ANTISEMITISM POLICY TRUST

Regulating Online Harms: TACKLING ANONYMOUS HATE

Contents

This report was co-authored by Dr. Limor Simhony, a policy advisor and researcher.

Published by the Antisemitism Policy Trust, copyright © 2020
Antisemitism Policy Trust is a registered charity (1089736) [England] and company (04146486) [England and Wales]

Introduction

The expansion of the internet from half a percent of the world population in 1990, to three quarters of the people in the US alone by 2016[1], has had many advantages. One of these is the ability to communicate with a large number of people anywhere in the world. However, there are also drawbacks to this vast communication ability, particularly when radicals, racists and bullies use online platforms to disseminate hatred and bigotry and adopt anti-social behaviour that often includes hate-speech. Frequently, those utilising an aggressive discourse choose to remain anonymous online, hiding their true identify for nefarious reasons.

Placing restrictions on anonymity of online users has been the subject of a continuing debate. Those supporting these restrictions claim they will reduce bullying and hate speech by promoting accountability. Those opposing restrictions, claim that rights to anonymity and privacy are fundamental, especially for vulnerable individuals, dissidents and others, and should therefore be guarded.

The UK Government's Online Harms White Paper recommended a review of current law enforcement powers for tackling anonymous abuse and that steps be taken "…to limit anonymised users abusing their services, including harassing others."[2]

The Antisemitism Policy Trust supports the approach set out in the White Paper. This briefing argues that the effect of anonymity on online discourse is harmful enough to merit regulation that will, on the one hand, allow some degree of anonymity while also reducing harms and protecting users.

[1] https://ourworldindata.org/internet

[2] 'Online Harms White Paper', The Department of Digital, Culture, Media & Sports and The Home Department, April 2019, p.70

Why is anonymity a problem?

Extremists, racists and bullies have been disguising their identities to avoid accountability and prosecution from before the internet was invented. Notorious examples include members of the Ku Klux Klan (KKK), who have traditionally disguised themselves with robes and hoods for anonymity. Islamist extremists also often disguise themselves in public images and videos that include violent extremism. The internet now offers anonymous abusers and spreaders of radical and violent ideologies some degree of protection by allowing them to hide their identities.

Anonymity can undoubtedly have positive effects, for example on a person's psychological wellbeing and an increased sense of freedom to express emotions and opinions.[3] However, there is a growing body of evidence establishing the positive correlation between online anonymity and the expression of extremist, racially biased and prejudiced hate-speech.

Anonymity, for example, can lead to group polarisation; the tendency of like-minded members of a collective to become more extreme in their views following group discussions.[4] One study found there was a much higher chance of group polarisation within anonymised computer-mediated communications (CMC) settings than within an identified face-to-face setting.[5] Meanwhile, a study from 2019 found that high levels of anonymity among Twitter users was a significant predictor of online expressions of extreme radical attitudes and behaviours, extreme anti-social behaviour and extreme prejudicial bias.[6]

Another recent analysis of online anonymity concluded that it can influence behaviour 'by reducing societal boundaries in human attitudes.'[7] The researchers studied the conduct of users on anonymous platforms, including Whisper and 4Chan. They determined that anonymity made user behaviour increasingly aggressive and violent by producing environments less constrained by social norms. Adding to these findings, another team of investigators who interviewed young social media users found that being anonymous allows users to express intolerance, racism and prejudice 'without the social limitations that exist in offline communication.'[8]

The Community Security Trust (CST) noted in its most recent report, that 44% of the 789 recorded antisemitic incidents between January and June 2020 occurred online, adding that "online platforms represent a convenient, far-reaching, anonymising and secure-feeling environment for those who wish to voice and incite hatred."[9] Some of those incidents included coordinated campaigns of antisemitic harassment aimed at Jewish public figures and other individuals.

