STOP THE ONLINE SAFETY BILL

Campaign Pack for ORG campaigners

Author – James Baker - james.baker@openrightsgroup.org

March 2023 – V1

Contents

radio.

IV). Press releasing your activity

1. The Purpose of this campaign pack

The pack is designed to empower and equip you to take action as a campaigner. This could be as an individual, part of one of ORG's local groups, or as an organization that shares ORG's concerns about the impact the Online Safety Bill will have on our freedom of expression, surveillance of private communications and burdensome regulation on small businesses.

The bill is advancing through Parliament and we have a limited window to try and have a positive impact on the legislation. So please do take action as soon as possible.

Image by Thomas Hawk https://flic.kr/p/S5FQJD Licence (CC BY-NC 2.0)

2. What is the issue?

Summary

The Government wants to control what content we can access online. The primary stated purpose for this control is to protect children from encountering what they define as harmful content. However the moderation of this content would be largely be done via AI algorithms. This would have a negative impact on our freedom of expression as content will be wrongly taken down or censored. People might also be prevented from posting it in the fist place with prior censorship returning to the UK in the form of 'upload filters.

The Government also wants to expand its surveillance of private chat messaging. They would achieve this through request by OFCOM that companies start automatically scanning private messages on platforms such as WhatsApp and Signal for CSE material. This has resulted in some providers such as WhatsApp warning that they might be forced to pull out of the UK market rather than break the encrypted security of their product.

One way in which these objectives would be achieved is via age-filters. This could either mean having to upload sensitive Identity Documents to gain access to websites or submitting to bio-metric age-checks. Previous attempts to introduce age checks for websites have failed, but with this bill they are very much back on the agenda.

Finally All online services will be designated as a category 1, 2A or 2B services. This will increase the bureaucratic compliance burden upon people providing services. We are concerned this will create additional hurdles and challenges to 'challenger services'. For example volunteers hosting a Mastodon instance.

The briefings

ORG has produced a number of briefings on different aspects of the bill as it progresses through Parliament. We would encourage you to read these to gain a full understanding of the problems with the bill.

All of these can be read and access on the Online Safety Bill Campaign Hub - https://www.openrightsgroup.org/campaign/online-safety-bill-campaign-hub

3. Key Messages

When communicating the threats and risks to the bill in your campaigning activities then it might be useful to repeat some of our key campaign messages around the bill.

