PRIVACY INTERNATIONAL

Privacy International's Response to the Open Consultation on the Online Harms White Paper

1 July 2019

Submitted to: onlineharmsconsultation@culture.gov

Introduction

While Privacy International ("PI") welcomes the UK government's commitment to investigating and holding companies to account, when it comes to regulating the internet in the expansive way described in the White Paper, we suggest moving with care. Failure to do so could introduce, rather than reduce, "online harms".

PI is concerned about both the tone and the proposals put forward in the Online Harms White Paper. Rather than seeking to review and strengthen existing efforts to challenge and limit the data exploitation that has become embedded in our online experience, the Paper includes broad and vague new proposals. Some of those proposals risk undermining human rights, in particular the rights to privacy and freedom of expression. If the scheme proposed in the White Paper is taken forward, there is a risk that the approach will ultimately cause more harm without making headway with the problems identified, many of which are societal in nature and require more detailed and context-specific responses.

PI is a leading charity advocating for strong national, regional, and international laws that protect the right to privacy around the world. Founded in 1990 and based in London, PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

PI employs technologists, investigators, policy experts, and lawyers, who work together to understand emerging technology and to consider how existing legal definitions and frameworks map onto such technology. PI is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Parliament of the United Kingdom, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

PI's response, concerns and recommendations in relation to the White Paper are detailed below and supplemented by specific answers to some of the questions posed.

General Response to the White Paper

Vague and Overbroad

The White Paper touts the proposition that "the UK will be the first to tackle online harms in a coherent, single regulatory framework that reflects our commitment to a free, open and secure internet." In our view, however, the reason such an approach has yet to be taken is that the premise - that it is possible to tackle all "online harms" with a singular approach - is fundamentally challenging. The diversity of harms addressed in the White Paper is very great as are the actors potentially within scope. Dealing with each type of harm requires a nuanced approach to balance the competing interests and rights involved. Certain of the identified harms, also have deep societal roots and are not limited to the 'online' space. Dealing with such harms may require a more coordinated and comprehensive effort than could be provided, for example, by one new regulator.

Clarity is key to any regulatory framework. However, the list of harms is, by design, neither exhaustive nor fixed. There are also many definitional issues with the White Paper. This is

acknowledged to an extent in the proposal (p 31, Table 1), where the various harms are classified as "Harms with a clear definition" and "Harms with a less clear definition". As will likely be highlighted by others, many of these definitions classed as "clear" are far from it in practice. This is also concerning given the inclusion of harms that are not illegal.

The focus on the harms in the Paper also implies an impact-based approach, focusing on outcome as opposed to motivation, and fails to address the contribution of a company's design decisions to such outcomes. This point is also made by some of the original proponents of a version of a 'duty of care'.[1]

We note that there will be exclusions when harms are already subject to a regulatory framework, including for example when they result directly from a breach of data protection legislation, including harm from unfair processing. It is unclear how such distinctions will work in practice. How will an individual know within which framework the harm that they have suffered falls? How will regulators delimit the scope of their jurisdiction, without at least some preliminary investigation?

The Paper also fails to set out in sufficient detail the shortcomings of existing regulatory frameworks and initiatives that are not excluded. As mentioned above, many of the harms are complex; they are societal and not limited to the 'online' world and will require a context specific approach as well as further consideration of how existing frameworks and efforts might be applied and strengthened where they fall short. With very little detail provided as to the Code(s) of Practice, it is extremely difficult to engage with the proposed 'Duty of Care' in a meaningful way.

The proposal may also have a significant international impact. The Paper states the Government's intention to lead through example. We are concerned, however, that the proposal may negatively impact certain rights such as privacy and freedom of expression. If these concerns are not addressed, the end result may be a template and a justification that authoritarian governments may adopt in their ongoing efforts to shrink public spaces and surveil internet users.

Against this backdrop, PI focuses in the next section of this submission on the importance of protecting the right to privacy and how data exploitation facilitates some of the harms identified in the report. These are two of the many areas in which there are already existing regulations and laws which could be impacted by the White Paper's proposals.

Will the White Paper lead to increased and potentially unlawful surveillance?

PI is concerned that the White Paper's proposals will lead to increased interference with the right to privacy. The right to privacy is explicitly protected in Article 8 of the European Convention on Human Rights (and in the UK by the Human Rights Act 1998) as well as in Article 7 of the Charter of Fundamental Rights of the European Union, while Article 8 of which explicitly recognises the right to data protection. It is important to ensure that any measure respects the rights to privacy and data protection.

