PI's response to DCMS' open consultation on data protection reform in the UK.

Data: A New Direction

November 18th 2021

Email to: DataReformConsultation@dcms.gov.uk

Privacy International (PI) welcomes the opportunity to respond to this consultation on proposed reforms to data protection in the UK as part of the Data: A New Direction consultation launched on September 10th 2021.

PI is a registered charity based in London that works at the intersection of modern technologies and rights. We regularly examine how company practices impact individual privacy and autonomy, especially where the use of data and technology is concerned. We campaign for strong regulations and better protections for the public.

PI has a long history of engaging with and supporting data protection policy and legislation around the world and upholding the rights contained therein. The right to privacy and data protection are linked to some of the most important political and heart-searching questions of our time. How can exploitation of the vulnerable be prevented? How does the UK treat its immigrants who bring key skills and prosperity to the country? What safeguards are there against potential corruption of the democratic process by new technologies and their use by political parties and third parties?

These are the questions that drive PI's work everyday. We are therefore disappointed by the framing of Data: A New Direction. At the core of the proposal is the suggestion that data protection is a burden on companies. It appears to be driven by the commercial interests of a few companies who may benefit from weaker rights protection, the result being the proposed loss of many important protections for people. Ultimately, removing protections in such a way means removing incentives for companies to respect privacy. This creates a race to the bottom that will not foster the innovation the government seeks. The proposal is a backward step. For example, innovation (eg. in AI) relies on people sharing data; in order for people to share their personal information, they need to feel confident about doing so. This

proposal does not foster trust. A better proposal would be to enforce what we have and improve protections rather than removing them.

PI's response therefore focuses on the real world impact the loss of protections would mean by drawing on examples of PI's research, investigations and advocacy from around the world.

Chapter 1: Reducing barriers to responsible innovation.

Section 1.2- "Scientific Interest"

- *Q1.2.8 To what extent do you agree that it would benefit researchers to clarify that data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of personal data processing at the time of data collection?*

Strongly disagree

- *Q1.2.8a Explanation and supporting evidence:*

PI urges caution with regard to provisions that seek to potentially undermine the strict conditions around obtaining consent. The GDPR placed stronger conditions on obtaining consent and in our work, we have seen how this is constantly sought to be undermined by various actors. Introducing concepts such as "general" or "broad" consent might inevitably result in people's (sensitive) personal data being used for purposes that go far beyond what they might have originally foreseen.

PI has investigated this issue extensively; we are shocked at how intrusive and harmful data collection has become under the cover of "consent", including health data that could, under this proposal, be interpreted as "scientific research". For example, see PI's investigations:

Your Mental Health For Sale: https://privacyinternational.org/campaigns/your-mental-health-sale

An Unhealthy Diet of Targeted Ads: https://www.privacyinternational.org/long-read/4603/unhealthy-diet-targeted-ads-investigation-how-diet-industry-exploits-our-data

PI's investigation, ***No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data***, found that several apps were sharing sensitive health data with third parties, which was not explicit in their privacy policies: https://privacyinternational.org/long-read/4316/we-asked-five-menstruation-apps-our-data-and-here-what-we-found

As the European Data Protection Board (EDPB) Guidelines 05/2020 on consent under Regulation 2016/679 undelrine, consent is only valid as a legal basis for processing if "a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment". It is hard to see how "general" consent can still allow individuals to maintain effective control over their personal data at all times during various research stages.

- *Q1.2.9 To what extent do you agree that researchers would benefit from clarity that further processing for research purposes is both (i) compatible with the original purpose and (ii) lawful under Article 6(1) of the UK GDPR?*

Strongly Disagree

- *Q1.2.9a Explanation and supporting evidence:*

Please refer to the concerns raised in Q1.2.8b. In addition:

Purpose limitation is one of the core principles of data protection law. Application of the principle ought to consider factors listed in Article 6(4) GDPR. The question of purpose limitation is intrinsically linked to what one can expect to be done with their personal data.

We would like to draw particular attention to EDPB Guidelines 05/2020 on consent under Regulation 2016/679, para 159:

"When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research."