The Covid-19 pandemic affected antisemitic incidents in two ways. First, there was an overall fall in incidents owing to the national lockdown, but an increase in online abuse – representing the highest number ever recorded by CST in the first half of a year. A great deal of the abuse was carried out anonymously, including leaving voice recordings and using antisemitic usernames. Second, was a rise in antisemitic conspiracy theories and the use of antisemitic rhetoric and stereotypes with reference to the pandemic.
In both, the internet and the ability for users to remain anonymous, was a significant factor in the dissemination of antisemitic hate speech and abuse.

[3] Christopherson, K. 'The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog.' Computers in Human Behaviour, 23 (2007), pp.3038-3056. https://www.researchgate.net/profile/Kimberly_Christopherson/publication/222428988_The_positive_and_negative_implications_of_anonymity_in_Internet_social_interactions_On_the_Internet_Nobody_Knows_You%27re_a_Dog/links/5dadf66d299bf111d4bf8bcc/The-positive-and-negative-implications-of-anonymity-in-Internet-social-interactions-On-the-Internet-Nobody-Knows-Youre-a-Dog.pdf , p.3040

[4] Ibid., p.3043.

[5] Sia et. al. (2002) in Christopherson, p.3043.

[6] Sutch, H. and Carter, P. 'Anonymity, Membership-Length and Frequency as Predictors of Extremist Language and Behaviour among Twitter Users.' *International Journal of Cyber Criminology*, 13:2, July-August 2019, pp., 439-459. https://www.cybercrimejournal.com/SutchCarterVol13Issue2IJCC2019.pdf , p.451,453.

[7] Mondal, M. Correa, D, and Benevenuto, F. 'Anonymity Effects: A Large-Scale Dataset from an Anonymous Social Media Platform. In Proceedings of the 31st ACM Conference on Hypertext and Social Media (HT '20),' July 13–15, 2020, Virtual Event, USA. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3372923.3404792 p.5.

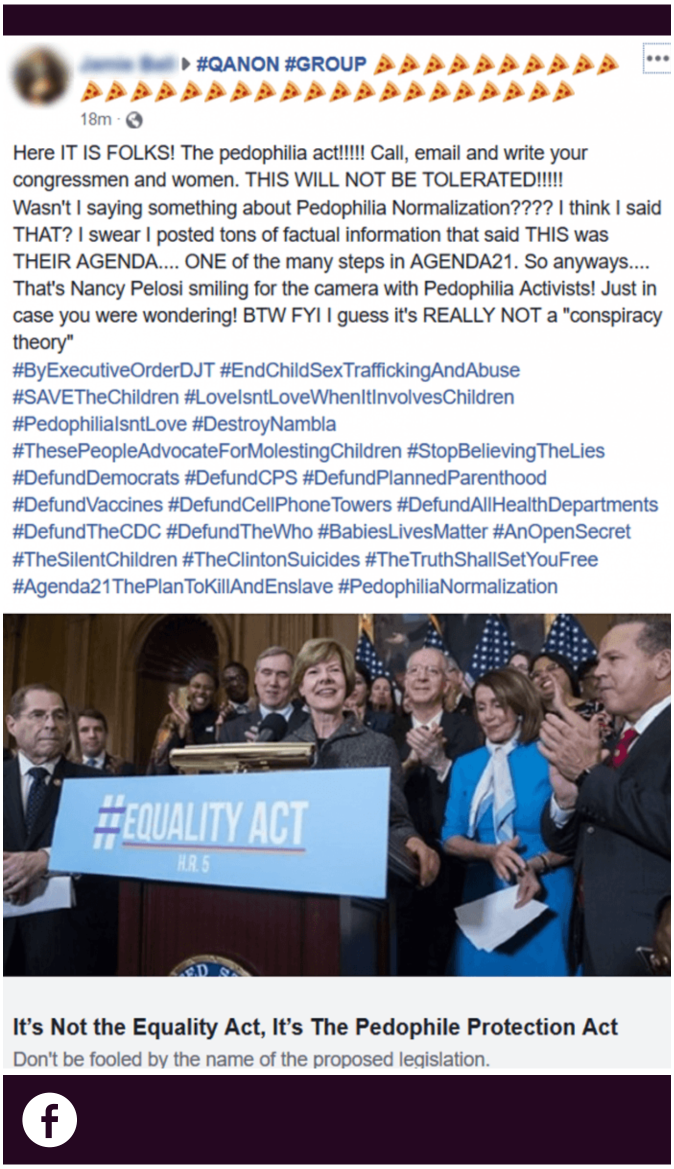
[8] Lopez, C. A., and Lopez, R.M. 'Hate Speech, Cyberbullying and Online Anonymity.' In Online Hate Speech in the European Union – A Discourse Analytic Perspective. Aritstar-Dry et. Al.eds. Springer Open. 2017, pp. 80-85. https://library.oapen.org/bitstream/handle/20.500.12657/27755/1002250.pdf?sequence=1#page=88 , P. 81.