The "proactive" monitoring of content in digital media platforms may constitute an interference with the right to privacy that needs to be regulated and justified as necessary in a democratic society. The European Court of Human Rights has long held that "there is […] a

[1] https://www.carnegieuktrust.org.uk/blog/online-harms-response-cukt/

zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".[2] It has underlined that "private life considerations may arise [...] once any systematic or permanent record comes into existence of such material from the public domain."[3] The government must strike a fair balance between the public interest – the necessity to take effective measures for the prevention of specific illegal activities – and the protection of each individual's right to privacy.

The White Paper states that "companies will be required to ensure that they have effective and proportionate processes and governance in place to reduce the risk of illegal and harmful activity on their platforms." Such steps include "prevent[ing] new and known terrorist content, and links to content, being made available to users." The regulator is expected to provide guidance "on proactive use of technological tools, where appropriate, to identify, flag, block or remove terrorist content" as well as guidance "on the content and/or activity companies should proactively prevent from being made available to users, which will help inform the design of technological tools." Such proactive measures are envisaged as addressing the entire scope of harms identified by the White Paper. Such monitoring could, for example, involve the removal of already-uploaded content (using, for example, algorithmic decision-making), the use of fingerprinting or hashing of content (for example the Child Abuse Image Databases or YouTube's Content ID), or the use of Domain Name System (DNS) blocking or deep packet inspection at Internet Service Provider (ISP) level.

Many of these techniques would involve imposing a general obligation on service providers to monitor their network for evidence of illegal activity, which is unlawful: the Court of Justice of the EU (CJEU) concluded in *Scarlet Extended SA v SABAM*[4] that a general monitoring function for an unspecified period was incompatible with the EU Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, construed in light of the fundamental rights to protection of personal data and freedom of expression.[5] The E-Commerce Directive does not allow for any exemptions from this prohibition.[6] In *Sabam v. Netlog*,[7] the CJEU concluded that a filtering system, which targets a specific type of content while indiscriminately monitoring all information shared by platform users for unlimited period of time, amounts to such a prohibited general monitoring obligation. The Court found that imposing such a general filtering system would not meet "the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other".

---

[2] *Von Hannover v. Germany* (no. 2), Appl. nos. 40660/08 and 60641/08, Judgment, Grand Chamber, ECtHR, 7 February 2012, para. 95*; Gillan and Quinton v. the United Kingdom*, Appl. no. 4158/05, Judgment, Fourth Section, ECtHR, 12 January 2010, para. 61

[3] P.*G. and J.H. v The United Kingdom*, Appl no. 44787/98, Judgment, Third Section, ECtHR, 25 September 2001, para. 57; *Peck v. The United Kingdom*, Appl. no. 44647/98, Judgment, Fourth Section, ECtHR, 28 January 2003, para. 59

[4] http://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10

[5] https://globalfreedomofexpression.columbia.edu/cases/scarlet-extended-sa-v-sabam/

[6] See https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-opinion-online-terrorism-regulation-02-2019_en.pdf p39

[7] http://curia.europa.eu/juris/document/document.jsf;jsessionid=C2F9E1F8806FC62117A9F45EC1CBBBB4?text=&docid=119512&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7961800

Protecting Encryption

The White Paper states that "The regulatory framework will apply to companies that provide services or tools that allow, enable or facilitate users to share or discover user-generated content, or interact with each other online." This will undoubtedly include messaging platforms, including WhatsApp, Messenger and Signal, regardless of whether or not they offer end-to-end encryption to users. Those which do offer well implemented end-to-end encryption are not able to view the contents of users' messages, and will therefore find themselves potentially subject to the full range of enforcement powers, including being blocked from providing services, unless they undermine their own security measures to allow them to view their own users' content.

Undermining end-to-end encryption in such a way is an ill-considered and unhelpful intervention into an ongoing and highly complex debate. While the Director of GCHQ has publicly stated that the agency is seeking to "provide for responsible law enforcement access with service provider assistance", he has also stated that the objective is to do so "without undermining user privacy or security", and that "we have no intention of undermining the security of the commodity services that billions of people depend upon".[8] To achieve this, GCHQ has developed six principles, which include seeking "exceptional access to data where there's a legitimate need, that access is the least intrusive way of proceeding and there is appropriate legal authorisation". The principles further state that "Targeted exceptional access capabilities should not give governments unfettered access to user data", and that any "exceptional access solution should not fundamentally change the trust relationship between a service provider and its users".[9] How to balance these principles with the desire to access data is highly contested: GCHQ has so far proposed one such technical means, which a wide range of civil society, security experts and companies believe contradicts GCHQ's own principles and poses "serious threats to cybersecurity and fundamental human rights including privacy and free expression".[10] Forcing providers to undermine their own security as potentially envisaged by the White Paper would not only violate people's security, data protection and human rights, it would violate the UK's own security agencies' principles.