For example, in the complaints that PI filed against Clearview AI[1], together with 3 other organisations across the EU, PI demonstrated that re-use of even publicly available personal data, such as facial images posted on social media or websites, for processing in a biometric database clearly falls outside of such expectations.

- *Q1.2.10 To what extent do you agree with the proposals to disapply the current requirement for controllers who collected personal data directly from the data subject to provide further information to the data subject prior to any further processing, but only where that further processing is for a research purpose and it where it would require a disproportionate effort to do so?*

Strongly Disagree

- *Q1.2.10a Explanation and supporting evidence*

Please refer to the concerns raised in response to Q1.2.8b. In addition:

One of the main notions underpinning data protection law is that of individual self-determination, namely the ability of individuals to exercise full and effective control over their personal data and decide how and whether they should be processed. Any restrictions placed upon existing guarantees contained in current European and UK data protection laws will achieve opposite results and essentially undermine the very essence of the rights that the legislation was intended to protect in the first place. The fully informed and freely given consent of individuals is essential to the design of ethical, unbiased and fair research. By re-purposing data without informing and obtaining consent from data subjects, controllers would violate the trust that individuals have placed in them by providing their data. They would also risk undermining the value of their research by relying on datasets that do not reflect what personal data was provided for, and whose context is wholly different to the original.

Section 1.3 Further Processing.

No comments at this time.

[1] https://privacyinternational.org/sites/default/files/2021-05/2021.05.27%20-%20Clearview%20AI%2C%20Inc.%20-%20Privacy%20International%20Complaint%20%28ICO%29%20%5BRedacted%5D_0.pdf

Section 1.4 Legitimate Interests

- *Q1.4.1 To what extent do you agree with the proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test?*

Strongly Disagree

- *Q1.4.1a Explanation and supporting evidence*

Legitimate interests of the controller or a third party may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. The use of this legal basis for processing requires controllers to carry out a balancing exercise between the specific interests they seek to protect and the impact of the latter on data subject's rights and freedoms.

As Recital 47 of the GDPR underlines, legitimate interests can only exist,

"where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place."

Essentially the balancing exercise lies at the heart of using legitimate interests as a legal basis for processing personal data. Depriving legitimate interests of the balancing exercise will in most cases result in processing operations that bear a disproportionate or onerous impact on data subjects' rights.

The ICO has stated that while 'legitimate interests' basis does allow for some flexibility on the part of controllers, this does not imply that it is without limits or can be moulded exactly to fit or justify any processing operation.[2]

[2] ICO, Guide to the General Data Protection Regulation (UK GDPR) – Lawful basis for processing – Legitimate interests. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UKGDPR/lawful-basis-for-processing/legitimate-interests/

In its resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)), the European Parliament raised serious concerns about how this legal basis keeps being abused, warning that it is "very often abusively mentioned as a legal ground for processing" (para 7). The European Parliament further pointed out that:

"controllers continue to rely on legitimate interest without conducting the required test of the balance of interests, which includes a fundamental rights assessment; is particularly concerned by the fact that some Member States are adopting national legislation to determine conditions for processing based on legitimate interest by providing for the balancing of the respective interests of the controller and of the individuals concerned, while the GDPR obliges each and every controller to undertake this balancing test individually, and to avail themselves of that legal ground […]"

Similar concerns are also raised in the 2014 Opinion by the A29 Working Party:

"At a time of increasing imbalance in 'informational power', when governments and business organisations alike amass hitherto unprecedented amounts of data about individuals, and are increasingly in the position to compile detailed profiles that will predict their behaviour (reinforcing informational imbalance and reducing their autonomy), it is ever more important to ensure that the interests of the individuals to preserve their privacy and autonomy be protected."

In its submission before the ICO[3], PI illustrated how the legitimate interests legal basis ensures a fair processing of individuals' personal data as well as how facial recognition companies often abuse it by failing to take the implications of their processing operations for data subjects' rights into consideration or by engaging in disproportionate data exploitation practices.

