OPEN RIGHTS GROUP

UK INTERNET REGULATION

PART I: INTERNET CENSORSHIP IN THE UK TODAY

About Jim Killock, Executive Director

Since joining Open Rights Group in January 2009, Jim has led campaigns against three strikes and the Digital Economy Act, the company Phorm and its plans to snoop on UK users, and against pervasive government Internet surveillance. He is working on data protection and privacy issues, as well as helping ORG to grow in size and breadth. He was named as one of the 50 most influential people on IP issues by Managing IP in 2012. In the same year ORG won Liberty's Human Rights Campaigner of the Year award alongside 38 Degrees, for work on issues from copyright to the Snooper's Charter.

Since 2009, ORG has doubled its supporter base, budget and workload, and held five activist conferences, ORGCon.

Jim is a trustee of FreeUKGen, the volunteer project to digitise genealogical records, and sits on the Governance Board of CREATe, the UK's research centre for copyright and new business models in the creative economy. He is on the Advisory Council of the Foundation of Information Policy Research.

Before joining ORG, Jim worked as External Communications Co-ordinator of the Green Party. At the Green Party, he promoted campaigns on open source, intellectual property, digital rights and campaigned against the arms and espionage technologist Lockheed Martin's bid for the UK Census. Lockheed Martin have since been prevented from handling UK Census data as part of their contract. He was also a leading figure in the campaign to elect their first party leader, Caroline Lucas MP. He has a blog at http://jim.killock.org.uk/

PGP key available via: pgp.mit.edu

OPEN RIGHTS GROUP

About Open Rights Group

As society goes digital we wish to preserve its openness. We want a society built on laws, free from disproportionate, unaccountable surveillance and censorship. We want a society in which information flows more freely. We want a state that is transparent and accountable, where the public's rights are acknowledged and upheld.

We want a world where we each control the data our digital lives create, deciding who can use it and how. We want the public to fully understand their digital rights, and be equipped to be creative and free individuals. We stand for fit-for-purpose digital copyright regimes that promote free expression and diverse participation in culture.

We campaign, lobby, talk to the media, go to court — whatever it takes to build and support a movement for freedom in the digital age. We believe in coalition, and work with partners across the political spectrum.

We uphold human rights like free expression and privacy. We condemn and work against repressive laws or systems that deny people these rights. We scrutinise and critique the policies and actions of governments, companies, and other groups as they relate to the Internet. We warn the public when policies — even well-intentioned ones — stand to undermine the freedom to use the Internet to make a better society.

www.openrightsgroup.org

EXECUTIVE SUMMARY

why we need independent, accountable and transparent decisions

The UK government's Digital Charter and online safety strategy proposes new controls on Internet content, stating that it wants to ensure that the country has the "same rules online as offline". It says it wants harmful content removed, while respecting human rights and protecting free expression.[1]

In response to this objective, the Open Rights Group (ORG) has conducted original research to ascertain areas where there is need for significant improvement in UK law on existing takedown procedures. We have found that, in fact, the same rules do not apply online as offline: many powers and practices the government employs to remove online content would be deemed unacceptable and arbitrary if they were applied to offline publications.

WE DETAIL FOUR AREAS:

- **Court injunctions for blocking copyright-infringing websites**
- **The scheme operated by .uk registrar Nominet to allow law enforcement to suspend domains that Nominet oversees[2]**
- **The work of the the Counter Terrorism Internet Referral Unit (CTIRU) based at the Metropolitan Police**
- **The powers of the British Board of Film Classification (BBFC) to block legal pornographic content**

Internet regulation in the UK fails to meet international standards, such as Council of Europe recommendations, by failing to ensure that decisions are independent, accountable and transparent. Legal processes are often absent and ad hoc procedures have been allowed to develop, with the result that current UK content regulation lacks proper legal oversight. This is particularly true of police suspension of domains via Nominet, and the work of the Counter Terrorism Internet Referral Unit (CTIRU), to which the police lodge requests for material to be removed. Even well-developed legal procedures like copyright injunctions for site blocking are not properly supervised. The list of what is blocked is not public, and up to 37% of blocks appear to be in error, as the reasons for the blocks no longer apply.[3] For instance, many domains are simply no longer actively used, but are still blocked.

At the very least, this shows that the holders of the injunctions and certain Internet Service Providers (ISPs) have very poor administration of block lists.

Other problematic developments include the regime for blocking pornography as a sanction to be administered by the British Board of Film Classification (BBFC), and ISP Internet filters, which appear to be very wide and are often enabled without user choice.

The UK government needs to evolve procedures in these areas and to set clear lines of accountability for itself as it demands action from others in the Digital Charter and the Internet Safety Strategy.

1 See https://wiki.openrightsgroup.org/wiki/Digital_Charter and https://wiki.openrightsgroup.org/wiki/Internet_Safety_Strategy

2 For more information about Nominet, see https://wiki.openrightsgroup.org/wiki/Nominet

3 For a full list from our research see https://www.blocked.org.uk/legal-blocks/errors

Finding	Detail
1. Court injunctions allowing copyright blocking is currently poorly administered by the parties, with the result that over 30% of blocked domains are no longer entitled to be blocked. Furthermore, there is no transparency over what is blocked, nor regarding how to resolve problems without resorting to a lengthy and unnecessary court process.	See Chapter 3 (a) (i)
2. Nominet are allowing eight law enforcement institutions to suspend .UK domains by filing a notice to Nominet. Law enforcement institutions can suspend .UK domains by filing a notice with Nominet, the .UK registar. Over 16,000 domains are suspended annually. Many participating institutions publish nothing about their reasons for requesting suspensions.The suspensions process lacks external accountability and has no independent appeals process. Appeals are instead directed to the participating law enforcement agency.	See Chapter 3 (b) (i)
3. The Counter-Terrorism Internet Referral Unit acts without sufficient supervision or transparency. It refuses to provide sufficient information to make it possible for parliament and the public to understand its work. Freedom of Information requests are routinely turned down on grounds of national security, sometimes without sufficient internal checks to ensure that relevant information exists, and even this reason is questionable. Individuals whose content is wrongly targeted lack the possibility of redress.	See Chapter 3 (b) (ii)
4. The Internet Watch Foundation (IWF) does offer an independent appeals process, which the Open Rights Group regards as a model for other organisations to emulate. There is scope to create a single body within the court system to manage appeals against content removal or blocking decisions made by Nominet, the CTIRU and the IWF.	See Chapter 3 (b) (iii)
5. The BBFC's powers to block websites by administrative order lack independent authorisation and are not based on an objective test for harm. This will lead to inconsistent and irrational blocking of legal content in some circumstances but not others. This does not appear to be compatible with internationally-recognised human rights standards.	See Chapter 3 (a) (ii)
6. There is a need for a single body to handle authorisations for blocking, takedown and suspension requests across law enforcement including PIPCU and other requests to Nominet as well as CTIRU and BBFC. This should include supervising IWF takedowns and blocks. This would provide external accountability for the actions of each agency. In emergencies, authorisations could be checked and vaidated after the fact.	See Chapter 4
7. An independent appeals process is also needed to handle complaints resulting from PIPCU and Nominet takedowns as well as CTIRU notices, along the lines of what is already provided by the IWF.	See Chapter 4

2 INTRODUCTION

a. Purpose and scope of this report

This report covers state regulation of Internet content in the UK, both formal and informal, and focuses on legal measures and illegal content. Our research has shown that the UK's approach to content regulation has created a lack of accountability and considerable scope for errors and abuse. We suggest some specific improvements that can be applied.