Data Exploitation and the Harms

The White Paper is ostensibly concerned with what people 'see' online i.e. content, and the harms that may result from this. In our view the paper does not give enough consideration or acknowledgement of the role that the 'back end' of content - that is the design choices and data which ultimately drives and shapes the content that we see - can play in creating and tackling online harms.

Most platforms, online retailers, social media platforms, music or video streaming services are now personalised, meaning that they deliver targeted content and adapt online experiences based on data they have collected about each visitor. As a result, the data that feeds into the largely automated architecture that is behind the content we see dictates much of our experience of the internet: when we search,[11] the posts that are pushed or promoted

[8] https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate
[9] https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate
[10] https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages
[11] https://www.google.com/intl/en_uk/search/howsearchworks/algorithms/

when we scroll through a social media feed,[12] what video is recommended next,[13] and what adverts we see, whether it is within an app, a platform or as we browse the web.

How data is used in the backend is characterised by a concerning lack of transparency, fairness and accountability. Tackling these is paramount to addressing the root causes of many online harms.

1. Harms caused by targeted online advertising ecosystem

A significant share of the content that people see on social media is either online advertising or content that has been promoted or sponsored. Every fifth post (or 20% of all content) on Instagram, for instance, is targeted advertising.

Online targeted advertising is facilitated by a complex and opaque ecosystem that includes AdTech companies, data brokers, and other third-party companies that track people on websites and apps and combine this data with offline information.[14] On the surface, online advertising may appear harmless. In practice, however, it results in different concrete harms for people: targeting mechanisms can be abused, for instance for political purposes (which may underly the disinformation harms referenced in the White Paper). Targeted ads can be discriminatory (someone might not be not shown a job because she is a woman or a loan because he lives in the wrong neighbourhood) and ads can seek to be manipulative (people can be served tailored information to target those that are most vulnerable). Secondly, the ecosystem of companies that collect, share and aggregate user data is so leaky and complex that it has become impossible for people to understand or control where information about them, their data, ends up as well as the consequences this has for both them as an individual and society.

2. Abuse of ad targeting for political purposes

Examples of the harm caused by using online advertising for political purposes are plenty, and reports from the UK's Information Commissioner Office (ICO), including "Democracy Disrupted", have highlighted concerns with the use of personal data in political campaigning.[15]

In 2018, the UK Information Commissioner's Office fined[16] Emma's Diary, a site offering pregnancy and childcare advice owned by Lifecycle Marketing Ltd, £140,000 for collecting and selling personal information belonging to more than one million people without disclosing in the site's privacy policy how it would be used. Although Lifecycle denied the allegations, the ICO found that the company sold the data to Experian Marketing Services to build into profiles for use by the Labour Party, which targeted mothers in marginal seats with

[12] https://www.facebook.com/help/1155510281178725
[13] https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html
[14] https://privacyinternational.org/long-read/2967/ad-supported-internet-broken-inefficient-and-privacy-nightmare-lets-fix-it
[15] https://ico.org.uk/media/action-wevetaken/2259369/democracy-disrupted-110718.pdf; https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analyticsfor-political-purposes-update.pdf
[16] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/

direct mail during the 2017 election campaign stating the party's intention to protect Sure Start children's centres.

This example shows how far data can travel in an ecosystem that involves more than just online platforms.

3. Abuse of ad targeting to exploit and harass people

In another example, from 2015, a US advertising executive developed[17] a system that used online advertising and tracking techniques, coupled with geofencing, to target ads at women located inside Planned Parenthood clinics and other abortion facilities.

