

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

**Big Brother Watch's Written
Evidence to the Communications
Committee's Inquiry, *The Internet: to
regulate or not to regulate?***

October 2018

About Big Brother Watch

Big Brother Watch is a cross-party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK. We expose and challenge threats to people's privacy, freedoms and civil liberties at a time of enormous technological change in the UK.

Contact

Silkie Carlo

Director

020 7340 6042

silkie.carlo@bigbrotherwatch.org.uk

Griff Ferris

Legal & Policy Officer

020 7340 6074

griff.ferris@bigbrotherwatch.org.uk

Contents

Introduction	3
Q1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?	3
<i>Regulation of expression must be based on international human rights law</i>	4
<i>Regulation of targeted advertising</i>	6
Q2. What should the legal liability of online platforms be for the content that they host?	8
Q3. How effective, fair and transparent are online platforms in moderating the content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?	9
<i>Effective or fair?</i>	9
<i>Transparency</i>	10
<i>Notification, appeal and remedies</i>	11
Q5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?	11
<i>Automated content monitoring and moderation systems</i>	11
<i>Online anonymity and encryption</i>	12
Q4. What role should users play in establishing and maintaining online community standards for content and behaviour?	13

Introduction

1. Internet and social media companies have become central platforms for discussion and debate, for information access, for commerce and increasingly even human development.¹ This has given internet and social media companies – primarily a small number of global, for-profit companies – a critical role mediating people’s ability to freely express themselves and their opinions online. Existing regulatory frameworks applied to these global platforms range from diverging national laws to self-regulatory guidelines produced by internet companies themselves. Big Brother Watch believes it is entirely possible and desirable to construct a harmonious online environment where expression is free and people’s privacy is protected, and where the rule of law is upheld.

Q1. Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

2. Firstly, it is important to acknowledge that the internet is a complex environment comprising communications networks, information storage and sharing, multiple forms of commerce, and many non-profit endeavours. The internet is an extension of society itself, and accordingly there is not simple or desirable way of ‘regulating the internet’ as a whole sphere. Indeed, many actions carried out on the internet are already subject to regulation in various forms. This is particularly the case with communications, which we wish to consider further in this submission.
3. Secondly, we believe that before deciding on a method by which to achieve change – regulation or otherwise - parliament, the public, and internet intermediaries still need to have a meaningful and engaging conversation about exactly what changes are needed to benefit society.
4. Big Brother Watch believes that the status quo needs to change. **We believe that internet intermediaries of a certain size, particularly social media platforms and search engines, should only restrict free expression to the extent that that right is limited in human rights law; and that any enforcement action should be safeguarded by transparent policies and clear and accessible appeals processes.** Whether it is desirable or moreover possible to achieve that model via the provision of new regulation is an outstanding question. However, with or without regulation, there is much more Government and the intermediaries can do.

¹ 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/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>)

5. Social media companies have become the modern public square, whilst search engines are like supersized modern libraries. These internet intermediaries have enabled the open and democratised sharing of information, and provided platforms for people to speak truth to power. Social media platforms in particular have connected people to engage in politics, form communities, to share views and debate. With over two billion users actively using Google and Facebook respectively, these internet companies are operating at a magnitude whereby they function as part of our modern communications infrastructure – much like public utilities. Therefore, any regulation of these companies implicates people’s rights to privacy, religious freedom and belief, opinion and expression, assembly and association, and public participation.² Accordingly, Government and the companies alike should ensure that people’s rights and freedoms are protected, and that the same harms proscribed by law and dealt with in the physical world are dealt with on the internet.

6. Since internet intermediaries are our modern public squares and super-libraries, it is really important for the health of society and democracy that they are not regulated or interfered with beyond those basic human rights principles. ‘Community values’ are not appropriate for a platform hosting billions of users – the notion of one community in this context is a fiction. The fictional ‘community’ is a notion used to justify enforcement policies and actions that pertain to the legal protection or simply the brand identity of the platform. But in reality, there is not one online community, or one Facebook community, but many thousands of communities on these platforms each with different values, interests, and norms. To provide an inclusive platform where rights are respected, ‘community values’ should not be thrust upon such a large number of users - only the legal boundaries within which they live.

