12	116	36

Auto-replies logged	0	28	35
Total replies logged	0	54	62
Avg reply interval	-	11 days	5 days
Unresolved count	4	32	1
Unresolved non-policy block count	1	14	0
Unresolved policy block count	3	18	1
Resolved & blocked against policy	0	0	4
Open report count	4	37	8

EE

	2017	2018	2019
Reports Sent	38	106	22
Auto-replies logged	0	22	21
Total replies logged	0	45	41
Avg reply interval	-	3 days	6 days
Unresolved count	0	24	1
Unresolved non-policy block count	0	18	1
Unresolved policy block count	0	6	0
Resolved & blocked against policy	0	12	6
Open report count	0	26	10

EE

	2017	2018	2019
Reports Sent	38	106	22
Auto-replies logged	0	22	21
Total replies logged	0	45	41
Avg reply interval	-	3 days	6 days
Unresolved count	0	24	1

Unresolved non-policy block count	0	18	1
Unresolved policy block count	0	6	0
Resolved & blocked against policy	0	12	6
Open report count	0	26	10

O2

	2017	2018	2019
Reports Sent	58	99	21
Auto-replies logged	0	0	6
Total replies logged	0	0	6
Avg reply interval	-	-	-
Unresolved count	9	29	9
Unresolved non-policy block count	4	19	6
Unresolved policy block count	5	10	3
Resolved & blocked against policy	0	0	0
Open report count	9	29	11

Plusnet

	2017	2018	2019
Reports Sent	-	21	14
Auto-replies logged	-	0	0
Total replies logged	-	0	0
Avg reply interval	-	-	-
Unresolved count	-	3	1
Unresolved non-policy block count	-	2	1
Unresolved policy block count	-	1	0
Resolved & blocked against policy	-	0	0
Open report count	-	3	1

Sky

	2017	2018	2019
Reports Sent	146	152	37
Auto-replies logged	0	29	32
Total replies logged	0	50	52
Avg reply interval	-	5 days	3 days
Unresolved count	16	51	4
Unresolved non-policy block count	10	30	1
Unresolved policy block count	6	21	3
Resolved & blocked against policy	0	0	6
Open report count	16	51	21

TalkTalk

	2017	2018	2019
Reports Sent	34	232	50
Auto-replies logged	0	0	0
Total replies logged	0	0	0
Avg reply interval	-	-	-
Unresolved count	19	87	10
Unresolved non-policy block count	4	40	1
Unresolved policy block count	15	47	9
Resolved & blocked against policy	0	0	0
Open report count	19	87	10

Three

	2017	2018	2019
Reports Sent	27	80	20
Auto-replies logged	0	10	1

Total replies logged	0	16	1
Avg reply interval	-	11 days	-
Unresolved count	0	39	4
Unresolved non-policy block count	0	15	2
Unresolved policy block count	0	24	2
Resolved & blocked against policy	0	0	0
Open report count	0	39	4

Virgin Media

	2017	2018	2019
Reports Sent	27	100	20
Auto-replies logged	0	6	1
Total replies logged	0	6	1
Avg reply interval	-	11 days	-
Unresolved count	3	39	4
Unresolved non-policy block count	2	15	2
Unresolved policy block count	1	24	2
Resolved & blocked against policy	0	0	0
Open report count	3	39	4

Vodafone

	2017	2018	2019
Reports Sent	45	59	28
Auto-replies logged	0	17	25
Total replies logged	0	17	25
Avg reply interval	-	21 days	-
Unresolved count	0	5	3
Unresolved non-policy block count	0	5	3

Unresolved policy block count	0	0	0
Resolved & blocked against policy	0	0	0
Open report count	0	12	17

Table H - Mobile network blocking inconsistencies

Blocked on 2 networks	32,969
Blocked on 3 networks	42,823
Blocked on 4 networks	71,768
Blocked only on EE	2,596
Blocked only on O2	3,242
Blocked only on Three	3,466
Blocked only on Vodafone	16,062

Appendix B - Methodology for reporting statistics

General

We have tried to be cautious in our statistical analysis, so that it is as accurate and reasonable as possible. This means that some calculations have not been made. In particular:

1. The time elapsed to a site being unblocked has not been calculated, as it cannot be determined why a block has been lifted, as multiple ISPs use the same filtering providers.
2. We have assumed that non-replies from ISPs do not count as a non-response when a block has been lifted. We have only counted non-replies when a block has remained in place.

