Response of the Information Commissioner's Office to the DCMS call for views on app security and privacy interventions

About the Information Commissioner's Office

The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Privacy and Electronic Regulations 2003 (PECR), the Network and Information Systems Regulations 2018 (NIS) and the Environmental Information Regulations 2004 (EIR).

The ICO is independent from government and upholds information rights in the public interest, promoting transparency and openness by public bodies and organisations and data privacy for individuals. It does this by providing guidance to individuals and organisations, solving problems where it can, and taking appropriate action where the law is broken.

Introduction

The ICO welcomes the opportunity to respond to the government's call for views on app security and privacy interventions. Addressing inconsistencies within the app ecosystem and raising standards of security and privacy are shared aims of government and the ICO. We therefore stand ready to work with government to assess opportunities for interventions that will deliver clear benefits for the public and industry.

Data protection law plays a critical role in addressing many of the concerns highlighted in the call for views; app developers and app store providers have existing responsibilities under data protection legislation (including the UK GDPR and DPA18) to ensure that they are creating and distributing apps with appropriate levels of security and privacy. While the call for views does, to an extent, recognise these requirements, the role the ICO plays in ensuring high standards of security and privacy across the app ecosystem should be given greater attention as proposals for potential interventions are developed.

As the government's work in this area progresses, it should undertake further analysis of the role that the ICO's regulatory regime plays in addressing harms arising within the app ecosystem and ensure that interventions are only pursued where regulatory gaps are clearly identified, or where evidence demonstrates that an increased level of regulatory or government oversight is necessary. The government should avoid creating unnecessary regulatory overlap where existing bodies, including the ICO, already have sufficient powers at their disposal to address concerns highlighted in the call for views. Any unnecessary regulatory overlap would be unhelpful, and lead to complexity and uncertainty for the public, industry and regulators.

In seeking to tackle the specific challenges the government has identified in relation to transparency and security within the app ecosystem, close cooperation with the ICO and other Digital Regulation Co-operation Forum (DRCF) regulators will be required to ensure alignment and consistency across regimes and delivery of coherent outcomes. Notably, the CMA's Digital Markets Unit (DMU) could potentially have powers to implement codes for app stores, and government should therefore clearly map out the roles that regulators will have to play as it further assesses the value, necessity, and practicality of potential interventions. The ICO benefits from a close and effective relationship with the DRCF and its members, and the government should make full use of this collaborative arrangement as it establishes the role that existing regulators have to play in this space.

The ICO's role in regulating apps and app stores

As noted above, the ICO plays a critical role in ensuring the privacy and security of apps and app stores via our oversight and enforcement of data protection law, including the UK GDPR and DPA18. The roles of app developers and app store providers under data protection law can be complicated, particularly in terms of identifying their respective responsibilities as data controllers or data processors, but we recognise that app stores act as critical interfaces between users and developers within the app ecosystem, potentially providing efficient opportunities to drive up privacy and security standards.

Regardless of the roles of developers and app store providers, all processing of personal data within the app ecosystem must take place in compliance with the rules and principles set out in data protection law. Below, we set out elements of the laws overseen by the ICO that play a critical role in mitigating harms associated with apps and app stores. Failure to comply with the principles may leave developers and app store providers open to substantial fines. For example, infringements of the UK GDPR principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to £17.5 million, or 4% of the total worldwide annual turnover, whichever is higher.

Security of processing

Given the security focus of the call for views, it is essential that government takes the existing security requirements of data protection law into account when determining the extent to which interventions are required within the app ecosystem.

Article 5(1)(f) of the UK GDPR concerns the integrity and confidentiality of personal data and requires that processing of personal data takes place in a manner that ensures security of information. Apps and app stores are required to have appropriate security in place to prevent personal data being accidentally or deliberately compromised.

While information security is sometimes linked solely to cybersecurity (i.e. the protection of networks and information systems from attack), it also covers physical and organisational security measures. Article 32(1) of the UK GDPR requires that, when identifying appropriate measures, apps and app stores take into account the state of the art, the costs of implementation and the nature,

scope, context, and purposes of processing, as well as risks to the rights and freedoms of individuals. For example, app developers may decide to implement encryption and or pseudonymisation to reduce security risks associated with personal data.