Regulation of expression must be based on international human rights law

7. As discussed, we believe that any regulation of online content on major internet platforms should be based on international and national human rights standards, with close regard due to the right to freedom of expression and the right to privacy which are particularly affected.³ This is the most inclusive way to host diverse communities and individuals, and to foster the open exchange of ideas, the development of views, and healthy debate.

² 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/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>)

³ 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/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>)

8. The first step to adherence to human rights standards would be for the major internet intermediaries to pledge to follow such a model and open their processes and policies to independent inspection by expert bodies. The Government should actively support such a process.
9. We see no purpose in Government creating additional legislation to further restrict content, speech or other forms of expression online beyond the restrictions imposed by existing human rights law and the current roster of communications laws in the UK. There are already a wide range of UK laws prohibiting violent and discriminatory forms of speech, including the Protection from Harassment Act 1997, Crime and Disorder Act 1998, Public Order Act 1986, Malicious Communications Act 1988, Communications Act 2003, and the Terrorism Act 2006.
10. It is already, for example, an offence to use “insulting words” whereby a person is “likely to believe that (...) it is likely that (*immediate unlawful*) violence will be provoked” - regardless of whether such violence is provoked (Public Order Act 1986, s.4). It is an offence to display “any writing, sign or other visible representation” that is “insulting” and causes a person “alarm or distress” (Public Order Act 1986, s.4A) or even “within the hearing or sight of a person likely to be caused harassment, alarm or distress” (Public Order Act 1986, s.5). Furthermore, it is an offence to send “a message that (*an individual*) knows to be false” for the purpose of causing “annoyance” or “inconvenience” (Communications Act 2003). Arguably, communications laws in the UK are already extensive and overly restrictive.
11. The vastly increased means by which to publicly exchange communications have given rise to unprecedented opportunities to monitor, regulate and restrict expression. As such, this is an important juncture for Government to consider reviewing existing laws that deal with the limitations on free expression to ensure that they are simple, accessible, compatible with Article 10 rights and conducive to a free and open society - rather than disproportionately censorious.
12. Government should apply UK laws dealing with the rights and limitations on free expression to the online sphere. The Director of Public Prosecutions’ has already indicated that online hate crimes can be prosecuted to the same degree as offline hate crimes.⁴

⁴ <https://www.independent.co.uk/news/uk/politics/hate-crimes-social-media-crown-prosecution-service-home-office-prejudice-a7903166.html>

13. It has been reported that Government is considering proposals to regulate ‘non-illegal content’.⁵ Any such proposals would clearly risk a disproportionate restriction on the right to freedom of expression. Big Brother Watch will robustly oppose any regulation that would risk eroding or chilling that vital right.
14. We are also opposed to the fledgling proposals set out in two Bills set to have their second reading in Parliament on 26th October 2018: the Social Media Service Providers (Civil Liability and Oversight) Bill presented to Parliament by John Mann MP,⁶ and the Online Forums Bill presented to Parliament by Lucy Powell MP.⁷
15. John Mann MP justified the necessity of his ‘Social Media Service Providers (Civil Liability) Bill’ with the argument that it’s impossible for police to force Internet platforms to provide evidence in criminal prosecutions.⁸ However this is incorrect, as UK police have the power to do so under the Regulation of Investigatory Powers Act 2000.
16. Lucy Powell MP’s ‘Online Forums Bill’ is intended to combat private groups on social media that are considered breeding grounds for hate and proposes making group administrators and moderators legally liable for the content in those groups. Whilst there is certainly an issue with hateful content online, as there is offline, this fundamentally flawed proposal would undoubtedly result in a shrinking space for community groups to discuss and organise amongst themselves. The burden of legal liability would deter most communities from maintaining their online groups, worst affecting minorities such as LGBT groups; those who are vulnerable or already suffer discrimination, such as women’s groups; and those who require on privacy and anonymity such as recovery or survivor groups, who rely on closed spaces for discussion and organisation. The problem of hate crime that Lucy Powell MP is understandably drawing attention to could, we believe, be dealt with under existing laws.