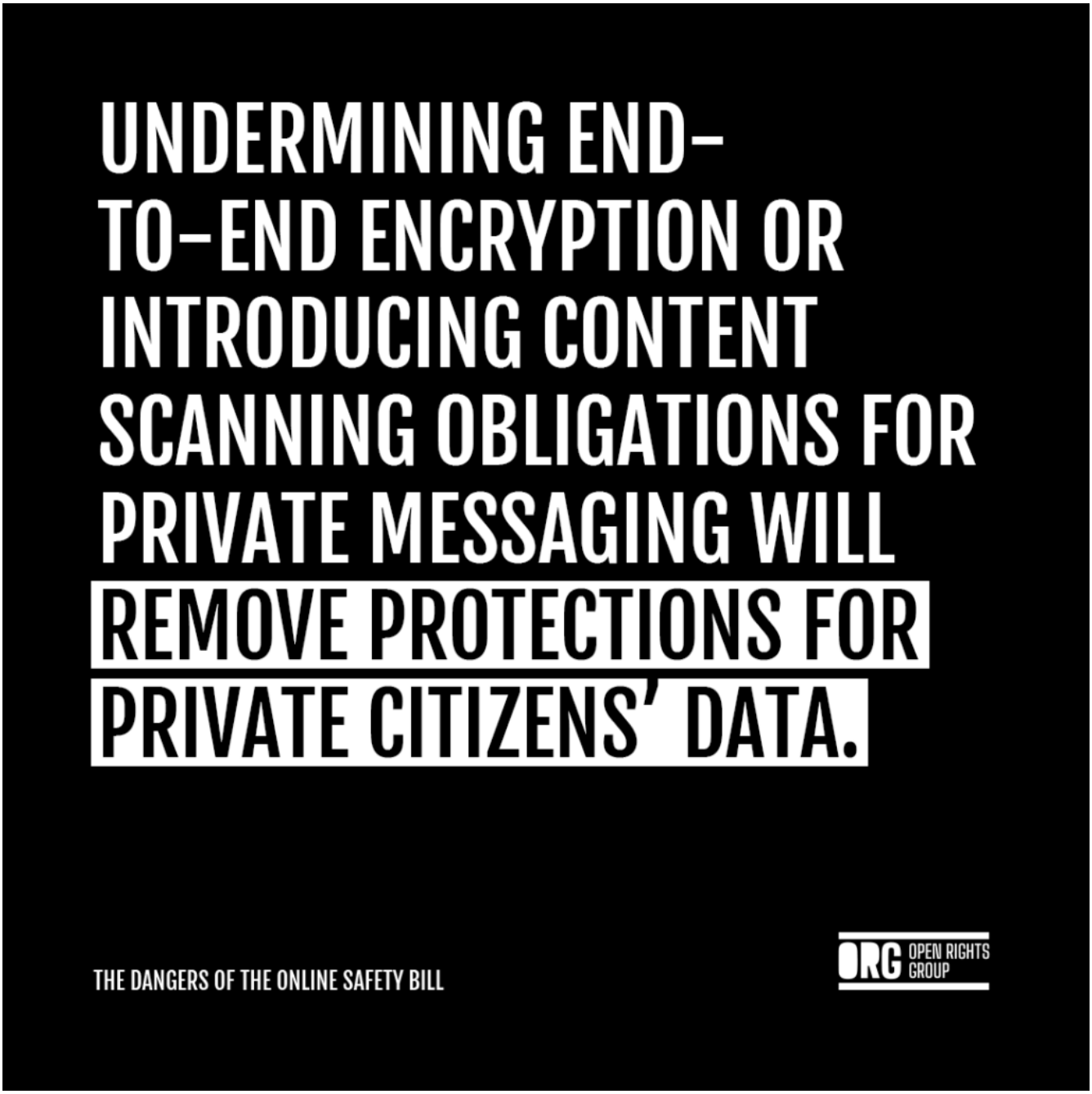

Figure 1: Image by ORG Licensed under a public works license

I). Don't Scan Me – Stop the Spy Clause

Key messages

1. The spy clause in the Online Safety Bill will give Ofcom the power to ask private companies to scan everyone's private messages on behalf of the government. It is state-mandated private surveillance.

2. This includes messages sent through WhatsApp, Telegram, Signal, Facebook Messenger and iMessage, and direct messages sent through platforms such as Snapchat, Facebook, Twitter and Instagram.

3. This is something that authoritarian regimes do. In China, the WeChat service conducts surveillance of images and messages sent through smartphones.

4. Services that use end-to-end encryption will have to compromise their encryption in order to scan the content of messages. Signal have said that they would stop providing services in the UK if the Online Safety Bill forced them to undermine encryption. (https://www.bbc.co.uk/news/technology-64584001). WhatsApp could also leave. (https://www.thesun.co.uk/tech/21075003/whatsapp-shut-down-for-brits-online-safety-bill/)

5. The Government could force companies like WhatsApp, Facebook and Signal to install 'government accredited' software on your phone, which can scan your private messages.

6. The Government says that it will only scan messages for images of child abuse. But once the technology in place, they could ask companies to scan for other content.

7. There is always mission creep when it comes to surveillance. Time and time again, the Government has given itself surveillance powers arguing that they are need to tackle terrorism and serious crime. They always end up being used for other reasons.

8. These new capabilities could be used to change your phone from a private device to a 'spy in your pocket'.

9. The spy clause in the Online Safety Bill will give the UK some of the most extreme surveillance powers of any democracy.

Preventing child abuse should be a government priority. But there are more effective

ways of tackling this crime than by scanning the private messages of the 40 million people in the UK who use messaging services.