[9] 'Antisemitic Incidents Report, January-June 2020.' *Community Security Trust*, https://cst.org.uk/data/file/c/5/Incidents%20Report%20Jan-Jun%202020-1.1596720071.pdf .P.4

Looking at October 2020 specifically, nearly 40% of reported antisemitic abuse online (not material proactively trawled) during that month came from fully anonymous and partially anonymous users. Further research is required, including data collection over a longer period and analysis of the effects of particular political trigger events but this finding points to a worrying trend.

Expressions of fundamentalist views, including racism, bigotry and extremism, often under the veil of anonymity, have been found to radicalise people and affect violence, hate crimes and terrorism offline. The Trust's briefing on the connection of online and offline harms provides numerous examples of this type of content. For example, the Christchurch mosque attack in 2019, the Pittsburgh synagogue attack in 2018 and the Finsbury Park mosque attack in 2017 were committed by far-right extremists who were radicalised, at least in part, by online extremism.[10] There is no indication whether anonymity was a driving factor in these specific cases but much of the content containing violent extremism which is used to radicalise and that is uploaded to social media, is done so under the cover of anonymity. Studies by the Counter Extremism Project (CEP) have also demonstrated the significance of online extremism in radicalising individuals.[11] CEP identified 168 individuals who had consumed official terrorist propaganda materials online. Of those profiled, 26 subsequently carried out terror attacks; at least 52 others had attempted to carry out or facilitate attacks; and 57 individuals had attempted to become foreign fighters for an extremist group, with at least 16 of them succeeding.

One notable example of an anonymised conspiracy theory that has become widespread and influential is that of QAnon.[12] Established by an anonymous individual calling himself Q, QAnon claim that there is a 'deep state' conspiracy to conceal 'the real truth' and a high-level paedophile ring. QAnon has been disseminating Covid-19-related conspiracies [13] and has also been found to use antisemitic rhetoric. These theories, originating in the U.S., have been gaining followers in Europe and the UK.



#QANON #GROUP 🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕🍕

18m

Here IT IS FOLKS! The pedophilia act!!!!! Call, email and write your congressmen and women. THIS WILL NOT BE TOLERATED!!!!!
Wasn't I saying something about Pedophilia Normalization???? I think I said THAT? I swear I posted tons of factual information that said THIS was THEIR AGENDA.... ONE of the many steps in AGENDA21. So anyways.... That's Nancy Pelosi smiling for the camera with Pedophilia Activists! Just in case you were wondering! BTW FYI I guess it's REALLY NOT a "conspiracy theory"
#ByExecutiveOrderDJT #EndChildSexTraffickingAndAbuse #SAVETheChildren #LoveIsntLoveWhenItInvolvesChildren #PedophiliaIsntLove #DestroyNambla #ThesePeopleAdvocateForMolestingChildren #StopBelievingTheLies #DefundDemocrats #DefundCPS #DefundPlannedParenthood #DefundVaccines #DefundCellPhoneTowers #DefundAllHealthDepartments #DefundTheCDC #DefundTheWho #BabiesLivesMatter #AnOpenSecret #TheSilentChildren #TheClintonSuicides #TheTruthShallSetYouFree #Agenda21ThePlanToKillAndEnslave #PedophiliaNormalization

It's Not the Equality Act, It's The Pedophile Protection Act

Don't be fooled by the name of the proposed legislation.