Regulation of targeted advertising

17. Big Brother Watch believes that parliament should consider passing an Act to prohibit micro-targeted advertising online. Targeted advertising is the practice of collecting data about internet users, including tracking users across websites and inferring their

⁵ <https://www.buzzfeed.com/alexwickham/uk-government-regulator-internet>

⁶ [https://hansard.parliament.uk/commons/2018-02-28/debates/18022838000002/SocialMediaServiceProviders\(CivilLiabilityAndOversight\)#contribution-151690EC-1DCA-4C1F-BE73-4F28F260A08F](https://hansard.parliament.uk/commons/2018-02-28/debates/18022838000002/SocialMediaServiceProviders(CivilLiabilityAndOversight)#contribution-151690EC-1DCA-4C1F-BE73-4F28F260A08F)

⁷ <https://hansard.parliament.uk/commons/2018-09-11/debates/BC2267F0-86BB-4746-B822-D6D8A55F31BF/OnlineForums>

⁸ “It is absurd that the police in this country cannot force Twitter, Facebook, Google or any of the others to provide evidence that is required for criminal prosecutions.” 28 February 2018
[https://hansard.parliament.uk/commons/2018-02-28/debates/18022838000002/SocialMediaServiceProviders\(CivilLiabilityAndOversight\)#contribution-151690EC-1DCA-4C1F-BE73-4F28F260A08F](https://hansard.parliament.uk/commons/2018-02-28/debates/18022838000002/SocialMediaServiceProviders(CivilLiabilityAndOversight)#contribution-151690EC-1DCA-4C1F-BE73-4F28F260A08F)

interests, in order to target tailored advertisements.⁹ This practice is enabled by the vast monitoring and tracking capabilities in the online sphere.

18. The very nature of targeting advertising, tracking and profiling users based on their browsing history; purchasing habits; sociodemographic traits such as age, gender, race, economic status; psychographic characteristics such as lifestyle, opinions and values; and geographic location is inherently privacy-invasive. To seek this level of detail about individuals' private lives for the purpose of commercial or political advertising is unethical and makes for an unhealthy online environment. In extremis, such targeted advertising could even jeopardise the integrity of our democratic processes – an issue raised by the Cambridge Analytica scandal this year.

19. For example, Facebook tracks users through 'Like' buttons across the internet, whether or not they are logged in, or even have a Facebook account;¹⁰ it maintains shadow profiles on people who don't use Facebook;¹¹ and it tracks location and targets adverts based on where an individual is, where they live, and where they work.¹² Facebook allows advertisers to target people in several different ways: through their demographics, including "age, gender, relationship status, education, workplace, job titles and more"; their interests, including their "hobbies, favourite entertainment and more", whereby advertisers group users based on specific words shared on their timelines; through their behaviors, including "purchasing behavior, device usage and other activities", and their location.¹³ For example, Facebook has allowed advertisers to run adverts that target only men or certain ethnic groups,¹⁴ and has allowed predatory "conversion therapy" adverts to be aimed at vulnerable young gay men.¹⁵

20. Advertising provides a lucrative revenue stream for social media platforms, which is only growing as those platforms consume more and more human attention. However, advertising on specific platform webpages would also be lucrative, without needing to target adverts at the individual level. **Big Brother Watch calls for a ban on micro-targeted advertising online.**

⁹ Toubiana, V, Narayanan, A, and Boneh, D, Nissenbaum, H and Barocas, S, 'Privacy Preserving Targeted Advertising' (2010). 'Proceedings Network and Distributed System Symposium', March 2010.