We do not currently index or check websites which exclude bots in robots.txt.[132] This limits the number of blocks detectable.

Indexing has aimed at breadth rather than fresh results, which means that search results needed to be refreshed for accurate results, particularly for .uk results which were tested early on. This also means that we will be underestimating current blocks through our search results.

ISP reply information

We count an ISP reply when it is received by email. Where we do not receive a reply, it is ignored for the purposes of calculating response times.

ISP replies are assessed to see if they are accepting a block be removed, or if the request is rejected.

The Blocked system has collected ISP email replies directly since 1 August 2018. They are incomplete as some ISPs replied directly to users. We continue to limit the possibilities for ISPs to amalgamate replies or avoid sending replies through our tool so that reporting becomes more accurate and complete over time.

ISP performance statistics

We have ignored unblock requests that were not sent, or were abusive (eg for known porn sites), for the

[132] *'Robots Exclusion Standard'. Wikipedia, 25 February 2019.* https://en.wikipedia.org/w/index.php?title=Robots_exclusion_standard

performance statistics such as the length of time it takes for an ISP to respond.

Categorisation of site, sender and damage types

Categorisation of sender and damage was done by the message and the sender address for the complaint originally sent. Often the message identifies the senders' relationship to the site.

Site categorisation was done manually, by checking the website and the message sent. In some cases, the sites' use had changed, so the classification was made on the basis of the message sent.

Categorisation statistics exclude sites, senders and damage classifications relating to messages that were unsent or abusive.

Blocked versus unblocked sites

Blocked sites are identified over http links only. Blocking pages are identified through standard pages on filtered lines. Statistics only relate to http blocking pages detected, and not DNS results or https links failing.

Filtering on ISP lines

The standard or recommended level of filtering is chosen on fixed lines. On mobile lines, the default filter is left in place.

We have additionally tested some sites for blocks using the 'strict' settings at BT.

What we have tested

Our lists of domains come from many sources, but the largest of these are the .uk zone file, tested from March 2017, the .org zonefile in 2017-18, and a partial test of the .com zonefile from May 2018. Zone files are complete lists of registered domains. We also used 3.5 million files from the DMOZ directory project and a now dated Alexa top 100,000 list in 2014-15.

What counts as a 'site'

We normally index the www. version of a website, rather than a version without. We are unable to guess other subdomains so these are not tested as they are not contained within zone files. We normalise URLs to lower case. However, there are cases where it makes sense for users to submit longer URLs for testing. This can lead to duplication of sites tested, however we have not observed this as phenomenon within our testing, and would regard it as abuse for statistical purposes.

Searches and lists of potential errors

The lists produced in Appendix A were produced through a keyword search of our data retained from when we indexed the sites. This data is prone to age, as we cannot re-index sites on a regular basis. Once the list of potential errors was created, we would check each site quickly from the description and where necessary a check of the site and remove immediately obviously irrelevant material, to give a reasonably but not perfectly accurate set of sites that should be checked for incorrect blocks. Up to 20% of the lists we have are typically untestable, as they have become unreachable. This can mean some results appear to be old.

Appendix A site search lists were produced in two different ways, by a process of individual checking of sites in the 'curated' tables, and by light pruning of obvious errors in the non-curated lsts. Both sets of searches excluded likely adult sites in the initial searches. Sites blocked by BT-Strict only are not counted in these figures, except in the initial site count, but can be found in the public lists. This is because BT Strict blocks a great deal of content but is not used by many households. The search summary results page allows users to see the different levels of blocking at each ISP or set of ISPs.