Arguments for surveillance	Rebuttal
"I've done nothing wrong I've got nothing to fear"	**Privacy is a universal right for us all:** "If I have done nothing wrong, why is my privacy being violated? Privacy is a universal human rights and should only be violated if there is reasonable suspicion people have committed offenses."
If it helps catch pedophiles then I'm all for it"	**The technology is known to fail.** And as a result, you may be accused of being a (child) sexual offender without having done anything wrong. **We can't afford to get it wrong.** We all agree: child sexual abuse is a horrendous act. As a society, we shouldn't waste our effort to tackle this issue on actions that are proven to be ineffective and harmful.
"This doesn't break encryption"	**It breaks the principle of end-to-end encryption:** The purpose of E2EE messages is that they can only be read by its intended recipient. If messages are scanned before they are encrypted then this breaks that secure trust. As the technology has not yet even been developed we don't know what security vulnerabilities it might create.
"Encryption means we are 'going dark' and are losing surveillance abilities"	**We are in a golden age of surveillance:** We have never lived in a time where people are subjected to this much surveillance. Government has never had the power to spy on every private conversation. Private

	companies should not have the power to spy on every single private chat.

Making arguments against message scanning

False Positives

The systems will attempt to try and detect images relating to CSAM. This will likely result in people being falsely accused. There are real-world examples of this already happening on some systems that attempt to scan for this content. See - https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html

It could weaponize the use of indecent CSAM by criminals

Criminals could threaten to send people indecent CSAM material so that they are automatically reported to the authorities. This could be used by organized gangs to blackmail and coerce vulnerable people, or as a dark-web service to hire in the same way as DDOS and other cyberattacks against individuals can be purchased.

It gives a green light for dictators and undermines global end-to-end encryption

Once a provider of this service agrees to start scanning the messages for one Government then it opens the doors for requests from more authoritarian countries to request message scanning for other purposes. How can we argue against Putin scanning Telegram messages for anti-war protestors when we are doing the same.

This undermines end-to-end encryption globally as a technology relied upon by human rights campaigners, journalists, activists and vulnerable communities persecuted by authoritarian regimes.

It's an intrusive form of mass surveillance

Everyone has a right to privacy – This is enshrined in the Universal UN declaration of Human Rights and the UK's Human Rights Act. The right to privacy is a democratic value that helps to protect individuals from abuses of power by Governments. Undermining the right to privacy makes the UK a less democratic and free country.

We risk losing WhatsApp and other services here in the UK

Some services have warned they will pull out of the UK rather than compromise on their products unique selling point of end-to-end encryption. This could mean the UK following the path of China, Syria and Qatar where WhatsApp isn't available.

https://www.the-sun.com/tech/7156207/whatsapp-shut-down-for-brits-online-safety-bill/

It's the thin end of the wedge

The security services are using child protection as a way for politicians and civil society to accept this intrusive form of surveillance. They are pushing the same line in other countries as well which shows it's a coordinated effort to break encryption.

Once the principle of scanning our private messages for one reason is accepted then it won't be long until the scanning is being used to detect all sorts of criminal and civic offenses.

ii) Censorship of online speech

Figure 2: Image by https://commons.wikimedia.org/w/index.php?curid=46776361 Gawler History under a CC-By-2.0 licence.

- The Online Safety Bill will have a negative impact on freedom of expression in the UK. The bill is not just about censoring content that is harmful to children.

The list of items the bill will censor increases to grow. The Government has made it clear that it wants to censor videos or content that promotes 'small boat crossings' in a 'positive light'.

Guardian story on censorship to share- https://www.theguardian.com/media/2023/jan/18/banning-channel-tiktok-traffickers-risks-censorship-uk-campaigners-say

Blog article on censorship to share - https://www.openrightsgroup.org/blog/could-public-debate-on-immigration-be-suppressed-by-the-online-safety-bill/

- Online posts will be subjected to surveillance under a duty to actively prevent people coming into contact with harmful posts. There will be a two tier system in which the free speech of ordinary residents has fewer protections than the mainstream media and state recognized journalists.
- Key question for MPs and Lords – What provisions have you made in the bill to ensure there is a right to appeal for individuals who experience wrongful censorship of their posts?