¹⁰ <https://gizmodo.com/all-the-ways-facebook-tracks-you-that-you-might-not-kno-1795604150>

¹¹ <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy>

¹² <https://www.eff.org/deeplinks/2018/04/facebook-doesnt-need-listen-through-your-microphone-serve-you-creepy-ads>

¹³ <https://en-gb.facebook.com/business/products/ads/ad-targeting>

¹⁴ <https://www.telegraph.co.uk/technology/2018/09/18/facebook-accused-discriminating-against-women-targeted-job-adverts/>

¹⁵ <https://www.telegraph.co.uk/news/2018/08/25/facebook-accused-targeting-young-lgbt-users-gay-cure-adverts/>

Q2. What should the legal liability of online platforms be for the content that they host?

21. Internet platforms are not arbiters of the law – like other companies, they are subject to the law. In addition, social media networks and search engines are clearly not publishers, but intermediaries. Therefore, they should not be held liable for third party or user content on their platform that they were not involved in modifying, or for failing to identify illegal content. They should only be liable for failure to adhere to lawful orders, such as court orders to remove content.
22. Intermediaries' technical ability to perform a quasi-policing function does not equate to a legal or even moral responsibility to do so – nor would their fulfilling such a function necessarily benefit society. The line between free speech and censorship is delicately maintained and is an indicator of democratic health. Adjudications around that line are complex and should not be deputised to private companies.
23. Any determination of whether content produced by a user is illegal is a determination that may result in the removal and restriction of that content, and therefore engages that user's right to freedom of expression. On platforms that function in practice as part of the modern communications infrastructure with billions of users, such restrictions on individuals' freedom of expression should ideally not be for a private company to determine, but an independent and impartial judicial authority in accordance with due process standards of legality, necessity and legitimacy.¹⁶ Since, in practice, companies do routinely make censorship decisions, we believe they should limit enforcement action to the standards set by human rights law whilst opening up their processes to independent audit and appeals, as discussed above.
24. Forcing internet intermediaries to accept liability for content on their platforms would likely incentivise them to be overly cautious and zealous in their approach to censoring content in order to avoid liability. It would undoubtedly result in internet platforms more actively monitoring, surveilling and censoring content on their platform at a mass scale – either by automated enforcement systems or non-judicial human moderators with extremely high workloads and limited decision-making time. These processes are not only likely to result in incorrect, inconsistent, and arbitrary decisions restricting people's right to freedom of expression, but would also lead to a generalised and persistent invasion of people's privacy. These regimes of regulation and online surveillance have a

¹⁶ 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/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>); Article 19, 'Internet Intermediaries: Dilemma of Liability, 20 August 2013 (https://www.article19.org/wp-content/uploads/2018/02/Intermediaries_ENGLISH.pdf)

chilling effect on freedom of expression as users, knowing they are being watched and monitored online, self-censor.¹⁷

Q3. How effective, fair and transparent are online platforms in moderating the content that they host? What processes should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for overseeing this?

Effective or fair?

25. Online platforms have not been sufficiently effective, fair or transparent in their moderation of content. There are innumerable cases of violent and plainly prohibited content remaining live, despite flagging and reporting; and innumerable cases of plainly unfair, overly zealous censorship.
26. The censorship of controversial right-wing media platform Infowars has been the first high profile example of an internet-based media outlet being virtually eliminated from common space by intermediaries, and demonstrates the deficiency in consistently effective, fair and transparent moderation. Rules had been applied to the platform sporadically and ineffectively, resulting in a public backlash that culminated in an impromptu industry-wide deplatforming after Apple delisted Infowars' podcasts. Bans by YouTube, Facebook, Twitter, Spotify, Paypal, MailChimp, LinkedIn, Discus and more followed, within days. The enforcement action lacked not only effectiveness, but fairness and transparency too - despite the prevalence of misogynistic and race-baiting content, almost all of the removals were unrelated to specific posts or videos and the reasons given were generalised ones. Operators were not notified as to exactly what content was harmful or what decisions could be appealed. Critically, millions of Infowars' mostly right-wing viewers and listeners are likely to now feel a toxic combination of important and silenced – an incendiary mix. The platforms missed numerous opportunities to demonstrate they could be responsible and even-handed regulators, and finally missed an opportunity to show, with total clarity, exactly how Infowars had caused harm or breached fair rules. This alarming incident sets a dangerous precedent.
27. It is not only the enforcement of rules that is questionable, but the rules themselves. Some policies, which are rarely publicised in detail to receive close scrutiny, risk