4. Ad targeting that discriminates

Examples of discrimination in online ads are also plentiful. For example, 2013 research on Google AdSense demonstrated that a black-identifying name was 25% more likely to get an ad suggestive of an arrest record.[18] Research from 2015 showed that males were shown ads encouraging the seeking of coaching services for high paying jobs more than females.[19]

5. Harms caused by the ecosystem itself

Over the past decade, targeted advertisement has become exponentially more invasive. To enable targeted advertisement, huge amounts of data about individuals are collected, shared and processed. Trackers from third-parties in the AdTech ecosystem are now included in most apps, on most websites, online shops, email newsletters and increasingly also smart devices. Large platforms like Google, YouTube, Facebook or Amazon collect data about users and non-users alike outside their platforms on hundreds of millions of websites and apps.[20] On top of this, AdTech companies, data brokers, loyalty cards, and even credit referencing agencies track peoples' behaviour both online and offline in ways that are impossible for the average consumer to know about or escape.

Data brokers buy personal data from companies people do business with; collect data such as web browsing histories from a range of sources; combine it with other information about a person (such as magazine subscriptions, public government records, or purchasing histories); and sell their insights to anyone that wants to know more. Even though these companies are on the whole non-consumer facing and hardly household names, the size of their data operations is astounding. Acxiom's Annual report of 2017, for instance, states that they offer data "on approximately 700 million consumers worldwide, and our data products contain over 5,000 data elements from hundreds of sources." Part of the problem is that this data can be used to target, influence, and seek to manipulate people ever more precisely. Acxiom was one of seven data broker, credit reference, and ad tech companies that Privacy International complained about to Data Protection Authorities, including the ICO, in November 2018.[21]

[17] https://rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/
[18] https://arxiv.org/abs/1301.6822
[19] https://content.sciendo.com/view/journals/popets/2015/1/article-p92.xml
[20] https://privacyinternational.org/appdata
[21] https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

A further problem is that this data can also end up being used for purposes other than advertising and also offline. An investigation by Big Brother Watch in the UK, for instance, showed how Durham Police in the UK were feeding Experian's Mosaic marketing data into their 'Harm Assessment Risk Tool', to predict whether a suspect might be at low, medium or high risk of reoffending in order to guide decisions as to whether a suspect should be charged or released onto a rehabilitation program. Durham Police is not the only police force in England and Wales that uses Mosaic service. Cambridgeshire Constabulary and Lancashire Police are listed as having contracts with Experian for Mosaic.[22]

Existing Frameworks

Certain pre-existing legal frameworks, including the relatively new Data Protection Act 2018, already provide the UK with tools to begin to tackle some of the issues identified in the White Paper. PI cautions against undermining these regulatory regimes, even inadvertently, if pursuing the new regime proposed by the White Paper.

Data protection law in the UK (the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 ("DPA")) strengthens the rights of individuals with regard to the protection of their data, imposes more stringent obligations on those processing personal data, and provides for stronger regulatory enforcement powers – in theory. In practice, just over one year on, a lot more still needs to be done and changes are only starting to take place.

The law requires that the processing of personal data (including profiling) complies with the following principles: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality and accountability. Among other obligations, data controllers must have a lawful basis for processing personal data and must facilitate individual's exercise of their rights (such as the right to information, the right to access data, an absolute right to object to direct marketing and the right to erasure). Furthermore, there are prohibitions on certain types of processing, including in relation to personal data revealing special category data (such as racial or ethnic origin, political opinion, religious or philosophical beliefs, health, sex life or sexual orientation) – with limited exceptions– and also in relation to automated decisions, including profiling, which produce legal or other significant effects. The law also imposes obligations in relation to data protection by design and by default and carrying out Data Protection Impact Assessments.

That targeted advertising can have significant effects on people is acknowledged in the Article 29 Working Party Guidelines (adopted by the European Data Protection Board) on Automated individual decision-making and Profiling.[23] As far as PI is aware, however, there are no specific decisions fully dealing with this question yet. There are also provisions and exemptions that threaten to undermine protections, such as paragraph 22 of Schedule 1 of the DPA 2018 that applies to political parties.[24]

---

[22] https://bigbrotherwatch.org.uk/2018/04/a-closer-look-at-experian-big-data-and-artificial-intelligence-in-durham-police/

[23] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi9uaK2vObiAhX76OAKHbguDygQFjAAegQIBBAC&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Fdoc_id%3D49826&usg=AOvVaw3Hbd9vdV-5JxpwJPUmrucm

[24] https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation-political-parties

This is just the beginning of a law that was years in the making, which is why there needs to be focus and resources on pro-actively implementing, strengthening and enforcing it and measures that complement it such as the ePrivacy regulation, if the protections are to become a reality.