Our report follows the announcement of a forthcoming government White Paper, which will set out new goals for internet content regulation in the UK. The government's primary concern is removing "harmful" content.[4] The government is considering changes to make platforms liable for content.[5]

We survey the current regulation of online content. This ranges from court injunctions to block copyright-infringing websites through to informal bulk suspension of domain names by Nominet following law enforcement "requests". Seventeen or more organisations appear to be making significant decisions about content without supervision. We show significant deficiencies that need to be rectified in each of these arrangements, formal and informal.

b. Human rights principles for the Internet

There has been a great deal of thinking about free expression on the Internet and the role of state regulation. The Council of Europe has set out principles and the UN Special Rapporteur on Free Expression has produced guidance. Government policy should be consistent with this guidance.

i. The Council of Europe

The UK will remain a member of the Council of Europe after Brexit. In 2011, it produced the following principles, two of which are of particular relevance:[6]

1. Protection of all fundamental rights and freedoms and affirmation of their universality, indivisibility, interdependence and interrelation. …

4. Empowerment of Internet users to exercise their fundamental rights and freedoms and participate in Internet governance arrangements.

In 2016, the Council of Europe produced further guidance,[7] which reiterates that:

"Any national decision or action restricting human rights and fundamental rights on the Internet must comply with international obligations and in particular be based on law. It must be necessary in a democratic society, fully respect the principles of proportionality and guarantee access to remedies and the right to be heard and to appeal with due process safeguards."

4 https://www.gov.uk/government/news/new-laws-to-make-social-media-safer

5 https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper See page 17: Online platforms need to take responsibility for the content they host. They need to proactively tackle harmful behaviours and content. Progress has been made in removing illegal content, particularly terrorist material, but more needs to be done to reduce the amount of damaging content online, legal and illegal.

We are developing options for increasing the liability online platforms have for illegal content on their services. This includes examining how we can make existing frameworks and definitions work better, as well as what the liability regime should look like in the long run.

6 https://www.coe.int/en/web/compass/media#Internet20%governance20%and

7 CoE (2016) *Safeguarding Human Rights on the Net* Recommendation CM/Rec 13) 5(2016)April (2016 https://edoc.coe.int/en/internet-7010/council-of-europe-safeguarding-human-rights-on-the-net.html

ii. UN Special Rapporteur Recommendations

The UN Rapporteur on Free Expression has also released recommendations to governments and industry on this topic. For governments, these include:

65. States should repeal any law that criminalizes or unduly restricts expression, online or offline

66. Ensuring company transparency and remediation to enable the public to make choices about how and whether to engage in online forums. …

    States should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy

67. States and intergovernmental organisations should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship

68. States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression. They should avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users

69. States should publish detailed transparency reports on all content-related requests issued to intermediaries and involve genuine public input in all regulatory considerations.[8]

iii. The Manila Principles

The Manila Principles on intermediary liability is a global civil society initiative to which the Open Rights Group has signed on.[9] The principles aim to protect freedom of expression and create an enabling environment for innovation. They take into consideration the needs of governments and other stakeholders and, as a result, articulated baseline safeguards and best practices on intermediary liability.

The principles are meant to be directed at laws, policies, norms, practices, and private terms of service that relate to content restriction, including removal, blocking or filtering by intermediaries.

The principles are:

1. Intermediaries should be shielded from liability for third-party content
2. Content must not be required to be restricted without an order by a judicial authority
3. Requests for restrictions of content must be clear, be unambiguous, and follow due process
4. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality
5. Laws and content restriction policies and practices must respect due process
6. Transparency and accountability must be built into laws and content restriction policies and practices

8 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 6 April 2018 https://freedex.org/a-human-rights-approach-to-platform-content-regulation/ See paras 64-72

9 https//:www.manilaprinciples.org

INTERNET CENSORSHIP IN THE UK TODAY

3

This report examines those areas where the law provides for specific Internet blocking powers such as copyright-blocking injunctions targeting websites, and informal censorship procedures that have evolved within the police services, Nominet, and ISPs via the Internet Watch Foundation. In each case, we examine the deficiencies in the current procedures and make recommendations for improvements.

a. Formal Internet censorship

i. Copyright blocking injunctions; 38% of blocks in error

1. Open-ended powers

Copyright-blocking injunctions have one major advantage over every other system except for defamation. They require a legal process to take place before they are imposed. This affords some accountability and that necessity and proportionality are considered before restrictions are put in place.

However, as currently configured, copyright injunctions leave room for problems. We are confident that court processes will be able to resolve many of these. Further advantages of a process led by legal experts are that they are likely to want to ensure that rights of all parties are respected, and appeals processes in higher courts and the application of human rights instruments can ensure that problems are dealt with over time.

A process led by legal experts offers further advantages, including that it will be likely to ensure that rights of all parties are respected and that appeals processes in higher courts and the application of human rights instruments will ensure that problems are dealt with over time.

Copyright blocking injunctions are usually open-ended. There is not usually an end date, so they are a *perpetual legal power*. The injunction is against the ISPs. Rights-holders are allowed under the standard terms of the injunctions to add new domains or IP addresses that are in use by an infringing service without further legal review. ISPs and rights-holders do not disclose what exactly is blocked.

It has been reported that around 3,800 domains[10] are blocked by 31 injunctions, against around 179 sites or services.[11]

The government is preparing to consult on making copyright blocking an administrative process. We believe this would be likely to reduce accountability for website blocking, and extend it in scope. At present, website blocking takes place where it is cost effective for private actors to ask for blocks. Administrative blocking would place the cost of privately-demanded blocking onto the UK taxpayer, making it harder for economic rationality to constrain blocking. Without economic rationale, and with widening numbers of blocks, it would be harder to keep mistakes in check.

2. 38% of observed blocks in error

Open Rights Group has compiled public information about clone websites that might be blocked, for instance the many websites that have presented full copies of the Pirate Bay website.

We ran tests on these domains to identify which domains are blocked on UK networks. As of 25 May 2018, we found 1,073 blocked domains. Of these, we found 38% of the blocks *had been done in error*.[12]

To be clear, each block would generally have been valid when the block was initially requested and put in place by the ISP, but not many of these blocks were removed once the websites ceased to infringe copyright laws.