In the event of a physical or technical incident, developers and app stores should also ensure the ability to restore availability and access to personal data in a timely manner. There should also be processes in place for regular testing, in order to assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of processing.

Poor information security can cause harm and distress to individuals. Some examples of the harm caused by the loss or abuse of personal data within the app ecosystem may include identity fraud, fake credit card transactions, fake applications for tax credits, and mortgage fraud. The risk of harm could be heightened depending on the nature of an app and the type of personal data processed. For example, security breaches that involve banking apps are likely to involve sensitive financial data that could increase the risk of fraud.

Information security can also support good data governance and help app stores and app developers to demonstrate compliance with other aspects of the UK GDPR. The ICO is also required to consider the technical and organisational measures in place when considering an administrative fine.

Network and Information Systems Regulations 2018

The ICO is the competent authority for Relevant Digital Service Providers (RDSPs) under NIS, meaning that we have a range of powers that we can use to enforce the regulation, including issuing fines of up to £17 million in the most serious cases. RDSPs are organisations providing digital services such as online marketplaces, online search engines, and cloud services. Online app stores are RDSPs, provided they are not subject to SME exemption, and therefore have obligations under the NIS Regulations.

NIS is intended to establish a common level of security for network and information systems. These systems play a vital role in the economy and wider society, and NIS aims to address the threats posed to them from a range of areas, most notably cyber-attacks. Although NIS primarily concerns cybersecurity measures, it also covers physical and environmental factors. NIS requires these systems to have sufficient security to prevent any action that compromises either the data they store, or any related services they provide.

Transparency

The transparency provisions of the UK GDPR play a critical role in mitigating the risk of potential individual harm presented in the app ecosystem, such as a loss of control of personal data, a lack of autonomy, manipulation, influence, and fraud. The provisions require organisations that process personal data, including app developers and app store providers, to provide users with clear information about the personal data that is collected, what they do with the data they

collect, who it is shared with, and how individuals can exercise their data protection rights in relation to their personal data.

Initiatives such as Apple's privacy labels and Google's safety labels, the introduction of which has been prompted by data protection law requirements, can provide key information to users to improve transparency and help users to understand the privacy and security practices of apps before they download them. Increased user information about how personal data is processed and steps to prevent and control cross-web and app tracking (such as Apple's App Tracking Transparency feature) are also likely to increase user understanding and transparency. They can also enhance user control over personal data by enabling informed decisions.

While the requirements of data protection law are pushing up transparency standards across the ecosystem, the information provided about app privacy and security and the language used by app developers and app store providers can often be inconsistent, potentially causing confusion for users. With this in mind, we support government's intention to improve standards and consistency but, again, stress the need for the ICO's role to be recognised and leveraged as part of efforts to enhance transparency from both a privacy and broader consumer protection perspective.

Lawfulness and fairness

The UK GDPR provisions on lawfulness and fairness require that the processing of personal data takes place in ways that comply with the law (not limited to data protection law) and in ways that users would reasonably expect. Individuals should not be misled about processing and app developers and app stores should consider the effects their processing may have on individuals and justify any adverse impact.

Fairness is intrinsically linked to transparency around personal data collection in the app ecosystem; the processing that takes place should match the information provided to users when they decide to install an app. Where processing is not fully explained to users, or would not be expected by them, it will fail to meet the requirements of the first data protection principle.

Organisations must anticipate and justify any adverse effect that their processing has on individuals. The fairness principle therefore provides an existing requirement for apps and app stores to anticipate and mitigate any harms that might arise from their processing of personal data.

Data minimisation

The data minimisation principle requires that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Apps and app stores must therefore not process more personal data than is necessary, the data must be kept up to date, and it should not be retained for longer than required.

App developers must only request permission to obtain personal data or access device features when it is necessary to allow the functioning of the app and this should be made clear to the user in line with the transparency requirements of UK GDPR.

Data protection by design

Article 25 of the UK GDPR requires app developers and app store providers to put in place appropriate technical and organisational measures to implement data protection principles effectively and safeguard individual rights. This means that developers and app store providers must integrate data protection into their processing activities and business practices by design and by default.

Adopting a data protection by design approach can help developers and app stores to ensure that they comply with the UK GDPR's fundamental principles and requirements, and forms a key part of demonstrating overall accountability for compliance with data protection law.