iii) Age filter with its privacy risks and bio-metric surveillance

- Online services will either have to remove all content that the Secretary of State and OFCOM define as harmful to children or introduce systems of 'age-gating' to try and ensure children are unable to access that content.
- Age-gating creates unique privacy and security risks to users. Age-gating might involve users having to prove their identity. Either directly with a service or via an age-verification provider. In order to do this users might have to upload sensitive government documents such as passports or driving licenses. This increases the risk of identity fraud occurring. It also risks databases of users accessing this content.
- This won't only apply to adult content, it will also apply to other forms of content such as violent content. This might encourage providers such as YouTube to change their content monetization policies having a big impact on the freedom of expression of YouTubers and other online content creators.
- Age-verification might also occur via bio-metric surveillance systems. For example software has already been developed that scans your face and tries to

determine your age, or software that monitors your keystrokes and mouse movements to try and determine age. This creates new systems of surveillance, and potentially lists of under-age users of sites.

- Finally children will have their access to information highly restricted. This could damage children's own rights. It might prevent children accessing important educational information around eating disorders, substance abuse or sexual education.

iv) Executive powers the bill grants Government to control services

- The bill grants the Secretary of State powers to influence and control the internet expanding executive powers of the Government. This risks politicization of the regulation of the internet. Members of the House of Lord and MPs should seek to limit the Secretary of State's powers within the bill.

V) Damaging to small business and startups

- The Online Safety Bill is looking at the internet through the lens of big tech providers like Facebook and Twitter. However smaller providers and challengers to these larger services such as Mastodon, Wikipedia, community based groups and startups will all get caught up in the regulations.
- This could result in some providers simply geo-blocking the UK so they don't have to deal with the legislation.
- It could also put others off hosting or running services resulting in less consumer choices and options to avoid services where users might get exposed to unwanted content, harassment and online harms.

You could share this article that makes this point - https://www.itpro.co.uk/business-strategy/startups/370036/jimmy-wales-online-safety-bill-could-devastate-small-businesses