Section 1.5: Artifical Intelligence and Machine Learning

- *Q1.5.17 To what extent do you agree with the Taskforce on Innovation, Growth and Regulatory Reform's recommendation that Article 22 of UK GDPR should be removed and solely automated decision making permitted where it meets a lawful ground in*

[3] https://privacyinternational.org/sites/default/files/2021-05/2021.05.27%20-%20Clearview%20AI%2C%20Inc.%20-%20Privacy%20International%20Complaint%20%28ICO%29%20%5BRedacted%5D_0.pdf

Article 6(1) (and Article 9-10 (as supplemented by Schedule 1 to the Data Protection Act 2018) where relevant) and subject to compliance with the rest of the data protection legislation?

Strongly Disagree

- *Q1.5.17a Explanation and supporting evidence*

The protection afforded by Article 22 of the UK GDPR cannot be overstated, and the suggestion of its removal constitutes a grave threat to individuals. Article 22 is designed to guard against the risks of automated-decision making. These risks are identified by the ICO[4] as follows: - Profiling is often invisible to individuals; - People might not expect their personal information to be used in this way. - People might not understand how the process works or how it can affect them. - The decisions taken may lead to significant adverse effects for some people. Importantly, the ICO further notes:

"Just because analysis of the data finds a correlation doesn't mean that this is significant. As the process can only make an assumption about someone's behaviour or characteristics, there will always be a margin of error and a balancing exercise is needed to weigh up the risks of using the results."

The risks above are expressed both in terms of risks to the concerned individual's rights and freedoms, as well as technical risks. In relation to individuals' rights and freedoms, the removal of Article 22 not only undermines the concept of consent, but blatantly defies the principles of fairness and transparency contained in Article 5 of the UK GDPR. From an objective standpoint, it is unfair for individuals to be subjected to solely automated processing with legal and similarly significant effects, as an error - if it were to occur - is unlikely to be immediately identified and/or rectified. The burden is therefore on the affected individual to identify the error, approach a complaint mechanism, and seek redress. This is an onerous burden for any individual to bear. Similarly, to the extent that automated processing can be of significant conceptual and technical complexity, it is unlikely that the affected individuals will fully understand the functioning and data processing activities of

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id2

such systems; making it nearly impossible for data controllers and processors to fully comply with the principle of transparency.

In relation to the risk of errors, government must consider that Article 22 exists to guard against mistakes which could be time-consuming and costly to government entities. Here we present some examples from PI's report, *"Benefitting whom? An overview of companies profiting from "digital welfare",*[5]

- "we filed a series of FOI requests to four London councils (Ealing, Islington, Camden, Croydon) concerning the London Counter Fraud Hub, a system designed by the Chartered Institute of Public finance & Accountancy (CIPFA) in order to detect fraud in applications for the council tax single person discount. The system was meant to process large amounts of data to identify fraudsters. The system was a cause of great concerns when it was first revealed in the media. With more and more dicussions on algorithmic bias and the revelations that the system had a 20% failure rate, many feared they would see their benefits cut unfairly."
- "Fundación Karisma's research into the Colombia' System of Identification of Social Program Beneficiaries (SISBÉN) which produces a household vulnerability index that is used to identify the beneficiaries of social assistance programmes in Colombia. They exposed how, as they were trying to modify the algorithm of the (SISBÉN), the Department of National Planning (DNP) had decided to include a prediction of "capacity to generate income" in an attempt to reduce the number of people who could be eligible for social benefits, and an exchange system was created with 34 public and private databases to verify the data that was being reported by applicants."

Section 1.6 Data Minimisation and Anonymisation

Any legal test must require to take into account the lastest technical developments in the field of data analsyis and be reviewed by independent data analysis experts.

[5] https://privacyinternational.org/long-read/4144/benefitting-whom-overview-companies-profiting-digital-welfare

PI has regularly raised concerns about the limits of pseudoanonymous and anonymised data. For example, journalists from the German public broadcaster Norddeutscher Rundfunk ("NDR") were able to identify the sexual preference and medical history of judges and politicians, using online identifiers.[6] This example serves to illustrate the insights that can be gleaned from seemingly mundane and pseudoanonymous data and the value it might have.