Appendix C - Technical challenges from filtering products

When adult content web filters of this type were first implemented, most websites on the Internet were served over unencrypted HTTP connections, meaning that it was trivial for an ISP to direct traffic away from a site they wished to block, and replace it with a block page explaining that the site had been filtered by the ISP due to the adult content filter. However, in recent years, there has been a marked increase in the number of sites being served over encrypted connections by default using HTTPS. Modern web browsers are even making moves to label sites which do not use encrypted connections as "Not Secure".[133] If a user's web browser requests the HTTPS version of a website, the user's ISP is still able to block their connection to that site, but the ISP is unable to redirect the user to a page explaining that the site has been blocked. From a user's perspective, the attempted page load will appear to hang indefinitely without completing. This is acknowledged directly by some ISPs, such as Sky Broadband, who note:

> *"If you've blocked a site that uses a secure https connection (such as Facebook and Twitter), the secure connection prevents us displaying the blocked page screen we would normally show."* [134]

This is a major issue from the perspective of transparency. Users may be prevented from viewing certain sites and may be left unaware that the filter is the reason they are unable to connect. Site or business owners may also receive reports from users who are unable to access their website but are unable to provide information that would allow the site owner to identify the issue as one which is being caused by web filters.

The increase in prevalence of websites which are encrypted by default also poses a difficulty for nuanced and targeted web filtering. On unencrypted connections, web filters can block individual pages, individual subdirectories, or even block based on the keywords visible on a particular page. With encrypted sites, ISP-level filters can no longer achieve this level of granularity in filtering and must instead opt to either block an entire domain, or to allow it. This lack of granularity is likely to lead to a situation in which some smaller sites find themselves blocked in their entirety due to a minority of the content they hold being unsuitable for minors, where much larger sites are able to escape unblocked due to their size. This is already apparent in the fact that only BT's 'Strict' filter blocks the primary domains for Twitter[135] or Reddit[136], and no ISP appears to restrict access to Imgur.[137] While the majority of the content on the aforementioned sites is not adult in nature, all of the sites can be used to locate a great deal of content which is pornographic or arguably inappropriate

[133] *'A Secure Web Is Here to Stay'. Google Online Security Blog (blog). Accessed 13 March 2019.* https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

[134] *'Sky Broadband Shield | Sky Help'. Sky. Accessed 13 March 2019.* https://www.sky.com/help/articles/sky-broadband-shield-explained

[135] *See:* https://www.blocked.org.uk/site/http://twitter.com

[136] *See:* https://www.blocked.org.uk/site/http://www.reddit.com

[137] *See:* https://www.blocked.org.uk/site/http://imgur.com

for minors. All three currently fall within the top 30 websites in the UK when ranked by Alexa.[138]

We suggest the above issues could be better tackled by shifting a focus away from network-level filtering and towards device-level filtering. Network-level filters are a blunt instrument that must increasingly make sweeping choices about whether to block or allow entire domains. Device-level filtering is still able to retain a nuanced approach. Filtering is done on a user's device, and this means that it is able to filter just certain sections of websites, certain pages, or even filtering particular content within a page, regardless of encryption. Device-level filters carry their own set of challenges to ensure they do not compromise user privacy or security, but are a crucial step better than the binary block-or-don't approach which must increasingly be taken by network-level filters.

[138] *'Top Sites in United Kingdom - Alexa'. Accessed 13 March 2019.* https://www.alexa.com/topsites/countries/GB

Appendix D - Bibliography

'A Secure Web Is Here to Stay'. Google Online Security Blog (blog). Accessed 13 March 2019. https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

'Anger as ISP Web Filters Block Access to Fifty Scottish Charity Websites | STV Edinburgh | Edinburgh', 15 July 2014. https://web.archive.org/web/20140715071104/http://edinburgh.stv.tv/articles/282356-anger-as-isp-web-filters-block-access-to-fifty-scottish-charity-websites/

'Appeals and Complaints | British Board of Film Classification'. Accessed 13 March 2019. https://www.bbfc.co.uk/what-classification/mobile-content/appeals

Atkinson, Shirley, Steven Furnell, and Andy Phippen. Using Peer Education to Encourage Safe Online Behaviour, 2019. https://www.researchgate.net/publication/237430450_Using_Peer_education_to_encourage_safe_online_behaviour