The largest group of errors identified concerned websites that were no longer operational. The domains were for sale or parked, that is flagged as not in use, (151), not resolving (76), broken (63), inactive (41) or used for abusive activities such as "click-fraud" (78).[13] At other times, we had detected three or four that had been employed in active unrelated legitimate use[14], and several that could be infringing did not seem to be subject to an injunction, but were blocked in any case.[15]

That means a total of 409 out of 1075 domains were being blocked with no current legal basis, or 38%.

These errors could occur for a number of reasons. Nearly all of the domains would have been blocked as they were in use by infringing services. However, over time they will have fallen into disuse, and some then reused by other services. In some cases, the error lies with ISPs failing to remove sites after notification by rights-holders that they no longer need to be blocked. In other cases, the rights-holders have not been checking their block lists regularly enough. While only a handful of blocks have been particularly significant, it is wrong for parked websites and domains for sale to be blocked by injunction. It is also concerning that the administration of these blocks appears very lax. A near 40% error rate is not acceptable.

To be clear, there is no legal basis for a block against a domain that is no longer being used for infringement. The court injunctions allow blocks to be applied when a site is in use by an infringing service, but it is accepted by all sides that blocks must be removed when infringing uses cease.

---

10 https://torrentfreak.com/uks-piracy-blocklist-exceeds-3800-urls-170321/

11 See https://wiki.451unavailable.org.uk/wiki/Main_Page and https://www.blocked.org.uk/legal-blocks for the lists of sites.

12 https://www.blocked.org.uk/legal-blocks/errors maintains the error rates; results as of 4 June 2018 are available here: http://web.archive.org/web/20180604092443/https://www.blocked.org.uk/legal-blocks/errors. Reports and data can be downloaded from https://www.blocked.org.uk/legal-blocks

13 These categories are defined as follows: (i) *Parked or for sale*: the site displays a notice explaining that the domain is for sale, or has a notice saying the domain is not configured for use; (ii) *not resolving* means that DNS is not configured so the URL does not direct anywhere; (iii) *broken* means that a domain resolves but returns an error, such as a 404, database error etc; (iv) *inactive* means that the site resolves, does not return an error, returns a blank page or similar, but does appear to be configured for use; (v) *abusive* means that the domain is employed in some kind of potentially unlawful or tortious behaviour other than copyright infringement.

14 A blog and website complaining about website blocking ,for instance .These were not functional as we completed the review.

15 See also our press release :https/:www.openrightsgroup.org/press/releases/2018/nearly-40-of-court-order-blocks-are-in-error-org-finds

Open Rights Group is concerned about its inability to check the existing blocks. What is or is not blocked should not be a secret, even if that is convenient for rights-holders. Without the ability to check, it is unlikely that independent and thorough checking will take place. Neither the ISPs or rights-holders have particular incentive to add to their costs by making thorough checks. As of the end of July 2018, most of the mistakes had remained unresolved, after three months of notice and a series of meetings with ISPs to discuss the problem. The number by October 2018 had reduced to nearer 30%, but progress in resolving these remains very slow.[16]

Many blocking regimes do not offer the flexibility to add on further blocks, but require rights-holders to return to court. The block lists are entirely public in many European countries.

ISPs should at a minimum publish lists of domains that they have "unblocked". This would allow us and others to test and ensure that blocks have been removed.

3. Poor notifications by ISPs

A further concern is that the explanations for website blocks and how to deal with errors is very unclear. This has no doubt contributed to the large proportion of incorrect blocks.

At present some basic information about the means to challenge the injunction at court is available. However, in most cases this is not what is really needed. Rather, a website user or owner needs information about the *holder of the injunction* and how to ask them to correct an error. This information is currently omitted from notification pages.

Notifications should also include links to the court judgment and any court order sent to the ISP. This would help people understand the legal basis for blocks.

Our project blocked.org.uk includes this information where available. We also generate example notification pages.

While ISPs could implement these changes without instruction from courts, they have been reluctant to improve their practice without being told. Open Rights Group's interventions in the Cartier court cases helped persuade the courts to specify better information on notification pages, but we believe there is some way to go before they are sufficiently explanatory.

4. Proposal for administrative blocking

The government is considering administrative blocking of copyright-infringing domains. This poses a number of problems. The current system requires rights holders to prioritise asking for blocks where is it is cost effective to do so. This keep censorship of websites to that which is economically efficient to require, rather than allowing this task to expand beyond levels which are deemed necessary.

As we see with the current system, administering large lists of website blocks efficiently and accurately is not an easy task. Expanding this task at the expense of the taxpayer could amount to unnecessary levels of work that are not cost efficient. It will be very hard for a government body to decide "how much" blocking to ask for, as its primary criteria will be ensuring material is legal. Unfortunately, there are very large numbers of infringing services and domains, with very small or negligible market penetration.

Secondly, it makes no sense for a growing system of censorship to keep what is blocked secret from the public. Administrative systems will need to be seen to be accurate, not least because sites based overseas will need to know when and why they are blocked in the UK in order to be able to appeal and remove the block. This may be resisted by rights-holder organisations, who have so far shown no willingness to make the block lists public. Administrative blocking could be highly unaccountable and much more widespread than at present, leading to hidden, persistent and unresolvable errors.

Thirdly, combining wide-scale pornography blocking with widening copyright blocking risks making the UK a world leader in Internet censorship. Once the infrastructure is further developed, it will open the door to further calls for Internet censorship and blocking through lightweight measures. This is not an attractive policy direction.

Recommendations to government:

1. Future legislation should specify the need for time limits to injunctions and mechanisms to ensure accuracy and easy review
2. Open-ended, unsupervised injunction and blocking powers should not be granted
3. Administrative blocking should be rejected

Recommendations to courts and parties to current injunction:

4. Current injunction holders and ISPs must urgently reduce the error rates within their lists, as incorrect blocks are unlawful
5. Courts should reflect on the current problems of accuracy in order to ensure future compliance with injunctions

16 https/:www.blocked.org.uk/legal-blocks/errors Errors on 10 October 2018 stood at 362 domains out of.1128

6. It should be mandatory for blocking notices to link to legal documents such as a judgment and court order
7. It should be mandatory for blocking notices to explain who holds the injunction to block the specific URL requested
8. Assurance should be given that there is transparency over what domains are blocked
9. ISPs and right-holders should be required to check block lists for errors

ii. BBFC pornography blocking

1. Administrative blocking powers

The Open Rights Group is particularly concerned that the BBFC, as the age verification regulator, has been given a general administrative power to block pornographic websites where those sites do not employ an approved age verification mechanism. We doubt that it is in a good position to judge the proportionality of blocking; it is simply not set up to make such assessments. Its expertise is in content classification, rather than free expression and fundamental rights assessments.[17]

In any case, state powers' censorship should always be restrained by the need to seek an independent decision. This provides accountability and oversight of particular decisions, and allows the law to develop a picture of necessity and proportionality.

The BBFC's blocking powers are not aimed at content but the lack of age verification (AV) in some circumstances. Thus they are a sanction, rather than a protective measure. The BBFC does not seek to prevent the availability of pornography to people under 18, but rather to reduce the revenues to site operators in order to persuade them to comply with UK legislative requirements.