Even if it is not a company's intention to directly identify an individual, this is still possible, due to the vast amounts of data it might collect, generate and process. And, even when data seem to be truly anonymised by companies, and consequently exempt from the protection guaranteed by data protection standards , this (pseudo-) anonymisation might still lead to the re-identification of individuals. For example, while personal data is routinely (pseudo-) anonymised within datasets, multiple studies have shown the potential de-anonymisation capabilities of AI technologies. In a study published in Nature, researchers were able to demonstrate that, despite the anonymisation techniques applied, "data can often be reverse engineered using machine learning to re- identify individuals".[7]

Section 1.7 Innovative Data Sharing Solutions

No comments at this time.

Section 2: Reducing burdens on business and delivering better outcomes for people.

Section 2.2 Reform of the Accountability Framework

- *Q2.2.7 To What extent do you agree with teh following statement: 'Under the current legislation, data protection impact assessment requirements are helpful in the identification and minimisation of data protection risks to a project'?*

Strongly Agree

- *Q2.2.8 To what extent do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments?*

[6] See Alexander Martin, Browsers nix add-on after Web of Trust is caught selling users' browsing histories, The Register, 7 November 2016, https://www.theregister.co.uk/2016/11/07/browsers_ban_web_of_trust_addon_after_biz_is_caught_selling_its_users_browsing_histories

[7] See: Luc Rocher, Julien M. Hendrick & Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models", 23 July 2019, https://www.nature.com/articles/s41467-019-10933-3)

Strongly Disagree

- *Q2.2.8a Explanation and supporting evidence.*

DPIAs are particularly important where there is a risk to the rights and freedoms of individuals, including where the processing involves sensitive personal data, automated decision-making, profiling, or monitoring of public spaces. An impact assessment requires, as a minimum:

- an assessment of the necessity and proportionality of the processing
- the risks to individuals
- how these risks are to be addressed.[8]

It is contradictory - and self-defeating - to promote transparency requirements for public bodies and government contractors that use algorithms and decision-makers in paragraph 290, and at the same time remove the requirement for a DPIA as is proposed.

The tone of the consultation places emphasis on the impact of data protection legislation on 'organisations', the desire for innovation and the need for responsible use of data. However, the Government and government authorities process vast amounts of data. For example the increasing use of mobile phone extraction in both policing and migration context, social media monitoring and facial recognition. The ICO has been critical about the excessive processing of personal data by the police in the context of mobile phone extraction. The Police, Crime, Sentencing and Courts Bill extends powers to other electronic devices and for the first time, at least publicly as far as we are aware, to Immigration Officers.

Further, an array of digital technologies are being deployed in the context of immigration and border enforcement and administration which gather and process increasing amounts of data. This includes aerial and space surveillance practices and GPS location tracking in immigration bail.

There is an existing lack of publicly accessible guidance, policy and legislation. In this context, the proposed removal of an obligation to carry out DPIAs will undermine

[8] See PI, A Guide for Policy Engagement on Data Protection: The Keys to Data Protection, August 2018 p78 https://www.privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

safeguards, and will only benefit government authorities when they do not act responsibly, do not consider the impact of their activities and potentially could be acting unlawfully. We already see variable quality in DPIA forms completed by government authorities - this shows a frequent lack of understanding of data processing activities and their consequences, but probing questions around DPIAs often leads to improvements in the design of these data processing activities to make them more useful, more efficient and less harmful to individuals. Removing the DPIA requirement would simply undermine the quality of public authorities' public policy and decision-making.

DPIAs play a crucial role in enabling public bodies to fully appreciate, assess and mitigate the negative impacts of proposed automated systems. This is vividly illustrated by the recent experience of the Ofqual grading algorithm. In 2020, during the aftermath of the issues arising from the Ofqual grading algorithm, the Ofqual privacy impact statement[9] - a simplified version of the DPIA carried out by Ofqual - enabled those adversely impacted by the algorithm to understand, albeit to a limited extent, some of the functioning of the system. This would not have been possible without a DPIA. Ultimately, the Ofqual grading algorithm was shown to have adverse impacts larger than originally foreseen. This clearly shows that while DPIAs are not a guarantee that an automated system will be fully observant of individuals' rights and freedoms, they constitute an important baseline.