Bailey, Reg. 'Letting Children Be Children'. UK Government Department for Education, June 2011. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/175418/Bailey_Review.pdf

Birtles, Alex. 'How HomeSafe Is Keeping TalkTalk Homes Safer | TalkTalk BlogBlog', 23 January 2015. https://web.archive.org/web/20150130140151/http://blog.talktalk.co.uk/newsroom/how-homesafe-is-keeping-talktalk-homes-safer/

Body of European Regulators for Electronic Commissions. 'BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules', August 2016. http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf

'BT Parental Controls: How to Keep Your Children Safe Online'. BT.com. Accessed 13 March 2019. http://home.bt.com/tech-gadgets/internet/broadband/stay-safe-with-bt-parental-controls-11363887238413

Child Rights International Network. 'Access Denied: Protect Rights - Unblock Children's Access to Information', June 2014. https://archive.crin.org/sites/default/files/access_to_information_final_layout.pdf

Digital Economy Act 2017, s.105 (2019). https://www.legislation.gov.uk/ukpga/2017/30/part/6/crossheading/internet-filters/enacted

European Commission. 'Andrus Ansip'. European Commission, 7 March 2019. https://ec.europa.eu/commission/commissioners/2014-2019/ansip_en

'Framework | British Board of Film Classification'. Accessed 13 March 2019. http://www.bbfc.co.uk/what-classification/mobile-content/framework

Geere, Duncan. 'O2 Installs 18+ Filter on the Mobile Web'. Wired UK, 4 March 2011. https://www.wired.co.uk/article/o2-mobile-web-filtering

Halperin, Alex. 'What Is CBD? The "miracle" Cannabis Compound That Doesn't Get You High'. The Guardian, 28 May 2018, sec. Society. https://www.theguardian.com/society/2018/may/28/what-is-cbd-cannabidiol-cannabis-medical-uses

House of Commons. 8 February Debate (Vol 778, Col 1786), 2017. https://hansard.parliament.uk/Lords/2017-02-08/debates/6EFC892A-F1A8-4156-B838-E8952E0908BA/DigitalEconomyBill#contribution-DBD7F39C-6A3F-4BDC-8759-E97AF7F26B59

House of Commons Women and Equalities Committee. 'Sexual Harassment and Sexual Violence in Schools: Third Report of Session 2016-17'. House of Commons, 7 September 2016. https://publications.parliament.uk/pa/cm201617/cmselect/cmwomeq/91/91.pdf

'Man-in-the-Middle Attack'. Wikipedia, 6 March 2019. https://en.wikipedia.org/w/index.php?title=Man-in-the-middle_attack

Matsakis, Louise. 'Parents, Here's How to Make YouTube Kids Safer'. Wired, 28 February 2019. https://www.wired.com/story/youtube-kids-parental-settings-safer/

'O2 Pulls Blocked URL Checker as Wave of New Customers Activate Their Phones'. Open Rights Group, 24 December 2013. https://www.openrightsgroup.org/blog/2013/o2-pulls-blocked-url-checker-as-wave-of-new-customers-activate-their-phones

'O2 Site Checker'. Accessed 13 March 2019. http://urlchecker18plus.o2.co.uk/

Ofcom. 'Children and Parents: Media Use and Attitudes Report 2018', 29 January 2019. https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf

'Internet Service Providers: Network Level Filtering Measures', 22 July 2014. https://www.ofcom.org.uk/__data/assets/pdf_file/0019/27172/Internet-safety-measures-second-report.pdf

'Strategies of Parental Protection for Children Online', 16 December 2015. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/31754/Fourth-internet-safety-report.pdf

'UK Code of Practice for the Self-Regulation of New Forms of Content on Mobiles', 11 August 2008. https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/ukcode

Open Rights Group. 10 x 10: Digital Rights for the Next Decade, 2016. https://www.openrightsgroup.org/about/reports/10-x-10-digital-rights-the-next-decade

'Mobile Internet Censorship: What's Happening and What We Can Do about It'. Open Rights Group, May 2012. https://www.openrightsgroup.org/about/reports/mobile-internet-censorship:-whats-happening-and-what-we-can-do-about-it

'Parliamentary Questions: Net Neutrality and Restriction of Access', 29 August 2017. http://www.europarl.europa.eu/doceo/document/E-8-2017-005328_EN.html

Phippen, Andy, and Henry Phippen. 'The UK Government Internet Safety Strategy – Time to Listen to the Youth Voice?' Entertainment Law Review 29, no. 8 (2018): 237–44.