This automatically leads to a risk of disproportionality, as the block will be placed on legal content, reducing access for individuals who are legally entitled to view it. For instance, this could lead to some marginalised sexual communities finding content difficult to access. Minority content is harder to find by definition, thus censoring that legal content is likely to affect minorities disproportionately. It is unclear why a UK adult should be prevented from accessing legal material.

At another level, the censorship will easily appear irrational and inconsistent. An image that is blocked on a website and lacks AV could be available on Twitter or Tumblr, or available on a non-commercial site.

The appeals mechanisms for BBFC blocks are also unclear. In particular, it is not clear what happens when an independent review is completed but the appellant disagrees with the decision.

2. BBFC requests to "Ancillary Service Providers"

Once section 14 of the Digital Economy Act (DEA) 2017 is operational, the BBFC will send requests to an open-ended number of support services for pornographic sites that omit age verification.[18] The BBFC hopes that once notified these services will comply with their request to cease service. Complying with a notice could put these services in legal jeopardy as they could be in breach of contract if they cease business with a customer without a legal basis for its decision. If these are companies based outside of the UK, no law is likely to have been broken.

Furthermore, some of the "services", such as "supplying" a Twitter account, might apply to a company with a legal presence in the UK, but the acts (tweeting about pornography) would be lawful, including sharing pornographic images without age verification.

If a voluntary notice is acted on, however, then free expression impacts could ensue, with little or no ability for end users to ask the BBFC to cease and desist in issuing notices, as the BBFC will believe it is merely asking for voluntary measures for which it has no responsibility.

This is an unclear process and should be removed from the Digital Economy Act 2018.

Recommendations to government:

1. The BBFC's blocking powers should be removed.
2. Cease obligations to the BBFC to notify ASPs for voluntary measures.

Recommendations to BBFC:

1. Ask for the application of the FoI Act to the BBFC's statutory work.

---

17 This report does not cover privacy concerns, but it is worth noting that privacy concerns could easily lead to a chilling effect, whereby UK residents are dissuaded from accessing legal material because of worries about being tracked or their viewing habits being leaked.

Robust privacy regulation could reduce this risk, but the government has chosen to leave age verification technologies entirely to the market and general data protection law. This leaves age verification (AV) for pornography less legally protected than card transactions and email records. See https://www.openrights-group.org/about/reports/response-to-bbfc-age-verification-consultation and https://www.openrightsgroup.org/blog/2018/the-government-is-acting-negligently-on-privacy-and-porn-av

18 Digital Economy Act 2017 s14 http://www.legislation.gov.uk/ukpga/2017/30/section/14/enacted

b. Informal censorship

In this section we examine a number of informal censorship regimes that have evolved as a result of policy demands made by the government and the police. In these areas, there has been little or no appetite to legislate, but nevertheless the government or law enforcement agencies have insisted that action is taken.

This may seem like a reasonable course of action, as it is simpler, but it means that the processes that have evolved are usually entirely one-sided in favour of complainants or law enforcement and lack independence, accountability and oversight. Two are particularly concerning – the practice of domain suspensions at Nominet, and the notification regime operated by the Counter Terrorism Internet Referral Unit.

This is not to say that either are making huge numbers of errors, but it is simply impossible to know. Except in isolated examples, it is not possible to ascertain how many errors there are, or how serious those errors may be. Transparency is required to get a better understanding. All systems, however, make errors. The question is whether errors will be corrected and whether the public can have confidence that complaints will be dealt with fairly.

i. Nominet domain suspensions

In December 2009, Nominet began to receive and act on bulk law enforcement requests to suspend the use of certain .uk domains believed to be involved in criminal activity.[19] criminal activity. At the request of the Serious and Organised Crime Agency (SOCA), Nominet subsequently consulted about creating a formal procedure to use when acceding to these requests and provide for appeals and other safeguards.[20] Nominet's consultations failed to reach consensus, with many participants including ORG arguing for law enforcement to seek injunctions to seize or suspend domains, not least because it became apparent that the procedure would be widely used once available.[21]

As with any system of content removal at volume, mistakes will be made. These pose potential damage to individuals and businesses.

Nominet formalised their policy in 2014.[22] It can suspend any domain that it believes is being used for criminal activity; in practice this means any domain it is notified about by a UK law enforcement agency.

A domain may be regarded as property or intellectual property. It can certainly represent an asset with tradeable value well beyond the cost of registration fees.

Many countries require a court process for such actions, including the USA and Denmark. Such actions usually result in control of the domain being passed to the litigant. The EU is asking for every member state to have a legal power for domain suspension or seizure relating to consumer harms.[23]

Some domains are used by criminals, as with any communications tool. There is a case for a suspension or seizure procedure to exist, although it should be understood that seizing or suspending a domain represents disruption for a website owner, rather than a means to cease their activities. For instance, it would not be difficult for the owner of *rolexreplicas.co.uk* to register *replicarolex.co.uk* and use the new domain to serve the same website.

Although Nominet failed to get agreement about a procedure for suspension requests, it has continued to accede to requests, which have roughly doubled in number each year from 2014, totalling over 16,000 in 2017.[24] The reasons requests have doubled is unclear, and ORG has not been given clear answers. It may be in part because the costs of domain registrations decreases over time, in part because detection has improved, and in part because it becomes necessary for a criminal enterprise to register new domains once they are suspended. Parties we spoke to agreed that it is unlikely that the number of criminals is doubling.

Around eight authorities have been using the domain suspension process, one of which, National Trading Standards, is legally a private company and not subject to Freedom of Information Act requests.

Nominet does not require any information from these organisations, it simply requires them to request suspensions in writing. For instance, they are not asked to publish a policy explaining when the organisation might ask for domains to be suspended, or what the level of evidence required to act might be.

---

19 http://www.dailymail.co.uk/news/article-1233016/Over-thousand-scam-websites-targeting-Christmas-shoppers-shut-online-raid-Scotland-Yards-e-crime-unit.html Over a thousand scam websites targeting Christmas shoppers shut down after an online raid by Scotland Yard's e-crime unit, 4 December 2009, dailymail.co.uk

20 http://web.archive.org/web/20111113021751/http://www.nominet.org.uk/news/releases/?contentId=8216 Nominet calls on stakeholders to get involved in policy process, nominet.org.uk, 09 February 2011 (webarchive)

21 https://www.theregister.co.uk/2011/11/25/nominet_domain_takedowns/ ISP outcry halts cybercops' automatic .UK takedown plan, The Register 25 November 2011

22 https://www.nominet.uk/nominet-formalises-approach-to-tackling-criminal-activity-on-uk-domains/

23 Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.345.01.0001.01.ENG&toc=OJ:L:2017:345:TOC https://wiki.openrightsgroup.org/wiki/Consumer_Protection_Cooperation_Regulation

24 https://wiki.openrightsgroup.org/wiki/Nominet/Domain_suspension_statistics has a table of statistics derived and referenced from Nominet's transparency reports

Several of the organisations making requests were unable to supply a policy, or refused to supply information about their policy, when we made Freedom of Information requests.[25] The National Crime Agency refused to respond, as it is not subject to the Freedom of Information Act. National Trading Standards spoke to us, but did not supply a policy; it is not subject to the Act. The Fraud and Linked Crime Online (FALCON) Unit at the Metropolitan Police Service confirmed that it has no policy, but decide on an ad hoc basis. The National Fraud Intelligence Bureau at City of London, which suspended over 2,700 domains last year, says: "We do not have a formal Policy".[26]

Nominet's process is:

1. The agency concerned files a request to Nominet, citing the domains it believes are engaged in criminal activity. This may be one or a list of thousands of domains.
2. Nominet ensure the owners are notified and given a period to remove anything contravening the law.
3. If there is a response from a domain owner, the law enforcement agency is asked to review its decision.
4. If there is no response from a domain owner, the domains are suspended.
5. Any further complaints are referred back to the law enforcement agency.