The importance of a DPIA was more recently brought to the fore as a result of the legal challenge against the automated visa streaming tool used by the Home Office. In response to the legal challenge, the government committed to redesigining the algorithm behind the visa streaming tool[10], and similarly committed to undertake a DPIA for the interim process it intended to use as a replacement. In other words, the Home Office understood the importance of a DPIA in ensuring that any future system observed individual rights and freedoms.

[9] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909372/6666_Privacy_Impact_Statement_-_Grading_2020.pdf

[10] https://techcrunch.com/2020/08/04/uk-commits-to-redesign-visa-streaming-algorithm-after-challenge-to-racist-tool/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAIe3qw9OQp2_RWwkRObxLMSfI_ywd5CoLHAgj08sXx3DGQUeU_Gm-W_FeSOceI4rlQvbtnWktjB4cijmYHCXrYoE09TB2FABZIK7Yv2wqne_U1eIJ_4DHsNsOB5gi-AH8AsWpYeqwCDJDWRrg95kLIAtwq8cUD-u47IyHRiso6cl

Lastly, DPIAs enable civil society organisations to scrutinise, inform and advise on proposed automated systems before, during and after their implementation. In preparing its response to the 2021 National Fraud Initiative consultation[11], PI extensively drew upon the published 2018 DPIA on the National Fraud Initiative[12]. This enabled PI to understand and in turn explain to others[13] the functioning of the National Fraud Initiative, as well as produce a robust response to the consultation.[14]

To highlight a recent global example on the importance and weight of DPIAs, in Kenya the rollout of the National Integrated Identity Management System (NIIMS) and processing of data was halted by the high court because they didn't complete a DPIA.[15]

Section 2.3 Subject Access Requests

- *Q2.3.4 To what extent do you agree with the following statement: 'There is a case for re-introducing a small nominal fee for processing subject access requests (akin to the approach in the Data Protection Act 1998)'?*

Strongly Disagree

Q2.3.4a Explanation and supporting evidence.

Introducing a fee would be problematic, particularly for the gig-economy sector and other lower income individuals. It is only through subject access requests that they are able to obtain information that numerous companies like Deliveroo, Uber, Amazon etc collect about them. Data collection by delivery companies is very opaque and the workers are not told how much data is collected about them, nor how this data is later used. The only way for them to understand how their data is processed, in order to allow them to assert their rights, is therefore through data subject access requests. However, considering the fact that gig-economy workers tend to be much lower paid, fees for data subject access request will have a significant negative impact on their ability to protect their rights. This is very concerning in

[11] https://https//www.gov.uk/government/consultations/consultation-on-the-expansion-of-the-national-fraud-initiative-nfi-data-matching-powers-and-the-new-code-of-data-matching-practice
[12] https://www.whatdotheyknow.com/request/693304/response/1693922/attach/5/2018 09 19 DPIA 18 19 Redacted.pdf?cookie_passthrough=1
[13] https://privacyinternational.org/explainer/4461/national-fraud-initiative
[14] https://privacyinternational.org/news-analysis/4462/resisting-profiling-our-response-national-fraud-initiative-consultation
[15] https://nation.africa/kenya/news/judge-orders-state-to-regularise-huduma-namba-roll-out-3582906

light of the inherent power imbalance that exists between delivery platforms/employers and their workers.[16]

Section 2.4 Privacy and Electronic Communications

- *Q2.4.2 To what extent do you agree with the proposal to remove the consent requirement for analytics cookies and other similar technologies covered by Regulation 6 of PECR?*

Strongly Disagree

Q2.4.2a Explanation and supporting evidence.

We disagree with the framing of the proposal that analytics cookies are harmless and consent notifications are bothersome for users.

"Analytics cookies and similar technologies" are currently a gateway to personal data collection and processing for micro-targeted advertising, and much more. PI's research into data collection from mental health websites[17] revealed that answers to depression tests were shared with third parties as a result of these technologies being blindly deployed, without a real assessment of how much data they can collect and for which purpose. Our investigation into diet ads online revealed similar issues.[18]

Given the complexity of online advertising and its heavy reliance on tracking and other invasive data collection processes, removing the need for consent would open a door to indiscriminate surveillance practices by private companies. Our devices and the web are already full of tracking and spying technologies and consent is currently the only protection that users have at their disposal to somewhat limit how they are being tracked and monitored.

The question posed here should not be about removing consent requirements, but rather what can be done to reign in such gratuitious data collection in the first place.

[16] https://privacyinternational.org/case-study/751/case-study-gig-economy-and-exploitation
[17] https://privacyinternational.org/campaigns/your-mental-health-sale
[18] https://privacyinternational.org/long-read/4603/unhealthy-diet-targeted-ads-investigation-how-diet-industry-exploits-our-data

- *Q2.4.9. To what extent do you agree that the soft opt-in should be extended to non-commercial organisations?*

Strongly disagree

Q2.4.9a Explanation and supporting evidence.

We have concerns with how the "soft opt-in" regime is failing in the context of commercial organisations and would not recommend it is extended, particularly to political parties (see Q2.5.2)

To illustrate harm that comes from people unknowingly giving consent for their personal data to be shared, consider the example of Bounty UK Limited. In April 2019, Bounty were fined £400,000 by the UK's Information Commissions Office for illegally sharing the personal information of mums and babies as part of its services as a "data broker" between 1 June 2017 and 30 April 2018.

Bounty collected personal data from a variety of channels both online and offline: its website, mobile app, Bounty pack claim cards and directly from new mothers at hospital bedsides.

The ICO's decision named only the four largest recipients of the data collected and shared by Bounty, out of 39. One of these companies was Sky - Bounty provided Sky over 30 million records.

In 2021, PI wrote to Sky to ask what actions they had taken to locate the data received from Bounty and whether they deleted it, if they had attempted to notify any affected people, or if they had changed their internal policy or practice with regards to receiving third-party data.

Sky refused to answer PI's questions, saying "due to both passage of time and the confidential nature of the information being requested, we are not able to respond to your questions".

It remains unknown whether and how the data that Bounty collected and shared is continued to be used to profile and target those 14 million mothers and their babies today.

"Soft opt-in" is another word for manipulation of users into agreeing to something they don't see or understand. This leads to anger and frustration when they are later targeted on the

basis of invisibly collected data. Rather than allowing soft opt-in, we should work towards models of information and consent that enable organisations to clearly explain what they seek to do with people's data - so that when the purpose is clear, valuable and not harmful, people are able to consent in full knowledge of the consequences and in support of the processing aims.[19]

Section 2.5 Use of personal data for purposes of democrativ engagement.

- *Q2.2.5.2 If you think political campaigning purposes should be covered by direct marketing rules, to what extent do you agree with the proposal to extend the soft opt-in to communications from political parties?*

Strongly Disagree

- *Q2.5.3 To what extent do you agree that the soft opt-in should be extended to other political entities, such as candidates and third-party campaign groups registered with the Electoral Commission?*

Strongly Disagree

Q2.5.3a *Explanation and supporting evidence.*

PI has investigated the use of personal data in political campaigning since the run up to 2017 Kenyan elections and the involvement of a then little known company called Cambridge Analytica. We have repeatedly raised concerns about the use of personal data in political campaigning: the lack of transparency and impact on privacy of gratuitous data collection, profiling and targeting of messages/adverts.

We must address that political parties use consultants/third parties/ "representatives" for campaigns/communications. It is extremely unclear how they are using personal data and this needs strong data protection and enforcement. PI is calling for urgent reform of the use of personal data in political campaigning, stronger protections and enforcement, not less.

[19] https://privacyinternational.org/long-read/4620/how-company-illegally-exploited-data-14-million-mothers-and-babies

PI examples:

- PI analysed publicly available material in order to profile 5 companies involved in political campaigning: Aristotle (USA), C|T Group (UK), Data Sciences Inc.(Canada), eXplain (France) and uCampaign (USA).[20] From the publicly available information, including the companies' own marketing material and privacy policies, we are concerned about the lack of information regarding the personal data they collect and process for election campaigning in line with the data protection principles of lawfulness, fairness and transparency. We also have further questions on how companies involved in political campaigning use personal data held by third parties.
- Following our research and investigation efforts, we are concerned about the lack of transparency C|T Group provides about their data collection, profiling and targeting practices in their work for political parties during elections. We have therefore asked the ICO to conduct such inquiries into CT Partners Limited's role in the UK 2019 General Election as part of the Commissioner's ongoing work into the the use of data analytics for political purposes.[21]

Chapter 3: Adequacy

- *Q3.2.1. To what extent do you agree that the UK's future approach to adequacy decisions should be risk-based and focused on outcomes?*

Disagree.

- *Q3.2.1a Explanation and supporting evidence.*

Reducing the standard of assessment to looking only at "actual" risks or risks "in practice" will lead to a complete disregard for (1) the invisible consequences of data processing, as the assessment will not seek to look beyond what is seen to be done, and (2) the potential for practices to change, so that what could be legally done but isn't currently done won't be considered. Reducing the standard of assessment for adequacy decisions can only lead to poorer decisions and to a race to the bottom. The current system for adequacy assessment,

[20] https://privacyinternational.org/long-read/4374/data-exploitation-and-political-campaigning-company-guide-resource
[21] https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem-political-campaigning

while far from perfect nor up to the intended standard, should lead to other countries improving their data protection frameworks, rather than lead the UK to lowering its own.

Chapter 4: Delivering Better Public Services

- *Q4.3.3 To what extent do you agree with the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies?*

Somewhat agree

Q4.3.3a Explanation and supporting evidence.

While it is undisputed that there are circumstances in which health data may be lawfully and legitimately processed by public and private bodies during public health emergencies, it is essential that there is full transparency on (i) the nature of the relationship between those actors, and (ii) the data processing activities pertaining to each of the actors involved in the handling of health data. Recent history in the UK shows that this is rarely the case.

In recent years, PI has investigated contracts between the NHS and private actors Palantir and Amazon. In the case of Palantir, and as PI reported[22], the limited documents disclosed by the government in relation to its contract with Palantir are unclear on the conditions limiting Palantir's access to data after the partnership ends. According to those disclosed documents, Palantir is permitted to undertake any processing activities it deems useful, making function creep a real concern. Another recent example is the contract between the National Health Service and Amazon, the full disclosure of which PI pursued by way of a complaint to the ICO[23] which was partially granted[24]. The fact that civil society organisations are essentially left with no other option but to raise a complaint with the ICO in order to access public-private contracts not only reveals poor transparency standards, but is also a reflection of the level of resources required to effectively scrutinise public-private partnerships. Against this background, while any clarification from the government is

[22] https://privacyinternational.org/long-read/3977/corona-contracts-public-private-partnerships-and-need-transparency
[23] https://privacyinternational.org/node/3298
[24] https://privacyinternational.org/legal-action/challenge-big-tech-commercial-interests-healthcare

welcome, it should not merely serve government or commercial interests: it should be used to inform civil society.

Section 4.4 Building Trust and Transparency

- *Q4.4.1 To what extent do you agree that introducing compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data will improve public trust in government use of data?*

Agree

Q4.4.1a Explanation and supporting evidence.

We support further transparency in this area and welcome compulsory transparency reporting on the use of algorithms in decision making. However, a transparency reporting requirement should not replace DPIAs, rather should sit on top as an additional measure to compliment the information required in a DPIA.

Chapter 5: Reform of the ICO

- *Q.5.2.5 To what extent do you agree with the proposal to introduce a duty for the ICO to have regard to competition when discharging its functions?*

PI urges caution on introducing this duty, because of the risk that the ICO would be put under pressure to consider potential negative implications on competition of limiting data processing/enforcing data subject rights. Some requirements under data protection might affect competition (e.g. limits on transferring data) but the enforcement of data protection standards should not be made conditional upon the effect it may have on competition. Additionally PI is concerned that by introducing this duty, the decision of the ICO risks been open to challenge on purely business/market grounds.