Apart from its radicalising potential, hate speech and bullying can cause emotional strain, depression, anxiety and fear to victims of online abuse. Certainly not all abuse is illegal and though harmful, social media companies do not always tackle it efficiently or effectively on their platforms. The platform Ask.fm was forced to take action after a number of teenage suicides, including cases of anonymous bullying.[14]

Limiting anonymity, or incentivizing against harm from anonymous accounts, can help victims regain a sense of control and confidence. It is also likely to reduce the overall volume of online abuse. Placing restrictions on anonymity will make it more likely that offline social norms will apply online, creating a positive change in the way individuals communicate and making the digital realm safer.

[10] 'Policy Briefing : Online and Offline Harms: The Connection.' *Antisemitism Policy Trust*, August 2020. https://antisemitism.org.uk/wp-content/uploads/2020/08/Online-Harms-Offline-Harms-August-2020-V4.pdf

[11] Counter Extremism Project, Written Evidence. Inquiry on Global Islamist Terrorism. Defence Committee, 2 April 2019, (GIT0022) http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-commitee/global-islamist-terrorism/written/96741.pdf

[12] Ibid., p.14.

[13] Ibid.

[14] https://www.businessinsider.com/askfm-and-teen-suicides-2013-9?r=US&IR=T

Legal framework for restricting anonymity

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 grant internet users the right to privacy and a right to withhold personal details. Despite this, users are rarely truly anonymous online; social media companies, apps, search engines and many other websites routinely collect personal data on users, often through ‘cookies’, including access to personal contacts, emails, photos, purchase history, location and much more, to be used for commercial purposes or sold to other companies. This undermines users’ expectation of privacy and the ability to remain anonymous.

In many cases, declarations of freedom are limited in some way, to ensure protection of others. This is true of the UN’s International Covenant on Civil and Political Rights, in the European Convention on Human Rights and here in Britain.

Freedom of expression is protected by the Universal Declaration of Human Rights, of which the UK is a signatory. According to Article 19, “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”[15] However, it can be argued that users who engage in abusive language and harassment prevent their victims from exercising their freedom of expression by making online space an unsafe environment in which they express opinions.

The Human Rights Act 1998 also guarantees freedom of expression. However, Article 10 of the Act determines that this freedom “may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.” [16]

Under these conditions, freedom of expression is already subject to restrictions and the police have powers to investigate certain expressions, such as those of abuse, threats and incitement for violence, anonymous or not. These restrictions should be applied to online abuse more vigorously than they currently are.

There are already some legal safeguards, remedies or incentives to address criminality by anonymous sources. Norwich Pharmacal Orders [17], are court orders which demand the disclosure of documents from a third party to assist applicants in pursuing alleged wrongdoing by another party. Section 5 of the 2013 Defamation Act incentivises a ‘know your customer’ approach, and the Regulation of Investigatory Powers Act 2000 allows public authorities to obtain communications data for the purpose of detecting a crime. However, jurisdictional issues often complicate matters and whilst it is usually possible to identify computers used to commit an offence, it is harder to identify users.

The Malicious Communication Act 1988, the Harassment Act 1997 and the Communications Act 2003 are meant to protect users from online harassment and hate speech. However, some of these predate the internet and are therefore outdated and unable to adequately protect victims of anonymous online hate, underlining the requirement for the Online Harms Bill.

[15] https://www.un.org/en/universal-declaration-human-rights/

[16] Article 10, Human Rights Act 1998, legislation.gov.uk, https://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/9

[17] http://www.bailii.org/uk/cases/UKHL/1973/6.html

Policy recommendations

The Antisemitism Policy Trust's recommendations regarding online anonymity rely on two main principles. The first, is the clear correlation between anonymity and increased risk of online abuse, and offline harms. The second, is that the same behaviour expected from offline hosts should also be expected from online equivalents.