¹⁷ <https://pen-international.org/app/uploads/Surveillance-Secrecy-and-Self-Censorship-New-Digital-Freedom-Challenges-in-Turkey.pdf>

suppressing legitimate speech while allowing abuse against marginalised groups.¹⁸ Allowing major internet companies to design and arbitrate free expression rules on their platforms has resulted in “platform law” in which “clarity consistency, accountability and remedy are elusive”.¹⁹ These platforms are enforcing systems of governance that are constantly changing, unaccountable, and opaque.²⁰ Platforms’ moderation of content has been shown to be influenced by financial motivations, such as the threat of losing advertising²¹ or losing users.²²

28. As it stands, people’s rights risk being arbitrated and even eroded by private intermediaries. It is vital that the internet intermediary companies inspire public trust and confidence in their judgments. They must take their responsibility to protect users from violent and unlawful content as seriously as their duty to uphold and promote free expression. Sensitive decisions about what is and is not permissible speech or information need to be made transparently and delivered honestly, objectively and equitably. The rules must be fair and, if they are breached, there should be clear, foreseeable consequences. Following a due process model along these lines would also mean that users would have the opportunity to appeal decisions.

29. Encouraging the major private, profit-driven internet platforms to create novel definitions for permissible and prohibited expression, and deal with the multitude of complex related issues, would allow them to set the standards by which modern society is governed and to shape the major public squares of the internet in their own moral image. That is why we believe Government should work with major intermediaries to ensure that their rules mirror international human rights law on freedom of expression and privacy, as well as UK laws, and are restricted to those standards.

Transparency

30. Internet intermediaries’ policies and enforcement processes should be transparent. Some have avoided such transparency claiming that users will adapt their behaviour to evade rules. However, this is illogical and undemocratic – we do not shield criminal law

¹⁸ ProPublica, ‘Facebook’s Secret Censorship Rules Protect White Men From Hate Speech But Not Black Children’, 28 June 2017 (<https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms>); <https://www.thedailybeast.com/exclusive-rohingya-activists-say-facebook-silences-them>; <https://www.wired.com/story/facebooks-hate-speech-policies-censor-marginalized-users/>; https://motherboard.vice.com/en_us/article/mbk7ky/leaked-facebook-neo-nazi-policies-white-supremacy-nationalism-separatism

¹⁹ 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/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>)

²⁰ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937985

²¹ <https://www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054>; <https://www.telegraph.co.uk/technology/2018/04/20/youtube-accused-still-airing-adverts-extremist-videos/>

²² <https://www.telegraph.co.uk/news/uknews/crime/11392109/Twitter-boss-admits-company-sucks-at-tackling-trolls.html>

from scrutiny for fear of the same. Rules must be accessible, and the consequences of breaching them should be foreseeable.

31. Intermediaries should produce comprehensive transparency reports reporting on enforcement actions, as well as Government requests for restriction and removals, whether statutory or informal requests. We welcome the initial reports of some platforms in this regard.²³

32. Government must also be transparent. The increasing use of extra-judicial mechanisms to censor and remove content online by authorities is very concerning. Transparency reports should include details on Government takedown requests to internet platforms, via statutory processes as well as any other informal mechanisms. This should include information on the reasons for removal requests and the outcomes of requests.

Notification, appeal and remedies

33. Platforms should provide users with immediate notice of any enforcement action taken, as well as the reasons for the decision and information about their options, including appeals. Platforms should provide users with an appeals process to dispute enforcement actions such as content removal, restriction or user suspensions. The appeals mechanism should follow a due process model, and meaningful remedies should be available.

Q5. What measures should online platforms adopt to ensure online safety and protect the rights of freedom of expression and freedom of information?