Przybylski, Andrew K., and Victoria Nash. 'Internet Filtering Technology and Aversive Online Experiences in Adolescents'. The Journal of Pediatrics 184 (1 May 2017): 215-219.e1. https://doi.org/10.1016/j.jpeds.2017.01.063

P&S Intelligence. 'Mobile VPN Market to Reach $1,560.7 Million by 2023', June 2018. https://www.psmarketresearch.com/press-release/mobile-virtual-private-network-products-market

Regulation (EU) 2015/2120, § 8 (2015). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120

'Robots Exclusion Standard'. Wikipedia, 25 February 2019. https://en.wikipedia.org/w/index.php?title=Robots_exclusion_standard

Rosen, Rachael. 'Ordinary Magic for the Digital Age: Understanding Children's Digital Resilience'. Parent Zone, January 2017. https://parentzone.org.uk/system/files/attachments/Parent%20Zone%20Ordinary%20Magic%20online%20resilience%20report.pdf

'Scottish NGO Results'. Open Rights Group. Accessed 13 March 2019. https://www.openrightsgroup.org/blog/2014/scottish-ngo-results

'Scunthorpe Problem'. Wikipedia, 12 March 2019.

https://en.wikipedia.org/w/index.php?title=Scunthorpe_problem

Sellgren, Katherine. 'Porn "Desensitising Young People"', 15 June 2016, sec. Education & Family. https://www.bbc.com/news/education-36527681

Sky Broadband. 'Sky to Automatically Turn on Parental Controls for All New Broadband Customers', 21 December 2015. https://web.archive.org/web/20161219184644/https://corporate.sky.com/media-centre/news-page/2015/sky-to-automatically-turn-on-parental-controls-for-all-new-broadband-customers

'Sky Broadband Shield | Sky Help'. Sky. Accessed 13 March 2019. https://www.sky.com/help/articles/sky-broadband-shield-explained

'Top Sites in United Kingdom - Alexa'. Accessed 13 March 2019. https://www.alexa.com/topsites/countries/GB

UK Council for Internet Safety. 'UK Council for Internet Safety - About Us'. GOV.UK, 7 March 2019. https://www.gov.uk/government/organisations/uk-council-for-internet-safety/about

UK Government. 'The Coalition: Our Programme for Government', May 2010. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78977/coalition_programme_for_government.pdf

'The Internet and Pornography: Prime Minister Calls for Action'. GOV.UK, 22 July 2013. https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action

'UK Schools Get .sch.uk Domain', 23 September 2004. https://web.archive.org/web/20130528081325/http://www.netimperative.com/news/2004/09/23/UK_schools_domain

UKCCIS Overblocking Working Group. Final Report, 2015. https://www.whatdotheyknow.com/request/320569/response/791574/attach/3/280405%20Final%20Version%20UKCCIS%20Overblocking%20Working%20Group%20Final%20Report.pdf

UNICEF. 'Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information, and Participation', June 2017. https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_EXPRESSION.pdf

United Nations General Assembly. 'Promotion and Protection of the Right to Freedom of Opinion and Expression', 21 August 2014. https://undocs.org/A/69/335

'UPDATE MP Claire Perry Claims UK ISP Internet Filters Will Not Overblock - ISPreview UK', 29 January 2014. https://www.ispreview.co.uk/index.php/2014/01/government-mp-claire-perry-claims-uk-isp-internet-filters-will-overblock.html

White, Geoff. 'One in Every Thousand Tweets Is Porn'. Channel 4 News, 17 February 2015. https://www.channel4.com/news/one-in-every-thousand-tweets-is-porn