There is no independent appeals mechanism. If a domain owner asks for a domain suspension to be reconsidered, they are referred back to the police or agency that made the request, who can revisit the decision. As most of the agencies have no policy, or will not publicise it, this does not seem to be a procedure that would give confidence to people whose domains are wrongly targeted.

This is in contrast to the Internet Watch Foundation (IWF)'s procedure, which provides an appeal process with an independent retired judge to consider whether in fact material should be removed or blocked, or left published, once the IWF has made an internal review of its original decision.[27]

The IWF's decisions are relatively simple compared to the range of concerns advanced to Nominet by the various agencies involved. Despite this, it is surprising that there is no independent review of the grounds for a suspension. It seems unlikely that the police and agencies will always be able to review their own work and check if their initial decision is correct without bias or repeating their error. It also seems unlikely that everyone who wishes to complain would have confidence in the police's ability to review a complaint.

Ultimately, the decision to suspend a domain is Nominet's. Nominet owes its customers, domain owners, a trustworthy process that ensures that domain owners are able to have their voices heard if they believe a mistake has been made. Asking the police to review their request does not meet a standard of independence and robust review.

There is also a lack of transparency for potential victims as a result of Nominet's policy to suspend domains rather than seize them. Suspensions simply make domains fail to work. A *domain seizure* would allow agencies to display "splash pages" warning visitors about the operation with which they may have done business. If goods are dangerous, such as unlicensed medicines or replica electronics, this may be important.

In our view, an independent prior decision and an independent reviewer are needed for Nominet's process to be legitimate, fair and transparent, along with splash pages giving sufficient warning to prior customers. Domain *seizure* processes should replace informal *suspension* requests and the process should be established by law.

Because some improvements can be made by Nominet that fall short of a fully accountable, court-supervised process, we propose these as short term measures.

Recommendations to Nominet:

1. Adopt Freedom of Information principles
2. Ask the government for a legal framework for domain seizure based on court injunctions for domain seizures
3. Require notices to be placed after seizures to explain the legal basis and outline any potential dangers to consumers posed by previous sales made via the domain. This could include contact details for anyone wishing to understand any risks to which they may have been exposed
4. Short term: Offer an independent review panel
5. Short term: Require government organisations to publish their policies relating to domain suspension requests
6. Short term: Publish the list of suspended domains, including the agency that made the request and the laws cited

25 The results of our FoI requests for domain suspension policies are summarised with references at https://wiki.openrightsgroup.org/wiki/Nominet/Domain_suspension_statistics

26 https://www.whatdotheyknow.com/request/national_fraud_intelligence_bure#incoming-1115354

27 See the discussion on the IWF below

7. Short term: Require government organisations to take legal responsibility for domain suspension requests

ii. The Counter Terrorism Internet Referral Unit (CTIRU)

The CTIRU's work consists of filing notifications of terrorist-related content to platforms, for them to consider removals. They say they have removed over 300,000 pieces of extremist content.

1. Censor or not censor?

The CTIRU consider its scheme to be voluntary, but detailed notification under the e-Commerce Directive has legal effect, as it may strip the platform of liability protection. Platforms may have "actual knowledge" of potentially criminal material, if they receive a well-formed notification, with the result that they would be regarded in law as the publisher from this point on.[28]

At volume, any agency will make mistakes. The CTIRU is said to be reasonably accurate: platforms say they decline only 20 or 30% of material. That shows considerable scope for errors. Errors could unduly restrict the speech of individuals, meaning journalists, academics, commentators and others who hold normal, legitimate opinions.

A handful of CTIRU notices have been made public via the Lumen transparency project.[29] Some of these show some very poor decisions to send a notification. In one case, *UKIP Voices*, an obviously fake, unpleasant and defamatory blog portraying the UKIP party as cartoon figures but also vile racists and homophobes, was considered to be an act of violent extremism. Two notices were filed by the CTIRU to have it removed for extremism. However, it is hard to see that the site could fall within the CTIRU's remit as the site's content is clearly fictional.

In other cases, we believe the CTIRU had requested removal of extremist material that had been posted in an academic or journalistic context.[30]

Some posters, for instance at *wordpress.com*, are notified by the service's owners, Automattic, that the CTIRU has asked for content to be removed. This affords a greater potential for a user to contest or object to requests. However, the CTIRU is not held to account for bad requests. Most people will find it impossible to stop the CTIRU from making requests to remove lawful material, which might still be actioned by companies, despite the fact that the CTIRU would be attempting to remove legal material, which is clearly beyond its remit.

When content is removed, there is no requirement to notify people viewing the content that it has been removed because it may be unlawful or what those laws are, nor that the police asked for it to be removed. There is no advice to people that may have seen the content or return to view it again about the possibility that the content may have been intended to draw them into illegal and dangerous activities, nor are they given advice about how to seek help.

There is also no external review, as far as we are aware. External review would help limit mistakes. Companies regard the CTIRU as quite accurate, and cite a 70 or 80% success rate in their applications. That is potentially a lot of requests that should not have been filed, however, and that might not have been accepted if put before a legally-trained and independent professional for review.

As many companies will perform little or no review, and requests are filed to many companies for the same content, which will then sometimes be removed in error and sometimes not, any errors at all should be concerning.

2 Crime or not crime?

The CTIRU is organised as part of a counter-terrorism programme, and claim its activities warrant operating in secrecy, including rejecting freedom of information requests on the grounds of national security and detection and prevention of crime.

However, its work does not directly relate to specific threats or attempt to prevent crimes. Rather, it is aimed at frustrating criminals by giving them extra work to do, and at reducing the availability of material deemed to be unlawful.

Taking material down via notification runs against the principles of normal criminal investigation. Firstly, it means that the criminal is "tipped off" that someone is watching what they are doing. Some platforms forward notices to posters, and the CTIRU does not suggest that this is problematic.

Secondly, even if the material is archived, a notification results in destruction of evidence. Account details, IP addresses and other evidence normally vital for investigations is destroyed.