As demonstrated, anonymity can exacerbate online hate and abuse. Users will be less inclined to use hate speech and other abusive language, images or videos, if their identity is known to a host and if they are in danger of wavering their right to anonymity if their behaviour violates the host's terms and conditions, or the law.

It should be up to a platform to determine the degree of anonymity it wishes to give users, and how to incentivise those user accounts against producing hateful content. This allows for whistle-blowers, victims of domestic abuse, and others to remain anonymous online on the platforms in scope of the proposed regulator. It is clear, as the failed Google + experiment shows, that forcing users to register with their own names is unpopular.[18] However, action to guard against hate emanating from anonymous accounts would, in the view of the Trust, fall within the reasonably foreseeable harms captured by a statutory Duty of Care on platforms.

Online companies should also stipulate in their terms and conditions that anonymous users engaging in hate speech and other abusive behaviour will be banned from using the platform and their identity may be revealed to law enforcement. This would act as a deterrent for offenders and better guarantee the right of users to a safe environment, free from hate speech, bullying and trolling.

If a crime or a libel has been committed in the UK on the regulated platforms and they cannot or will not provide proof of identity, where a magistrate's court order demands it (subject to an appropriate burden of proof), then a range of options should be considered. The Trust believes that the civil or criminal liability should pass to the platform itself (this would be in line with existing measures in the e-Commerce Directive), and fines or other corrective measures could be put in place. We would suggest giving the platforms a year to become compliant.

Companies should apply the 'Know Your Client/ Customer' principle, familiar to those in the financial sector. Using some of the legal framework required by companies offline, such as Customer Due Diligence in The Money Laundering, Terrorist Financing and Transfer of Funds regulations 2017, [19] online companies should verify users' identities before allowing use of their platform. This should be done even if use of the platform is free of charge and when users are not regarded as 'customers'.

Electronic identification techniques are already used by governments, financial institutions and other businesses, and have been found to be more accurate than old fashioned IDs. One example is the Pan Canadian Trust Framework (PCTF) developed by the Digital ID & Authentication Council of Canada (DIACC) and the Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada.[20] The PCTF's building principles include asking users to provide only the minimum amount of personal information, and privacy enhancing tools such as the 'right to be forgotten', inclusion and transparency. [21] It also allows the registration of legal entities such as businesses for a Digital Identity.

It is crucial that while maintaining freedom of expression, people not be able to exploit anonymity for aggressive and abusive behaviour that will deny others their own freedom of expression. It should still be possible to maintain anonymity, so long as a platform's terms and conditions are followed. This will give all users confidence that their fellow users are real and known individuals

.

[18] https://www.nbcnews.com/tech/social-media/google-plus-ends-real-name-policy-after-three-years-n156841

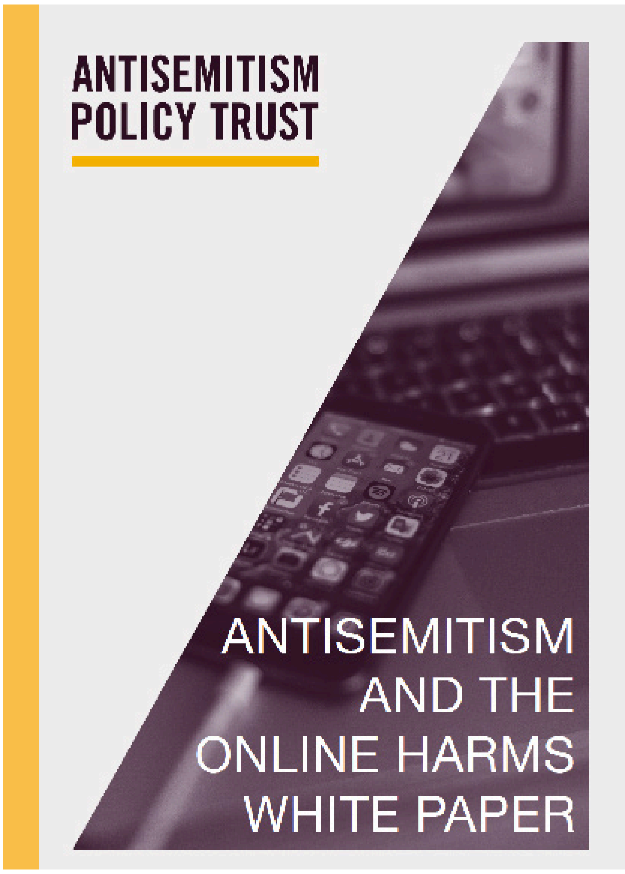
[19] https://www.legislation.gov.uk/uksi/2017/692/part/3/made