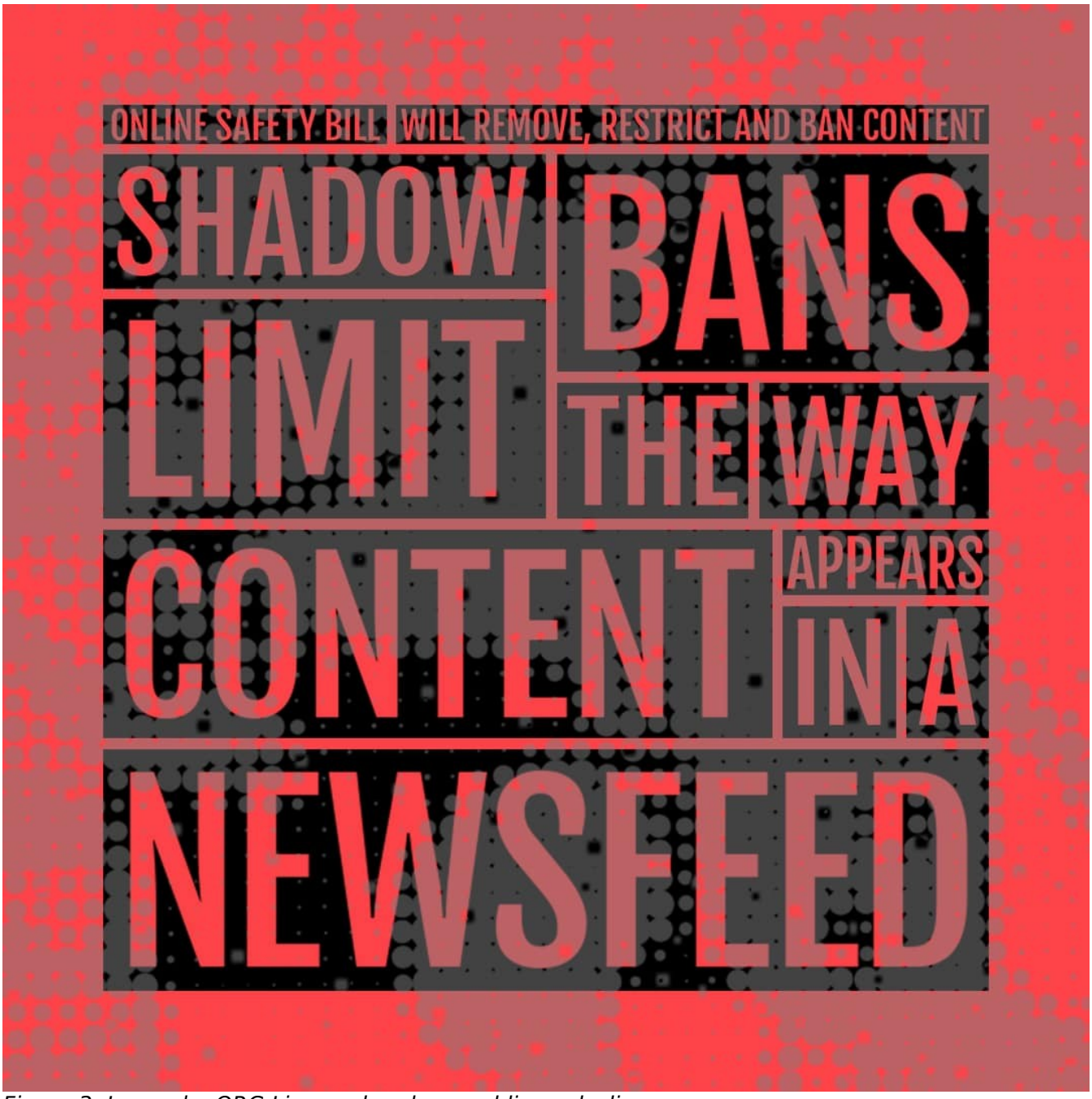

Figure 3: Image by ORG Licensed under a public works license

4. Taking Action as an Individual

I). Writing to your MP

MPs monitor the volume and nature of letters they receive in their constituency offices. Writing to your MP to express your concerns is still an effective means of trying to influence Government policy.

Despite the Online Safety Bill having passed through the Commons MPs will still have to consider any amendments from the Lords.

The Open Rights Group has produced an online tool that makes writing to your MP very easy. You can do this on our website at the following address - https://action.openrightsgroup.org/write-your-mp-help-stop-online-safety-bill

II) Lobby a Lord

Online Safety Bill - Campaign Pack

Lords are currently considering the Online Safety Bill. The most important Lords to lobby will be those sitting on the bills committee. You can also focus on writing to the whips of different political groups, Lords that have commenting on the bill during debates, and finally any other member of the House of Lords.

You can share and use our tool for Lobbying a Lord

https://action.openrightsgroup.org/dont-scan-me-lobby-lord

II). Signing up to support our campaign online

If you haven't done already please do sign up to support our campaign on our website- https://action.openrightsgroup.org/stop-state-censorship-online-speech

This will ensure we can keep you up to date on all the latest news and activity around the campaign.

III). Writing a letter to the local paper

Local newspapers are always willing to print letters. Although circulation of papers is lower than it used to be, the letters page is still the most widely read page of a local paper. Also local politicians pay attention to the issues being raised in the letters page.

- When writing to the local papers, remember the following:
- React fast. A letter reacting to something that appeared in the paper is more likely to be published if you send it in straight away: the press has a short memory.
- Be topical. Your letter should cover a subject that the newspaper itself might use in a news story so it should have a local angle if possible.
- Keep it short. It is often harder to write a short letter than to write a long one, but people are more likely to read it.
- Keep it simple. Use clear and simple language and try to avoid cliches.

IV). Sharing ORG's content with friends and family on social media.

We need more of our supporters to engage with our content on social media. Please to like, share and re-tweet our content.

Details of our social media accounts are:

ORG is on twitter at @OpenRightsGroup

Reddit – u/OpenRightsGroup

Facebook - https://www.facebook.com/openrightsgroup

Mastodon - https://mastodon.social/@openrightsgroup

You Tube - https://www.youtube.com/user/OpenRightsGroup

V). Working with an ORG local group or forming a new group.