This suggests that law enforcement has little interest in prosecuting the posters of the content at issue. Enforcement agencies are more interested in the removal of content, potentially prioritised on political rather than law enforcement grounds, as it is sold by politicians as a silver bullet in the fight against terrorism.[31]

---

28 European E-Commerce Directive (2000/31/EC) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000L0031

29 https://www.lumendatabase.org

30 Communication with Automattic, the publishers of *wordpress.com* blogs

31 https://www.theguardian.com/uk-news/2017/sep/19/theresa-may-will-tell-internet-firms-to-tackle-extremist-content and https://www.bbc.co.uk/news/uk-42526271 for instance

Beyond these considerations, because there is an impact on free expression if material is removed, and because police may make mistakes, their work should be seen as relating to content removal rather than as a secretive matter.

3. Statistics

Little is know about the CTIRU's work, but it claims to be removing up to 100,000 "pieces of content" from around 300 platforms annually. This statistic is regularly quoted to parliament, and is given as an indication of the irresponsibility of major platforms to remove content. It has therefore had a great deal of influence on the public policy agenda.

However, the statistic is inconsistent with transparency reports at major platforms, where we would expect most of the takedown notices to be filed. The CTIRU insists that its figure is based on individual URLs removed. If so, much further analysis is needed to understand the impact of these URL removals, as the implication is that they must be hosted on small, relatively obscure services.[32]

Additionally, the CTIRU claims that there are no other management statistics routinely created about its work. This seems somewhat implausible, but also, assuming it is true, negligent. For instance, the CTIRU should know its success and failure rate, or the categorisation of the different organisations or belief systems it is targeting. An absence of collection of routine data implies that the CTIRU is not ensuring it is effective in its work. We find this position, produced in response to our Freedom of Information requests, highly surprising and something that should be of interest to parliamentarians.

Lack of transparency increases the risks of errors and bad practice at the CTIRU, and reduces public confidence in its work. Given the government's legitimate calls for greater transparency on these matters at platforms, it should apply the same standards to its own work.

Both government and companies can improve transparency at the CTIRU. The government should provide specific oversight, much in the same way as CCTV and Biometrics have a Commissioner. Companies should publish notifications, redacted if necessary, to the *Lumen* database or elsewhere. Companies should make the full notifications available for analysis to any suitably-qualified academic, using the least restrictive agreements practical.

4. Fols, accountability and transparency

Because the CTIRU is situated within a terrorism-focused police unit, its officers assume that their work is focused on national security matters and prevention and detection of crime. The Metropolitan Police therefore routinely decline requests for information related to the CTIRU.

The true relationship between CTIRU content removals and matters of national security and crime preventions is likely to be subtle, rather than direct and instrumental. If the CTIRU's removals are instrumental in preventing crime or national security incidents, then the process should not be informal.

On the face of it, the CTIRU's position that it only files informal requests for possible content removal, and that this activity is also a matter of national security and crime prevention that mean transparency requests must be denied, seems illogical and inconsistent.

The Open Right Group has filed requests for information about key documents held, staff and finances, and available statistics. So far, only one has been successful, to confirm the meaning of a piece of content.

During our attempts to gain clarity over the CTIRU's work, we asked for a list of statistics that are kept on file, as discussed above. This request for information was initially turned down on grounds of national security. However, on appeal to the Information Commissioner, the CTIRU later claimed that no such statistics existed. This appears to suggest that the Metropolitan Police did not trouble to find out about the substance of the request, but simply declined it without examining the facts because it was a request relating to the CTIRU.[33]

We recommend that the private sector takes specific steps to help improve the sitation with CTIRU.

Recommendations to Internet platforms:

i. Publication of takedown requests at Lumen

ii. Open academic analysis of CTIRU requests

iii. The Internet Watch Foundation (IWF)

The IWF, as a de facto Internet censor, has been popular with some people and organisations and controversial with others. The IWF deals with deeply disturbing material, which is relatively easily identified and usually uncontroversial to remove or block. This is relatively unique for content regulation.

---

32 https://www.whatdotheyknow.com/request/ctiru_statistical_methodology *"A terrorist group may circulate one product (terrorist magazine or video) – this same product may be uploaded to 100 different file-sharing websites. The CTIRU would make contact with all 100 file sharing websites and if all 100 were removed, the CTIRU would count this as 100 removals."*

33 Freedom of Information Act 2000 (FOIA) Decision notice: Commissioner of the Metropolitan Police Service; ref FS50722134 21 June 2018 https://ico.org.uk/media/action-weve-taken/decision-notices/2018/2259291/fs50722134.pdf

Nevertheless, their partners' systems for blocking have in the past created visible disruption to Internet users, including in 2008 to Wikipedia across the UK.[34] Companies employing IWF lists have often blocked material with no explanation or notice to people accessing a URL, causing additional problems. Some of its individual decisions have also been found wanting. Additional concerns have been created by apparent mission creep, as the IWF has sought or been asked to take on new duties. Its decisions are not subject to prior independent review, and it is unclear that ISP-imposed restrictions are compatible with EU law, in particular the EU Open Internet regulations, which indicate that a legal process should be in place to authorise any blocking.[35] Ideally, this would be resolved by the government providing a simple but independent authorisation process that the IWF could access.

The IWF has made some good and useful steps to resolve some of these issues.

It has chosen to keep its remit narrow and restricted to child abuse images published on websites. This allows it to reduce the risk that its approach creates over-reach. The IWF model is not appropriate where decisions are likely to be controversial.

It has an independent organisational external review, albeit this is not well-publicised, which could be a good avenue for people to give specific and confidential feedback.

The IWF has an appeals process, and an independent legal expert to review its decisions on appeal. The decisions it makes have the potential for widespread public effect on free expression, so could be subject to judicial review, which the IWF has recognised.

A significant disadvantage of the IWF process is that the external review applies legal principles, but is not itself a legal process, so does not help the law evolve. This weakness is found in other self-regulatory models.

There is also a lack of information about appeals, why decisions were made, and how many were made. There is incomplete information about how the process works.[36] Appeal findings are not made public.[37] Notifications are not always placed on content blocks by ISPs. This is currently voluntary.

Recommendations to IWF:

1. Adopt Freedom of Information principles for information requests
2. Ensure that the IWF's external evaluation process is visible and accessible by third parties
3. Ensure that processes are clearly documented
4. Require notices to be placed at blocked URLs
5. Publish information about appeals, such as: the numbers made internally and externally each year; whether successful or not; and the reasoning in particular decisions

iv. ISP content filtering

The government requested that ISPs offer content filtering to customers to help them protect children from accessing unwanted content. For the purposes of this report we would point out that filtering decisions are largely unaccountable. ISPs devolve their blocking decisions to third parties. The decisions are known to be poor, but this is usually felt to be unconcerning because they affect children, and parents can be expected to resolve particular problems by unblocking things on a case-by-case basis.