[20] Pan Canadian Trust Framework Model, Final Recommendation V1.0. *DIACC*, 15 September 2020. https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf

[21] Ibid., p.7.

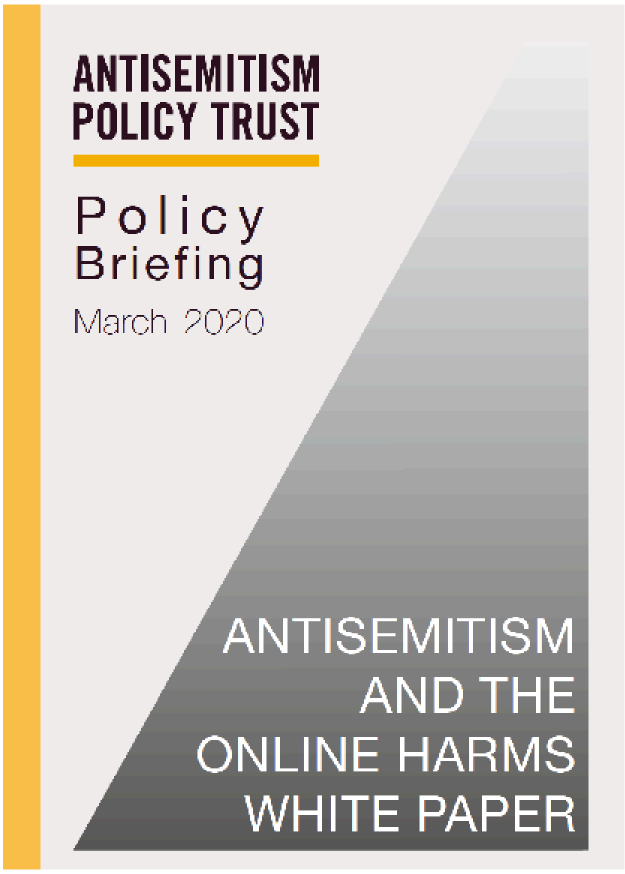
Antisemitism Online Series

Published by the Antisemitism Policy Trust



ANTISEMITISM POLICY TRUST

ANTISEMITISM AND THE ONLINE HARMS WHITE PAPER

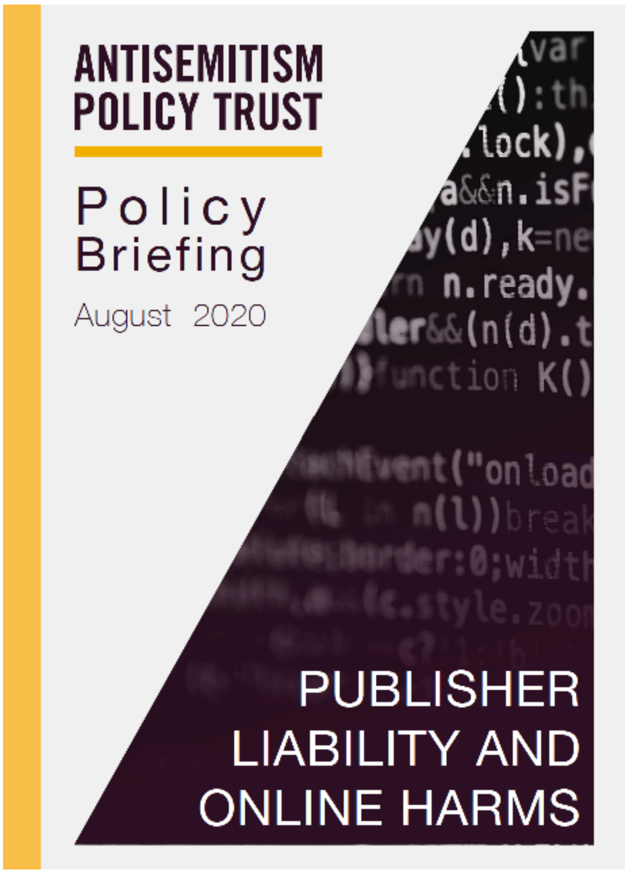


ANTISEMITISM POLICY TRUST

Policy Briefing

March 2020

ANTISEMITISM AND THE ONLINE HARMS WHITE PAPER

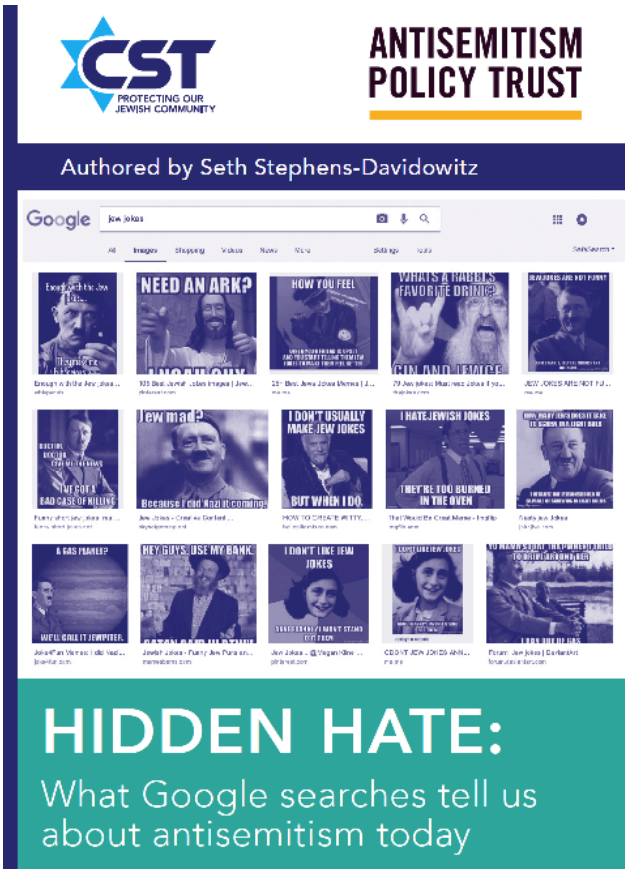


ANTISEMITISM POLICY TRUST

Policy Briefing

August 2020

PUBLISHER LIABILITY AND ONLINE HARMS



CST PROTECTING OUR JEWISH COMMUNITY

ANTISEMITISM POLICY TRUST

Authored by Seth Stephens-Davidowitz

HIDDEN HATE:

What Google searches tell us about antisemitism today

The Antisemitism Policy Trust's mission is to educate and empower parliamentarians, policy makers and opinion formers to address antisemitism. It provides the secretariat to the British All-Party Parliamentary Group Against Antisemitism and works internationally with parliamentarians and others to address antisemitism. The Antisemitism Policy Trust is focussed on educating and empowering decision makers in the UK and across the world to effectively address antisemitism.

Contact APT

www.antisemitism.org.uk

@antisempolicy

Antisemitism Policy Trust

mail@antisemitism.org.uk

The Antisemitism Policy Trust is a registered charity (1089736) [England]
and company (04146486) [England and Wales]