Accountability

The UK GDPR accountability principle holds organisations responsible for complying with the law, and requires that they are able to demonstrate their compliance.[1] The principle introduces an obligation on organisations, including app developers and app store providers, to take appropriate action to achieve compliance, maintain records about how they process personal data, and be able to provide information to individuals about how their data is processed.

If developers or app stores process personal data that is likely to result in a high risk to individuals, a Data Protection Impact Assessment (DPIA) should be carried out prior to any processing to demonstrate accountability. For example, the processing of children's data is considered as high risk processing.

DPIAs provide a framework for identifying risks and mitigation measures, which might include different or additional security features. The accountability principle therefore plays a crucial role in providing additional transparency and security around the processing of personal data within the app ecosystem.

Children's data

The Children's Code (formally, the Age Appropriate Design Code)[2] is a statutory code of practice prepared under section 123 of the DPA 2018, that protects children within the digital world by ensuring that online services are designed with them in mind.

Online services likely to be accessed by children, including apps and app stores, should ensure that the processing of children's personal data is compliant with the UK GDPR, and that the best interests of the child are considered. The Code is intended to ensure that a child-centric approach is built into the design of online

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/#documentation

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

services from the ground up. The ICO's Children's Code Design Guidance[3] illustrates how to apply some of the standards in practice, in order to create an open, transparent and safe place for children online.

Compliance with the Children's Code means that the best interests of the child must be a primary consideration when collecting and processing children's personal data. As such, compliance with the code will limit collection, profiling, and targeting using children's personal data. Services must avoid detrimental use of data and turn profiling and geolocation off by-default, unless they can demonstrate a compelling reason otherwise.

The code also provides autonomy to children. If apps and app stores provide parental controls, they should give the child age appropriate information about this and if parents or carers are able to monitor their child's online activity or track their location, app developers must also provide an obvious sign to the child to notify them when they are being monitored.

Apps must also avoid nudge techniques that lead or encourage children to provide unnecessary personal data or turn off privacy protections and transparency information must also be provided to children in clear language that is suited to the age of the child.

ICO feedback on the call for views proposals

Proposed voluntary code of practice

Noting the issues highlighted by the call for views, such as the need for baseline security and privacy requirements and consistency of information provided to users and developers across the app ecosystem, the ICO broadly supports the concept of a voluntary code of practice for app store operators and developers that sets out baseline security and privacy expectations. However, as noted earlier in our response, before determining whether to pursue this proposal, government should clearly map out the respective roles of relevant regulators in improving practices across the ecosystem and set out:

1. Whether the code is designed to fill regulatory gaps or reinforce existing regulatory requirements;
2. How or if regulators will be expected to take the code into account, where it interacts with their remits;
3. How or if government expects regulators to collaboratively monitor or assess levels of adherence to the code, noting the cross-cutting nature of the draft principles; and
4. How app developers and app store providers might be expected to demonstrate their adherence with the code to regulators.

A successfully implemented code of practice, applicable to all types of app stores, could help protect more users across different devices by raising current

[3] The Children's code design guidance | ICO

standards of best practice in app security and privacy. A code could also help to proactively prepare the UK market for potential changes to the mobile ecosystem and provide a potential route for mandating minimum requirements should the ecosystem change. However, it is critical that relevant regulators are engaged from the outset and that their respective roles in relation to the code are identified and communicated clearly. Any code of practice must also account for both the impending data protection legislative reform and potential change to ICO's duties under the NIS Regulation.

Code of practice principles

The ICO is broadly supportive of the principles in the draft code of practice. While app developers and app stores are already required to adhere to the security and privacy requirements set out in data protection law, the reinforcement of these requirements through a set of app ecosystem-specific principles has the potential to improve consistency of approach across app stores and apps.

However, as stated earlier in our response, we would welcome clarity on government's proposals for practical introduction of such a code and how it views the role of the ICO in relation to the code, particularly as multiple elements interact firmly with our remit. To serve as a guide for future discussions with government on the role of the ICO, we have provided examples of areas of potential interaction between some of the proposed code principles and existing data protection law below:

1. **Implementing vulnerability disclosure processes**

- The proposed requirement to implement vulnerability disclosure processes overlaps with the UK GDPR security principle (Article 5(1)(f)) which provides that personal data should be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Article 32(1) of the UK GDPR also requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security that is appropriate to the risks arising from processing.