This is not much comfort to businesses or individuals whose websites are blocked, however. They may not be aware of the block if their own ISP has not blocked their website or they have not enabled the filters. If they are aware of the block, they cannot easily ask everyone to remove the block or disable all filters. Neither is it helpful for children to find that age appropriate material is blocked, nor to teachers who are responsible for helping children to learn.

It is also highly concerning that filters are often opt-out, for instance for Sky customers and many mobile phone users. Filters should always be chosen, and never imposed, on adults. We have also yet to understand the legal basis of ISP filters in relation to EU law. The Body of European Regulators for Electronic Communications (BEREC)[38] and EU Commission has indicated that they are not compatible with open Internet regulations.[39] This needs to be clarified by Ofcom as a matter of urgency.[40]

34 See https://en.wikipedia.org/wiki/Internet_Watch_Foundation_and_Wikipedia

35 See reference 38 below

36 http://web.archive.org/web/20180605155231/https://www.iwf.org.uk/sites/default/files/inline-files/Content%20assessment%20appeal%20flow%20chart%20process.pdf

37 The BBFC, for instance, operates a system of publishing the reasoning behind its content classification appeals.

38 See para 17 of the BEREC guidelines http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf

39 "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(1). Whether the end-user has the ability to disable that restriction would not affect the above assessment." http://www.europarl.europa.eu/doceo/document/E-8-2017-005328_EN.html?redirect

40 See https://wiki.openrightsgroup.org/wiki/Internet_filters_in_the_Digital_Economy_Act_and_EU_Net_Neutrality_Regulation for more details

CONCLUSION

independent supervision, authorisation and appeals

4

The government can swiftly resolve the key problems we have found with Nominet, the CTIRU and the BBFC and improve the accountability of the IWF by creating bodies that oversee key aspects of their work. In particular, a Commissioner should oversee all work involving internet takedowns and suspensions to assure that there are consistent standards being applied.

Takedown and domain suspension requests could easily be subject to a prior review before they are sent to Nominet. Additionally, it would be sensible and easy to create an independent appeals process that could handle complaints about takedown and suspension requests that covered work through Nominet, the CTIRU and the IWF.

The government must also ensure that any state regulatory body that is making content removal requests is fully transparent and accountable, including being subject to the Freedom of Information Act. Thus, in addition to the specific recommendations we have made, we recommend that the government should:

a. Extend Freedom of Information obligations to organisations regulating Internet material such as domains, among them National Trading Standards

b. Create an independent authorisation process that could be used for domain suspensions or seizures and IWF blocks

c. Create an independent appeals panel that can handle appeals relating to content requests at Nominet, the CTIRU and the IWF

d. Create a Commissioner to oversee all work relating to Internet takedown requests

The private sector also has a role to play, above and beyond its legal obligations. They should pursue the maximum transparency available. We therefore recommend that companies:

1. Ensure the publication of takedown requests at Lumen
2. Allow open academic analysis of CTIRU and Europol requests
3. Require legal frameworks rather than voluntary schemes for state requests
4. Ensure the publication of legal documents such as injunctions
5. Adopt standards such as Error 451 where content is removed or blocked for legal reasons

RECOMMENDATIONS 5

a. Recommendations to the Government

i. Future legislation should specify the need for time limits on court-blocking injunctions and mechanisms to ensure accuracy and easy review

ii. Open-ended, unsupervised injunction and blocking powers should not be granted

iii. Administrative blocking should be rejected

iv. Extend Freedom of Information obligations to organisations regulating Internet material such as domains

v. Create an independent authorisation process that could be used for domain suspensions or seizures and IWF blocks

vi. Create an independent appeals panel that can handle appeals relating to content requests at Nominet, the CTIRU and the IWF

vii. Create a Commissioner to oversee all work relating to Internet takedown requests

viii. Remove obligation to block websites for pornography

ix. Cease obligations to the BBFC to notify ASPs for voluntary measures

b. Recommendations to the private sector (platforms, domain registrars and ISPs)

i. Publication of takedown requests at Lumen

ii. Open academic analysis of CTIRU requests

iii. Require legal frameworks rather than voluntary schemes

iv. Publication of legal documents

v. Adopt standards such as Error 451 where content is removed or blocked for legal reasons

c. Recommendations to courts granting blocking injunctions and to parties to the injunctions

i. Current injunction-holders and ISPs must urgently reduce the error rates within their lists as incorrect blocks are unlawful

ii. Courts should reflect on the current problems of accuracy in order to ensure future compliance with injunctions

iii. Require blocking notices to link to legal documents such as a judgment and court order

iv. Require blocking notices to explain who holds the injunction to block the specific URL requested

v. Ensure that there is transparency over what domains are blocked

vi. Ensure duties exist for ISPs and rights-holders to check block lists for errors

d. Recommendations to Nominet

i. Adopt Freedom of Information principles

ii. Ask government for a legal framework for domain suspensions based on court injunctions for domain seizures

iii. Require notices to be placed after seizures to explain the legal basis and outline any potential dangers to consumers posed by previous sales made via the domain. This could include contact details for anyone wishing to understand any risks to which they may have been exposed

iv. Short term: Offer an independent review panel

v. Short term: Require government organisations to publish their policies relating to domain suspension requests

vi. Short term: Publish the list of suspended domains, including the agency that made the request and the laws cited

vii. Short term: Require government organisations to take legal liability for domain suspension requests

e. Recommendations to IWF

i. Adopt Freedom of Information principles

ii. Ensure that third parties are aware of the IWF's external evaluation process

iii. Ensure that processes are clearly documented

iv. Require notices to be placed at blocked URLs

v. Publish information about appeals, such as: the numbers made internally and externally each year; whether successful or not; and the

f. Recommendations to BBFC

i. Ask for the application of the FOI Act to the BBFC's statutory work

g. Recommendations to National Trading Standards

i. Ask for the application of the FOI Act to National Trading Standards' work

APPENDIX A

Organisations claiming a role in content regulation

This information has been compiled by Open Rights Group and is maintained on our public Wiki, with references and links.[41]

These organisations regulate Internet content in the UK, along with preliminary information about their governance, transparency, accountability and oversight arrangements.

Crime

The Counter-Terrorism Internet Referral Unit (CTIRU): produces a single statistic of takedown requests. It appears to lack any formal oversight of its takedown requests and refuses to be transparent in its work work, applying FoI exemptions to everything it does. The CTIRU also make requests for domain suspensions to Nominet, again without supervision.

The National Police Chiefs' Council: has a role co-ordinating counter-terrorism police work, including that of the CTIRU. The NPCC is not subject to the FoI Act, although it does respond to requests.

The Home Office: administers the CTIRU's list of websites to block across the public estate, with no oversight of the list or information about where or why it is applied. There is no oversight of any potential monitoring or information flow relating to persons making visits to sites on the list. There is no oversight of relationships with vendors within the programme.

The National Crime Agency: engaged in some takedowns, and is entirely exempt from FoI. It is unclear what, if any, oversight is applied to takedown or suspension requests.