We have a network of local groups across the country. You can sign up to their mailing lists or Meet Up groups online. If there isn't a group active in your area then you might

want to consider becoming one of our volunteer organisers. If you would like to take on a role like this please email supporters@openrightsgroup.org

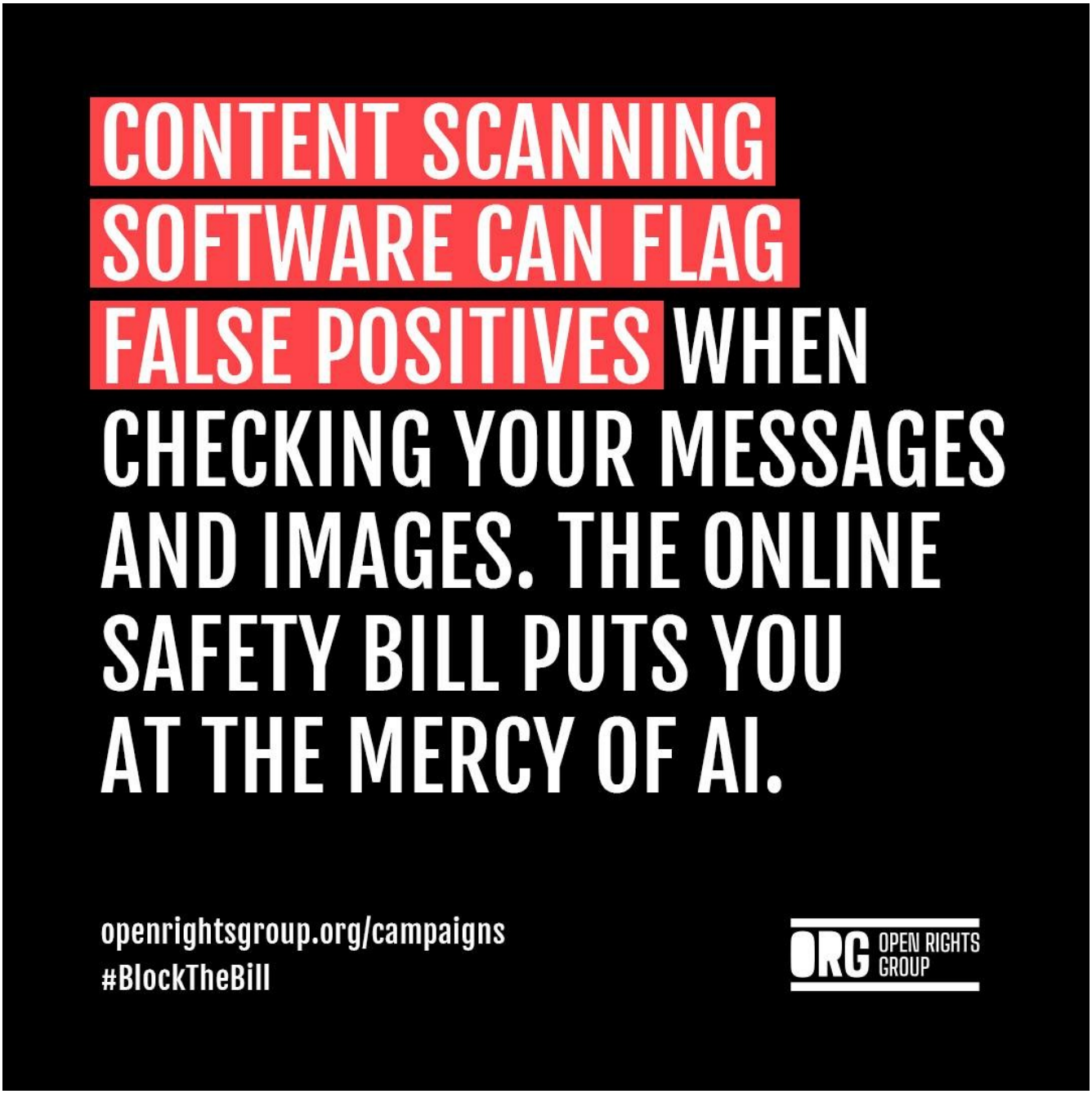

Image by ORG Licensed under a public works license

5. Taking Action as a Group

I). Going to visit and lobby your MP or a Lord as a small group

Writing to your MP or a member of the Lords is a good first step.It can be even more effective to arrange a meeting as a small group to go and speak to them in person. You can search for the contact details of your MP or a Lord online on Parliament's webpage. Many MPs hold regulary surgeries in their constituencies that you might be able to book an appointment at.