2. **Keep apps updated to protect users**

- In accordance with the security principles of UK GDPR, apps should be updated in order to prevent security breaches and manage security risks.
- The data protection by design and default requirement under Article 25 of the UK GDPR requires developers and app store providers to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.
- Data must also be processed lawfully and fairly in ways that users would reasonably expect. It is therefore reasonable for a user to assume that apps will be kept updated. App developers and app stores should also consider the effect their processing may have on individuals and justify any adverse impact.

- The accountability principle also holds organisations responsible for complying with the law, and requires that they are able to demonstrate their compliance. DPIAs provide a framework for identifying risks and mitigating measures, which might include different or additional security features. The accountability principle therefore plays a crucial role in providing additional transparency around the processing of personal data within the app ecosystem and helps to increase transparency.

3. **Provide important security and privacy information to users in an accessible way**

- The provision of important security and privacy information to users can be linked to the transparency requirements of the UK GDPR.
- Articles 13 and 14 of UK GPDR set out a minimum level of information that must be provided to individuals in circumstances where data is collected directly and indirectly from them.
- While security information is not specifically covered by Articles 13 and 14, provision of additional information in this area is consistent with transparency element of Article 5(1)(a).

4. **Ensure only legitimate apps that meet security and privacy best practice are allowed on the app store**

- This principle potentially creates scope for app stores, in becoming 'trusted digital marketplaces,' to set baseline security and privacy standards that go above and beyond the minimum requirements of data protection law.
- While we are supportive of measures that seek to improve best practice, there is clear overlap with the ICO's remit and we would welcome clarity from government on the role it sees us playing in this area. If this principle is implemented, safeguards may also need to be considered that would prevent app stores abusing their position by self-preferencing their own apps over third party apps.

Trusted service providers

We note the suggestion that adherence to a code of practice could provide an opportunity for developers and app store operators to demonstrate improvements to their baseline privacy and security practices and for app stores to act as 'trusted digital marketplaces' ensuring minimum standards are adhered to.

While we agree that app stores could serve as trusted service providers with stronger vetting processes to check that apps are not a risk to users' security and privacy (again noting their position as a key interface between users and app developers), government will need to ensure that pro-privacy interventions do not inadvertently lead to negative competition outcomes.

Government should also recognise that, if app stores are given further responsibility to take steps to ensure developers are adhering to the requirements of a code of practice and, there are likely to be cost and resource

implications, which potentially could discourage some app stores from signing up to the code. Noting this challenge, and the potential privacy-competition interface highlighted above, we are keen to work with government and the CMA to explore possible options for leveraging the influential position of app stores to help drive up levels of transparency and security.

5. Further considerations

Beyond further analysis of the proposals put forward in the call for views, we recommend that government works with the ICO and other regulators to explore potential for improving best practice standards in transparency across the app ecosystem in the following areas:

1. Language, and privacy and security iconography

In acting as 'trusted digital market places' app stores could drive further consistency and user transparency through the use of common privacy and security language and standard cross-industry iconography. Fostering a consistent approach to language and iconography could aid user understanding of common privacy and security terms and practices, which in turn is likely to increase user control and empowerment.

2. Age ratings and information

App age ratings presented in app stores are often based primarily or solely on content considerations, rather than factors such as data processing risks. The ICO has observed that there can be a disconnect between the minimum age stated in an app's terms of service and the age rating presented at app store level. This raises concerns around inaccurate signals being sent to users about the non-content-related risks associated with apps.

The ICO is keen to see standards of transparency improved in order to provide greater clarity around the basis on which app store level ratings are set and give increased prominence to information contained within terms of service. However, we recognise that data processing risks are not the only consideration in seeking to address this challenge, and we therefore stand ready to work with government and our regulatory partners to address these inconsistencies within the app ecosystem.

Conclusion

The ICO is committed to working alongside the government as it strives to improve levels of security and privacy across the app ecosystem. While we are broadly supportive of the government's work in this area, our response has highlighted clear challenges that will need to be addressed, particularly in relation to identifying the roles of existing regulators and avoiding areas of unnecessary regulatory overlap.

We look forward to engaging further on the issues highlighted in our response and any other areas where the ICO's experience and expertise would assist the government.