The Internet Watch Foundation (IWF): a private company and charity, and lacks FoI obligations, although it acknowledges it acts as a state authority when blocking child abuse material. It is unclear what its current presentation of block pages is, and whether this is any help for victims, or what impact it might have on people thinking about breaking the law or correcting errors.

The Crown Prosecution Service (CPS): prosecutes cases on a basis that can often be unclear, despite the guidelines.

41 https/:wiki.openrightsgroup.org/wiki/UK_Internet_content_regulation

General

Nominet: a private company, is subject to DEA 2010 clauses that allow the government to disempower it in the event of it failing to meet public objectives. It is not subject to FoI in relation to these public objectives. It is transparent in general terms, but it recently reduced transparency about its governance. There is no transparency surrounding the 16,000 domains suspended via the Police Intellectual Property Crime Unit (PIPCU) and others, except in numerical terms. It is no longer transparent in terms of governance.

Ofcom (The Office of Communications): is subject to high levels of transparency and accountability, but as of yet it has no clear policy or accountability around net neutrality complaints and violations.

Consumer protection

Police Intellectual Property Unit (PIPCU): is subject to FoI and has been very co-operative in this regard. There is no formal oversight of their takedown work. It removes over 13,000 domains annually via Nominet. These are mostly related to trademark violations, fake goods and fraud.

National Fraud Intelligence Bureau: makes domain suspension requests to Nominet. There is no formal oversight of these requests.

Veterinary Medicines Directorate of the Department for Environment, Food and Rural Affairs: makes domain suspension requests to Nominet. There is no formal oversight of these requests.

The Metropolitan Police Fraud and Linked Crime Online (FALCON): makes domain suspension requests to Nominet. There is no formal oversight of these requests.

The Medicines and Healthcare Products Regulatory Agency (MHRA): makes domain suspension requests to Nominet. There is no formal oversight of these requests.

National Trading Standards: a private company not subject to FoI or external oversight, which co-ordinates local trading standards' work. It makes domain suspension requests to Nominet.

The Gambling Commission: regulates gambling for the UK, and requires non-UK-hosted Internet gambling sites to hold a licence, which includes an obligation for age verification.

Intellectual property

The Intellectual Property Office (IPO): supports PIPCU's work and has a role in its governance, as well as having a role in wider IP enforcement. It is unclear whether e-commerce advice and policy development for IP takedowns comes under its remit, or a matter for another body.

Court injunctions for blocks: Court injunctions delegate responsibility for the identification of duplicate sites and are obtained by various private organisations that have copyright or trademark claims, such as the British Phonographic Industry or the Music Publications Association. No transparency over their role in error correction on block pages. Confusing block pages at ISPs.

The Federation Against Copyright Theft (FACT) has issued domain seizure requests to registrars and redirected domains to a redirect page.

Child protection

ISPs: implement soft blocking, which is lacking any legal requirements for user choice, error correction or visibility of what is blocked. It is most likely in violation of net neutrality laws barring ISPs from interfering with internet traffic.

The BBFC: a private company, it has has statutory duties in different legislation. It acquires new duties for blocking under the Digital Economy Act 2017. Generally, it is reasonably transparent, but not subject to FoI. It provides limited accountability for specific mobile operators' website blocks, and publishes reasons for decisions about specific complaints.

The UK Council for Child Internet Safety: responsible for industry co-ordination, but often tasked with patching up problems generated by government-pushed policy, such as Internet filters. Although it is transparent and subject to FoI as a government initiative, it is unclear in its accountability as its measures generally count as industry self-regulation.

UK Safer Internet Centre: Provides advice aimed at protecting children online.

Internet Matters: an industry-led initiative to educate parents in matters of child protection, but also provides advice to website operators about getting sites unblocked.

APPENDIX B
informal transparency and accountability

a. Blocked.org.uk

ORG's Blocked project monitors both filtering blocks and copyright blocks. We look at transparency, errors and complaints in each case using technical means. This allows us to better understand the scale of problems caused by both, and the specific kinds of problem caused.

A separate report covers the kinds of problems arising from filtering. Advice, counselling and LGBT+ material is very prone to blocking, for instance. We have been able to demonstrate that many legitimate businesses are routinely blocked.[42]

Relating to copyright blocking, we uncovered serious maladministration of the blocking lists. Thirty-eight percent of domains blocked by one or more ISPs should not have been blocked under the terms of the injunctions at the time of the tool's release in April 2018. After releasing our results, ISPs have begun to correct the mistakes we had identified. Nevertheless, we cannot test all sites blocked by injunction, as the lists are not public. As around 2,500 domains are blocked, we could expect approximately 950 domains (some in use, others for sale or parked) to be blocked incorrectly, given the 38% error rate we established.

b. Lumen database

The Lumen database allows companies to submit takedown requests from any party so that academics, journalists and the public can understand what kind of content removal requests take place.

Google, Oath (which includes Yahoo), and Twitter are the major contributors at present. Most of the requests relate to Digital Millennium Copyright Act notifications. Some CTIRU requests have also been filed, mostly in redacted form. These have been very helpful in allowing us to see the likely scale of the CTIRU's work, which we believe to be significantly smaller than that outlined by government ministers to parliament.

Some companies are not currently submitting takedown notices to Lumen. Even redacted notices are better than none at all. We would also like to see UK ISPs and domain registrars submitting information to Lumen.

c. Freedom of Information

One way to try to establish some kind of transparency relating to content takedowns is to request information about the practices. ORG, journalists and individuals have attempted to find out about the CTIRU's work, and the agency's requests to Nominet for domain suspensions. Often the response has been patchy. Law enforcement tends to expect to deny access to documents because of law enforcement exemptions and, in the CTIRU's case, national security.

One exception to this has been the PIPCU. While some information requests have been turned down, it provided us with most documents we requested. This has been very helpful. While we believe that improvements need to be made, this baseline approach of giving us access to their policy documents shows that transparency can be applied even to police work. It also means that any criticism we make can be more focused and helpful.

While there are no other means to establish the reasons for action being taken, agencies need to be as open as possible with the public about their actions. The public interest in establishing basic information and content removals should be uppermost in agencies' thinking when responding to FoI requests.

APPENDIX C
organisations consulted

In the course of the this report, we discussed the approaches taken directly with the folllowing organisations, who we would like to thank for their co-operation:

BT; Facebook; Internet Watch Foundation; TalkTalk; National Trading Standards; Nominet; Police Intellectual Property Crimes Unit; Sky.

42 Forthcoming ,Open Rights Group .See also https/:www.blocked.org.uk/lists for lists of legitimate ,non-harmful business and local websites that have been blocked in error or on purpose by filters

**Written by Jim Killock, Executive Director,
Open Rights Group**

Open Rights is a non-profit company limited by Guarantee, registered in England and Wales no. 05581537

Open Rights Group, Unit 7, Tileyard Acorn Studios, 103-105, Blundell Street, London, N7 9BN

Registered Office: 12 Duke's Road, London WC1H 9AD

www.openrightsgroup.org/contact/

www.openrightsgroup.org