When you go to visit your MP or a Lord consider if there is a photo opportunity to be had. Perhaps as a group you could get a picture of a few of you with an ORG banner, T-shirt or leaflets? Also make sure you think of the key points you want to get across in advance. Go prepared!

II) Talking to your local media on the radio.

Not everyone will feel confident about going on the radio, but don't be discouraged from trying. Practice first by calling phone-in shows. Once you are used to that, perhaps you can go on a show and answer callers yourself. When you are going on air, remember the follow-ing:

- Decide key points two or three things (no more) that you want to say
- Rehearse your key points. Try recording you saying them to see how it sounds. Make sure you know them backwards.
- It's a good idea to have three or four points noted down. Then if you get anxious just look down at them and remember to go back to them,
- Anticipate the questions that somebody might ask you, whether on the
- subject or on some other topical subject. Then prepare some answers in advance.
- Answer briefly and don't waffle. Less is often more.
- You are there to make your own points. Don't get deflected by the line of questioning someone wants to take you down. You can use phrases like *"Thats an interesting question, and I'll respond to it, but first I want to make the point":*

- Speak slowly and clearly otherwise people will not understand. If you are calling in from you computer on something like Skype then having a decent microphone makes a big difference.

- Be friendly. Try to sound sympathetic to callers if you're on a phone-in, no matter how wrong, hostile or rude they are to you.

- If the opposition comes across as being extremist, that's a victory for us Look friendly and smart if on TV. It really makes a difference.

Remember coming across as natural takes a lot of practice.

III) Organising a public meeting to talk about the Online Safety Bills impact

Many people have only heard the arguments around why we need to censor material online to protect children. They have not considered what will happen when their own posts are wrongly flagged and they start to have their freedom of expression curtailed.

Others have no idea that the Online Safety Bill also includes the scanning of their private DMs and personal messages.

As a local ORG group you could advertise a public meeting (in person or online) on the topic of the Online Safety Bill and its threats to privacy and freedom of expression. If you speak to us then we might also be able to arrange a speaker to come along and address an audience on the issues.

IV). Press releasing your activity

If you carry out any campaign activity such as a street stall, or got to lobby your MP then it's well worth letting your local newspaper know about it. The best way of doing this is to send them a press release and a picture. Many newspapers are desperate for copy, so if you can send them something to print, with a good picture then you have a good chance of them running it as a story.

Below is an example press release that you might wish to edit and change.

BEGINS

Tittle: Campaigners from [AREA NAME] Open Rights Group raise alarm over Online Safety Bill's Spy Clause

Local residents from the [AREA NAME] Open Rights Group are raising concerns with [NAME OF LOCAL MP] over Government's plans to introduce automatic scanning of our private messages. The group is warning that a 'spy clause' in the Online Safety Bill will introduce message scanning as an intrusive new form of mass surveillance.

Local ORG organiser [INSERT NAME] said: "In a democracy we all have the right to privacy, yet this spy clause in the Online Safety Bill will force providers to spy on our private encrypted personal messages. This will be applied to all law-abiding citizens even though we have done nothing wrong"

"The consequences of this move could mean providers such as WhatsApp pulling out of the UK. That would put the UK alongside China, Syria and Qatar which have all moved to stop people being able to send private and secure personal messages."

The group hopes that in meeting with [AREA NAME] MP they will help to raise awareness of the importance of protecting private and secure messaging apps.

ENDS

Notes to Editor

1.The Open Rights Group is a UK-based organisation that works to preserve digital rights and freedoms by campaigning on digital rights issues and by fostering a community of grassroots activists. It campaigns on numerous issues including mass surveillance, internet filtering and censorship, and intellectual property rights

2.The data protection and digital information bill has been laid before Parliament but has yet to become law https://bills.parliament.uk/bills/3137. ORG's anaylsis of the bill's threat to private message can be read at = https://www.openrightsgroup.org/app/uploads/2022/11/Whos-Checking-on-your-chats-in-private-online-spaces.pdf

3. For further information please contact info@openrightsgroup.org or contact ORG's local organiser on – [INSERT YOUR OWN CONTACT DETAILS]