There has already been some focus in the UK on the need to update Electoral Law in relation to digital campaigning.[25] However, the White Paper fails to go into any depth on this subject and it is not clear that the proposals in the White Paper would lead to necessary changes.

These above examples serve to illustrate that if it is the online nature of the harms that the White Paper is concerned with, then more attention must be paid to the back end of what we see. The backend includes the data that is collected and inferred as well as the decisions that shape the systems, designs and defaults as well as the unintended consequences of such systems. When it comes to the data, as set out above, data protection law already offers some safeguards through principles, obligations and rights, yet too often what is missing is pro-active implementation and enforcement. There are also some protections that are undermined due to exemptions in the law. Further attention is needed as to how to strengthen existing regulation that has the potential to rein in data exploitation at the back end of what we see (i.e. data protection and ePrivacy) and those that are context specific and need to be urgently updated in the digital age (e.g. electoral law).

Privacy International recommends that the Government focuses more on the back end of our online experience i.e. data and decisions that shape what we see. In doing so, the Government should seek to strengthen existing frameworks (data protection, ePrivacy, and electoral law) rather than starting afresh.

3. Response to specific questions

Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

The response to this question should be understood in the wider context of our response and concerns with the White Paper as set out above.

Transparency reporting can be useful in further understanding how companies operate and how third parties such as advertisers are using these platforms. Transparency is also important in terms of understanding companies' decision-making process. PI questions the need to have a regulator in-between the public and the companies for such transparency reporting to occur, and urges reports be made available to the public without undue delay.

Companies are subject to the principle of Transparency under Article 5 of GDPR and under a duty to provide information to those whose data they process (Article 13 and 14 of GDPR) as well as how it has been processed and access to it (Article 15). To date, companies have a long way to go in terms of their compliance with these provisions (as PI highlighted in submissions to the ICO and other DPAs about a number of companies in the data broker and

[25] E.g., https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf

ad tech sector[26]). GDPR is only just over a year old and still in the early phases of enforcement. More needs to be done to ensure that companies pro-actively implement and respect these obligations.

Transparency must be proactive and up to date, rather than limited to an annual transparency report. However, as a minimum, annual transparency reports provided by companies should include detailed information about how content is being targeted to users, which at present still remains unclear on all large social media platforms in the UK. Such transparency should not be limited to advertising, but also include other content, such as the methods of curation, filtering, pushing, and recommendation of content.

In relation to 'political' advertising, transparency reporting should include, as a minimum, insights into:

- how a company defines political advertising and social 'issue-based' advertising;
- number of impressions that an ad received within specific geographic and demographic criteria (e.g. within a political district, in a certain age range), broken down by paid vs. organic reach;[27]
- targeting criteria used by advertisers to design their ad campaign, as well as information about the audience that the ad *actually* reached;[28]
- information about ad spend per political actor;
- information about microtargeting, including whether the ad was a/b tested and the different versions of the ad; if the ad used a lookalike audience; the features (race, gender, geography, etc.) used to create that audience; if the ad was directed at platform-defined user segments or interests, and the segments or interests used; or if the ad was targeted based on a user list the advertiser already possessed;[29]

With showing this information, it is simultaneously important to understand the potential necessity of organisations to reach narrow vulnerable communities through microtargeting. For example, including detailed data about a micro-targeted campaign focused on showing informational ads to a small affected community raises potential risks, which must be considered.

Any such transparency measure should be developed in consultation with those regulators already considering this issue, including the UK ICO and the Electoral Commission as well as civil society and researchers.

[26] https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad
[27] https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/
[28] https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/
[29] https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/

Some failures in relation to transparency more generally and what more must be done by certain companies is highlighted in Ranking Digital Rights Index, the most recent from 2019.[30]

Question 2: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

The response to this question should be understood in the wider context of our response and concerns with the White Paper as set out above. Furthermore, more information is needed about how any such 'super complaint' system is envisaged.