34. Platforms should implement consistent, harmonised and structured processes for users – and law enforcement – to report allegedly illegal content. Platforms should improve reporting tools and the information given to users, so that these are easily and clearly available, with sufficient signposting and reporting mechanisms allowing users to report illegal content to both the platform and the police. Platforms should temporarily block the most serious content (such as threats of violence, sexual abuse imagery) pending the outcome of a formal review.

Automated content monitoring and moderation systems

35. Automated content restriction systems such as image hashing algorithms should only be used in extremely limited circumstances against narrow, clearly defined and

²³

<https://www.eff.org/who-has-your-back-2018>; <https://transparencyreport.google.com/?hl=en>

specified content that has already been held to be illegal – for example, known child sexual abuse or terrorist content that has been prohibited through due process.²⁴ Any automated technology used for content moderation should be transparent, rigorously audited and subject to an appeals mechanism.

36. Academic studies have shown the difficulty with creating successful content or comment filters that can distinguish between speech that is offensive but lawful and speech that is illegal.²⁵ Studies have also demonstrated that automated systems are unable to understand the complexity of human language,²⁶ specifically “the meaning of human communication” or to “detect the intent of the speaker”.²⁷ Even automatic tools that scan music and video for copyright infringement at the point of upload have raised concerns of “overblocking”.²⁸

37. It is only appropriate to use such technology in relation to material already deemed unlawful. Automated filtering, flagging or restriction algorithms are not able to sufficiently analyse rhetorical devices such as satire, parody or irony in text or images. Such technology often results in arbitrary and incorrect restrictions of speech, rendering these tools entirely insufficient to the task of making determinations about unique content online. There should always be a human review of any unique content that is considered for restriction or removal.

Online anonymity and encryption

38. Online anonymity and encryption are key guarantors of the right to freedom of expression and opinion, and the right to a private life.²⁹ Anonymity allows people to express themselves freely, speak truth to power, and blow the whistle. As the former UN Special Rapporteur on Freedom of Expression, Frank La Rue, noted: “throughout history, people’s willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously.”³⁰ Government should not unduly interfere with tools that allow people to remain anonymous online.

²⁴ <https://www.iwf.org.uk/our-services/image-hash-list>

²⁵ Davidson, T, Warmley, D, Macy, M, and Weber, I, ‘Automated hate speech detection and the Problem of Offensive Language’, 11 March 2011 (<https://arxiv.org/abs/1703.04009>)

²⁶ <https://www.eff.org/files/ai-progress-metrics.html#Reading-Comprehension>

²⁷ Duarte, N, Llanse, E, Loup, A, ‘Mixed Messages? The Limits of Automated Social Media Content Analysis’, 2018 (<https://cdt.org/files/2017/12/FAT-conference-draft-2018.pdf>)

²⁸ 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/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>), page 12

²⁹ UN Special Rapporteur, ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’, 2015

(https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc)

³⁰ UN Special Rapporteur, ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 16th May, A/HRC/17/27.

(www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

Government should never require internet platforms to implement real-name requirements, or ID-related age verification requirements.

39. Encryption protects digital communications so that people can express themselves privately and securely. It is used to protect private communications, health data, financial transactions, and other sensitive transfers of information online.³¹ Government should never require internet platforms or indeed any other communications providers to allow ‘backdoor’ access to encrypted communications. Government should expressly protect encryption tools.

Q4. What role should users play in establishing and maintaining online community standards for content and behaviour?

40. Users should be able to curate their own communities and environments. It would be good practice for platforms to make tools available for users to protect themselves from various categories of content, ensuring such tools do not restrict others’ free expression. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression advocates for user autonomy in the creation of online spaces, encouraging tools that allow users to “shape their own online environments”.³² This includes muting or blocking other users or specific kinds of content, or the use of private groups moderated by users themselves. Major internet platforms should provide the means for affinity-based groups to form given their “value in protecting opinion, expanding space for vulnerable communities and allowing the testing of controversial or unpopular ideas.”³³

Silkie Carlo

Griff Ferris

³¹ <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>

³² <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>

³³ <https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf>