ICO submission to the inquiry of the House of Lords Select Committee on Communications - The Internet : To Regulate or not to Regulate?

16 May 2018

ico.
Information Commissioner's Office

Contents

About the ICO

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The ICO is the UK's independent public authority set up to uphold information rights. The Information Commissioner does this by promoting good practice, ruling on complaints providing information to individuals and organisations and taking appropriate action where the law is broken.

The ICO enforces and oversees the Freedom of Information Act, the Environmental Information Regulations, the Data Protection Act and the Privacy and Electronic Communication Regulations.

Introduction

Thank you for the opportunity to take part in this important consultation. We agree that a discussion of internet regulation is an important and relevant one. In our response we aim to provide you with an insight into the ICO's role; what can and is already being done to protect individuals' online privacy.

In answering your specific questions we have primarily focused on matters that fall within our area of statutory responsibility, primarily as regulator for data protection law in the UK.

Specific questions

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

The ICO is the UK's regulator for data protection and as such has a key role in the regulation of the internet, when it relates to the processing of personal data online.

The Data Protection Act 1998 (DPA), soon to be replaced by the General Data Protection Regulation (GDPR) and the Data Protection Bill currently making its way through Parliament, all provide the Commissioner with a broad remit and powers to help protect personal data online. There is regulation of the internet in respect of data protection - GDPR strengthens the obligations and accountability of data controllers, enhances the rights of individuals and strengthens the powers of the Commissioner.

Because of the above, any proposed further regulation of the internet, would need to ensure it complements and not duplicates the functions that the Commissioner has.

The question of the desirability of regulating the internet is a complex one. One of the main aims of the internet at conception was the free, uninhibited exchange of information. There are important questions about the balance between further statutory regulation and what role self-regulation should have, involving softer measures such as codes practice. The Commissioner believes that both have a role to play, combined with other measures such as improved digital literacy.

There is growing consumer unease about how online platforms are using personal data and potentially limiting consumer choice. Research conducted by the Commissioner shows less than one in ten (8%)[1] of UK adults say they have a good understanding of how their personal data is made available to third parties and the public. Improving transparency is a key aim of the forthcoming GDPR.

The risks thrown up by the current internet ecosystem also go beyond compliance with data protection law and trigger wider ethical considerations and how this drives trust.

The activities of online platforms are therefore not entirely unregulated, but it is fair to say that some aspects of the law have not kept pace with the rapid development of the internet. In terms of data protection GDPR is an important step forward to catch up.

[1] http://www.comresglobal.com/polls/information-commissioners-office-trust-and-confidence-in-data/

Search engines are no longer simply that and social media organisations can no longer be described as purely host platforms. They filter news, micro-target advertising, and in most cases facilitate and generate content.

Where these activities use personal data it is important to be clear that data protection law applies and can provide effective protection for individuals. Recent case law, such as CJEU case of Google Spain, has made clear that online platforms such as search engines are data controllers under data protection law. They can be fully liable for their use of personal data. This has enabled individuals to exercise their rights, including a 'right to be forgotten' to request that personal data is removed from platforms. These rights are strengthened under the GDPR.

The Commissioner recognises that there is a role for regulation of internet content, beyond data protection, and the wider information fiduciary duties of the online platforms must be considered.

The global nature of the internet may raise territorial difficulties in terms of jurisdiction and the ability to enforce regulation. The GDPR will operate under the concept of the 'one stop shop' – creating a 'lead data protection authority' for organisations established in the EU and providing services across EU borders.

Where organisations are not established in the EU, territorial scope under the GDPR is still broad – any organisation directly providing online services to individuals in the EU will be covered. The challenge for the EU is to establish the enforcement mechanisms to make this work in practice outside the EU, which may require multi-lateral agreements.

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

Online platforms are no longer just platforms allowing individuals to access content. As mentioned above they also produce content, filter what individuals view and in some cases micro-target individuals with advertising. The Commissioner considers that, beyond compliance with data protection law, these organisations have a legal and an ethical duty to treat people's personal data appropriately.

These organisations have control over what happens with an individual's personal data and how it is used to filter content - they control what individuals see, the order in which they see it and the algorithms that are used to determine this. Online platforms can no longer say that they are merely a platform for content, they need to take responsibility for the provenance of the information that is provided to users. Looking beyond data protection, the Commissioner would propose exploring a range of solutions to make organisations more accountable for the content they produce, involving soft and hard measures, to enable the balance between responsibility and freedom of expression to be fully addressed. The ICO recognises that platforms are already taking responsibility for content, beyond data protection

law, such as removing extreme content and hate speech but more evidence is needed to understand how these new measures are working in practice.

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

The Commissioner has also published guidelines for search engines, explaining how to consider requests for links related to individuals to be removed from search results, which provides an example of how to balance competing rights in the context of internet regulation.[2]

There is a particular requirement under GDPR for online content to be appropriate to its audience, particularly where that audience is part of a vulnerable group, for example, children. Both the GDPR and the Data Protection Bill have specific requirements in relation to children. Article 8 GDPR provides additional protections in respect of the provision of information society services to children, including parental consent. Recital 38 GDPR makes clear that children merit further protection in relation to their personal data, in particular its use for '…the purposes of marketing or creating personality or user profiles…'. As the Data Protection Bill currently stands it also requires the Commissioner to produce a code of practice about age appropriate design relevant to online services. This responsibility will be unique in the EU, and important in setting standards for websites and services targeted at children. The UK has an opportunity to be a leader in this context.

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

The Commissioner is supportive of involving users in this process. The internet enables people to interact with each other and creates unprecedented numbers of relationships, often without meeting the people they connect with. Many disputes that emerge about online content can relate to information that individuals post about each other. Education and standards therefore play an important role beyond the law.

The process of undertaking data protection by design and data protection impact assessments, required under GDPR, should also place the user at the heart of any process involving use of personal data.

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

[2] https://ico.org.uk/for-organisations/search-result-delisting-criteria/

As discussed above, the Commissioner sees what online platforms do about online content and the use of personal data as a freedom of expression issue as well as a data protection one. It is important that online platforms ensure that individuals can clearly understand and control any profiling or filtering that can affect the types of information they see as part of personalised content. It is important in a democratic society that people are not left uninformed of varying views and opinions, to avoid echo chambers that can fuel divisions.

In conjunction with this, the concept of open data and open information is an important one. Being available to view and use information in a free and open manner is beneficial for society, democracy and business. An internet that is open and transparent ensures that people have a greater understanding of the key issues and challenges that different parts of society face and can lead to more informed debate between different groups.

What information should online platforms provide to users about the use of their personal data?

The GDPR has a clear focus on requiring organisations to be upfront and transparent about their use of individuals' personal data and to give individuals greater control over their personal data.

In particular, the GDPR includes the right to be informed (this is mainly covered by articles 13 and 14 of GDPR). The Commissioner has produced guidance[3] which discusses this in more detail. Essentially, the GDPR requires organisations to be clear about what they do with individuals' personal data, how they do it, on what basis they do it, what data they hold, how long they will hold it for and who they will share it with (this is not exhaustive). Beyond this, organisations are required to give any further information that is needed in order to make the processing of personal data fair.

Organisations should be giving individuals this information as soon as possible. A specific means of providing this information is in a privacy notice, which outlines all of the requirements of articles 13 and 14 in a clear and concise manner that is written in plain language and aimed at its intended audience. The Commissioner has produced detailed guidance[4] on the right to be informed, which provides advice and guidance on the best way of providing this information. The code also encourages organisations to be innovative in providing this information – embedding and layering the information as part of the design process, not just in one long notice.

The Commissioner considers that organisations should be as open and transparent as possible and view the opportunity to be transparent as not only

[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/
[4] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/

achieving compliance in a data protection sense but also as an opportunity to engender trust and improve relationships with their customers.

In what ways should online platforms be more transparent about their business practices—for example in their use of algorithms?

The Commissioner is currently undertaking an investigation into political campaigning and the use of personal data and data analytics online[5]. As this is an ongoing investigation the Commissioner cannot comment in detail, however, it is already clear that significant concerns exist about the transparency of micro targeting and political content. Our report will be published in June 2018. Enforcement actions taken against individuals or organisations will follow the publication of the report.

Online platforms must be transparent in the way they are using both their customers' data and other sources of personal data they combine it with. For example, under the 'partner category' system for Facebook advertising user data was combined with data from credit reference agencies to inform ad targeting. In the Commissioner's political targeting investigation, the Commissioner raised concerns about the lack of transparency in this program; in March 2018, Facebook announced it was discontinuing the partner category program.

The GDPR focuses heavily on the importance of transparency and accountability and increases the rights individuals have over how their data is to be used. The GDPR gives people the right to object to organisations using their personal data, the right be forgotten (the right to erasure of personal data) and the ability to challenge decisions made by machines and algorithms. It also requires the use of tools such as data protection impact assessments and data protection by design and default to address risks to privacy.

The issue of the use of algorithms and more generally, automated processing of personal data, is a key area where organisations must be clear with individuals about their use and the purpose of their use. Article 22 GDPR provides rules around the processing of personal data by automated decision making (including profiling of individuals). It requires that solely automated decisions should not be made, where it produces legal effects or similarly significant effects. Furthermore, such personal data processing can only take place where it is in relation to the performance of a contract, is allowed by EU or member state law or is based on explicit consent.

Beyond this, the right to be informed includes the right to be told of such processing and to receive meaningful information about the logic involved in the decision making as well as the significance and envisaged consequences of such processing. Organisations who process personal data by means of

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-statement-investigation-into-data-analytics-for-political-purposes/

algorithms without human intervention must be aware of this requirement and comply with it.

The Commissioner is working with the Turing Institute on guidance about the explainability of algorithms, to be published later this year. This is a challenging topic – technical information will not engage the average user. Transparency measures must explain data inputs, how outputs will be used and what the implications are. Innovation will be needed to do this clearly and engage users. Informing the users at a non-technical level must be paired with a deeper requirement to explain and account to the regulator. Under the new Data Protection Bill the Commissioner will have stronger powers to undertake inspections of online systems to examine how algorithms work in practice and act on behalf of the user.

The Commissioner provided detailed submissions[6] to the House of Commons Science and Technology Committee inquiry into algorithms in decision-making in April 2017.

However, as well as transparency and strongly linked to it, the Commissioner would encourage organisations to give individuals greater control over what happens to their personal data, without the need to formally exercise their rights. Control can be provided in the form of dashboards and other online tools within mobile applications.

What is the impact of the dominance of a small number of online platforms in certain online markets?

The Commissioner is concerned about the pervasiveness of big data analytics and micro targeting and the impact on the democratic process in particular. A small number of online platforms increasingly play an important role in how the public receive news and information, plus engage with online content during elections and campaigns. The platforms therefore have a key responsibility to ensure an effective balance between freedom of expression and other competing rights, including data protection.

A small number of online platforms dominate the market and have broad and deep collections of personal data that they can use to profile and target individuals. These concerns are magnified by mergers and acquisitions where personal data is the primary asset. The Commissioner recently took action over proposed data sharing between WhatsApp and Facebook, following WhatsApp's acquisition by Facebook. The Commissioner found the proposed data sharing between the two companies failed to comply with transparency and consent rules under the Data Protection Act. As a result of the Commissioner's investigation, WhatsApp signed an undertaking not to share personal data until these issues are addressed[7].

[6] https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2013970/ico-response-house-of-commons-science-tech-algorithms-20170410.pdf
[7] https://iconewsblog.org.uk/2018/03/14/whatsapp-signs-public-commitment/

What effect will the United Kingdom leaving the European Union have on the regulation of the internet?

The Commissioner has set out her views to Parliament in a number of submissions previously[8] – she most recently gave evidence to the Exiting the EU Select Committee on 9 May[9].

Leaving the EU could have a significant impact on regulation of the internet. Firstly, when the UK leaves the EU and becomes a third country it will no longer benefit from the legal certainty that EU member states enjoy under data protection law. This allows data to flow freely between member states and no legal assessment is required before data is transferred. As a third country the UK will need to demonstrate how its data protection regime is essentially equivalent to EU law, to enable it to gain a statement of 'EU adequacy'. This would then allow personal data to continue to flow without restriction. Without an adequacy decision organisations in the UK who want to receive personal data from the EU would need to rely on more burdensome measures such as standard contractual clauses and binding corporate rules.

Whilst this would enable data flows between the EU and the UK the Commissioner supports the Government's ambition for a bespoke agreement with the EU on data protection – this would include adequacy and also enable the Commissioner to participate in the one stop shop system within the EU. Participating in this mechanism would allow UK businesses operating online to work with a single regulator and the public could complain to the Commissioner about online services provided by EU based companies.

The Commissioner would also lose significant influence over the direction of decision making on key data protection cases if it is unable to take part in the European Data Protection Board, the EU group of data protection authorities under the GDPR. The board can take binding decisions and there is a risk of losing influence in precedent setting cases involving online platforms under the GDPR, on areas such as profiling and the right to be forgotten. A bespoke agreement should also aim for the Commissioner to retain her position on the Board.

In August 2017 the Government set out its position on the future data protection relationship with the EU. The Commissioner supports the partnership paper and is working closely with the Government to provide expert advice on the practicalities of any new partnership.

---

[8] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.html

[9] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/exiting-the-european-union-committee/the-progress-of-the-uks-negotiations-on-eu-withdrawal/oral/82783.html

House of Lords Select Committee on Communications inquiry – The Internet: To Regulate or Not to Regulate

For further information on this submission, please contact Richard Sisson on 03304 146 346 or email richard.sisson@ico.org.uk

If you would like to contact us please call 0303 123 1113.

www.ico.gov.uk

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF

Information Commissioner's Office