Here we want to emphasise that regulatory regimes are stronger and more effective if the ability of individuals to make complaints is supplemented by the ability of civil society acting in the public interest to bring complaints. This is particularly important if complaints are to address and prompt scrutiny of systemic issues, including those that might impact on more than one individual, particular groups, or society as a whole. This is recognised to an extent, for example, in the introduction of Police Super-complaints.[31] This mechanism has been used by Liberty and Southhall Black Sisters, for example, to challenge Police data sharing for immigration purposes.[32]

Such mechanisms are particularly important from a privacy perspective, as privacy invasions are often invisible, harms frequently only happen in the future, and they always affect some people more than others. The need for a form of collective redress and to empower civil society to take action is recognised in Article 80(2) of GDPR. Article 80(2) provided for the ability of "not-for-profit body, organisation or association, which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data" to make complaints and seek an effective remedy under GDPR independently of a data subject's mandate. The benefits of such a provision are explained by the European Data Protection Supervisor[33] and by PI[34]. In spite of this, Article 80(2) of GDPR was not implemented in the UK DPA 2018. Instead, it will be the subject of a review 30 months from the Act having come into force. Review of Article 80(2) of GDPR under section 189(2)(c) of the DPA 2018 should be a priority for the Government. At EU level, the proposed Representative Action Directive would improve the ability to take collective actions but seems unlikely to apply in the UK.

Failure to include a super complaint mechanism or other form of collective redress (such as in Article 80(2) of GDPR) to enable civil society to tackle systemic issues undermines protections for individuals and society. To reiterate, any such measure should supplement and bolster, not replace, the ability of individuals to complain and/or to be represented by civil society in complaints.

[30] https://rankingdigitalrights.org/index2019/
[31] https://www.gov.uk/government/collections/police-super-complaints
[32] https://www.gov.uk/government/publications/police-data-sharing-for-immigration-purposes-a-super-complaint
[33] https://edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_en
[34] https://privacyinternational.org/blog/1050/why-we-need-collective-redress-data-protection

Question 6: In developing a definition for private communications, what criteria should be considered?

The response to this question should be understood in the wider context of our response and concerns with the White Paper as set out above.

The paper states that "the framework will ensure a differentiated approach for private communication, meaning any requirements to scan or monitor content for tightly defined categories will not apply to private channels". We find this question problematic to the extent it seeks definitions that differ from those already provided by international instruments and judicial organs that have pronounced on the distinction between private and public communications.

Private life and communications have been interpreted broadly by the European Court of Human Rights. The Court has highlighted that "Private life is a broad term not susceptible to exhaustive definition."[35]

Private communications include a wide range, from electronic messages to internet use and telephone communications. The content and form of the correspondence is irrelevant to the question of interference.[36]

All forms of censorship, interception, monitoring, seizure and other hindrances come within the scope of Article 8. Various circumstances inform the distinction between public and private communications, but they are always motivated by an element of 'reasonable expectation of privacy'. The Court has long held that "there is […] a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".[37] It has highlighted that "private life considerations may arise [...] once any systematic or permanent record comes into existence of such material from the public domain."[38] Compilation of data and file gathering on particular individuals, even without the use of any covert surveillance method, constitutes an interference with the right to privacy and therefore needs to be justified as necessary to pursue a legitimate aim in a democratic society.[39]

Definitions of different forms of communication are also contemplated in the EU Directive on privacy and electronic communications (implemented in the UK through the Privacy and Electronic Communications Regulations and regulated by the ICO). The ePrivacy framework is currently undergoing revision through the negotiation of the ePrivacy Regulation.

There is therefore no need to define private communications again, but to recognise that they must be construed broadly and consistently with existing legal protections and case law. This

[35] *Niemietz v. Germany*, Appl. no. 13710/88, Judgment ECtHR, 16 December 1992, para. 29; *Pretty v. the United Kingdom*, Appl. no. 2346/02, Judgment, ECtHR, 29 April 2002, para. 61.
[36] *A. v. France*, Appl. no. 14838/89, Judgment, ECtHR, 23 November 1993, paras. 35-37; *Frérot v. France*, Appl. no. 70204/01, Judgment, ECtHR, 12 June 2007, para. 54.
[37] Von Hannover v. Germany (No. 2), Appl. nos. 40660/08 and 60641/08, Judgment, Grand Chamber, ECtHR, 7 February 2012, para. 95.
[38] P.*G. and J.H. v The United Kingdom*, Appl no. 44787/98, Judgment, ECtHR, 25 September 2001, para. 57; *Peck v. The United Kingdom*, Appl. no. 44647/98, Judgment, ECtHR, 28 January 2003, para. 59.
[39] *Rotaru v. Romania*, Appl. no. 28341/95, Judgment, Grand Chamber, ECtHR, 4 May 2000, paras. 43-44; *Amann v. Switzerland*, Appl. no. 27798/95, Judgment, Grand Chamber, ECtHR, 16 February 2000, paras. 65-67.

will ensure that any interference is prescribed by an appropriate legal framework and is necessary and proportionate to the legitimate aim pursued.