- *Q.5.2.6 To what extent do you agree with the proposal to introduce a new duty for the ICO to cooperate and consult with other regulators, particularly those in the Digital Regulation Cooperation Forum (CMA, Ofcom and FCA)?*

Strongly agree

In the digital economy the growing need for increased cooperation and coordination between regulators in in order to achieve a better understanding of companies' practices which affect individuals and businesses has long been recognised in the UK, the EU and elsewhere. Introducing a duty to cooperate and consult would strengthen the capacity of relevant regulators to assess consider the data protection and consumers' implication of the business models that rely on the processing of data, building on the activities of the UK Digital Regulation Cooperation Forum.[25]

- *Q5.5.3 To what extent do you agree with the proposal to give the Secretary of State a parallel provision to that afforded to Houses of Parliament in Section 125(3) of the Data Protection Act 2018 in the approval of codes of practice, and complex and novel guidance?*

Strongly Disagree

Q5.5.3a

We believe this provision would harm the regulator's independence.

- *Q.5.6.2 To what extent do you agree with the proposal to introduce a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller prior to lodging a complaint with the ICO (with guidance and exemptions)?*

Strongly Disagree

Q.5.6.2a *Explanation and supporting evidence.*

At the moment, no such requirement is placed upon data subjects. Introducing this will have a negative or disproportionate impact on data subjects' right to seek remedy for any infringements of their data protection rights.

Engaging with companies can be daunting and time consuming. A data subject may not always know who the controller is as certain ecosystems are shrouded in opacity. PI has repeatedly called upon regulators in the EU and globally to investigate and take enforcement action against adtech and data brokers because of this.
As PI research has illustrated, it can be extremely difficult for a data subject to obtain

[25] https://www.ofcom.org.uk/__data/assets/pdf_file/0017/215531/drcf-workplan.pdf

answers from data controllers, either through companies not responding to requests or seeking to evade their GDPR obligations.[26]

In many of our investigations we have not received any responses at all following our submission of DSARs.[27]

Q5.6.4 To what extent do you agree with the proposal to set out in legislation the criteria that the ICO can use to determine whether to pursue a complaint in order to provide clarity and enable the ICO to take a more risk-based and proportionate approach to complaints?

Strongly disagree

Q5.6.4a Explanation and supporting evidence.

PI is concerned that any criteria that enable the ICO to ignore complaints will impede the effective exercise of individuals data protection rights. While existing data protection legislation allows for individuals to (also) seek remedies before courts, this is not always an appropriate or affordable alternative for many data subjects. The introduction of any statutory powers for the ICO to ignore complaints will interfere with individuals' right to privacy as well as their right to seek effective remedy under Article 13 of the ECHR, which must be carefully balanced against the interests they seek to promote. Due to the opaque nature of many data processing activities, many complaints need to be fully investigated in order to determine the extent of the risk to individuals. Allowing the ICO to brush off complaints because "not risky enough" on the face of it is a blatant affront to the exercise of fundamental rights.

- *Q5.7.7 To what extent do you agree with the proposal to amend the statutory deadline for the ICO to issue a penalty following a Notice of Intent in order to remove unnecessary deadlines on the investigations process?*

Strongly disagree

---

[26] See PI's investigation into obtaining data from advertisers on Facebook: https://privacyinternational.org/campaigns/advertisers-facebook-who-heck-are-you-and-how-did-you-get-my-data

[27] See PI's research into diet ads. https://privacyinternational.org/long-read/4603/unhealthy-diet-targeted-ads-investigation-how-diet-industry-exploits-our-data

Q5.7.7a Explanation and supporting evidence.

PI urges caution as certain situations will inevitably require urgent action by the regulator, especially with regard to data protection law infringing processing operations that can involve sensitive/special-category data and take place at a large scale. The amount of time it takes for the ICO to reach a Notice of Intent following the opening of an investigation is already long, and leaves many individuals without remedy for this protracted time. Extending the deadline for the issue of penalty notices would simply add to these already unacceptable delays.

END