App security and privacy interventions - BCS Response

June 2022

BCS
The Chartered Institute for IT
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY
BCS is a registered charity: No 292786

Table of Contents

This document

This is the BCS response to the DCMS consultation[1] on 'App security and privacy interventions'.

1 BCS response on App security and privacy interventions

BCS welcomes the government's proposal to introduce a Code of Practice for all App store operators and developers. Our main comments are:

- The proposed Code of Practice is a good place to start, but is unlikely to bring sufficient change while it is voluntary
- The Code of Practice should be aligned with Codes of Conduct from professional bodies that provide professional registers where they are relevant to App stores and App developers
- The Code of Practice needs to be conducive to UK and international governments efforts to develop a thriving ecosystem for effective auditing of artificial intelligence systems[2], which is intended to galvanise responsible innovation
- Consideration needs to be given to potential tensions between the commercial imperatives of App store owners and public policy priorities, which may be exacerbated by a Code of Practice that fails to adequately recognise such possibilities (see Section 3)
- Vulnerabilities in software supply chains is a key area of concern, which is unlikely to be solely addressed by a Code of Practice (see Section 4)

A key outcome of the Code of Practice is ensuring Apps are effectively reviewed in a consistent way by different App stores. For any algorithmic system (App or otherwise) to be reviewable it needs to be

- standards compliant to enable effective use of state of the art analysis/auditing tools and techniques, and
- auditable data about the algorithm needs to be generated in a standardised way that can be readily assimilated by reviewers (and future regulators)

[1] https://www.gov.uk/government/consultations/app-security-and-privacy-interventions

[2] https://cdei.blog.gov.uk/2021/04/15/the-need-for-effective-ai-assurance/

These points need to supported by a Code of Practice, particularly if it is to be mandated through regulation at a later stage.

2 Further comments on the principles underpinning the Code of Practice

This section includes more detailed comments on the principles that underpin the proposed Code of Practice included in the consultation.

Principle: Seek to ensure that only legitimate apps that meet security and privacy best practice are allowed on the App store.

For this principle to be enforceable it is important that security and privacy best practice needs are properly defined. Security best practice should be aligned with one or more established security frameworks (e.g. Cyber Essentials, ISO27001, NIST CSF, OWASP). Privacy best practice should be aligned to ICO guidance on privacy by design and default as well as UK GDPR. It is also essential that widely recognised code testing standards should be enforced when setting benchmarks for allowing apps into the App stores.

Principle: Implement vulnerability disclosure processes.

The Code of Practice should make it clear that an App will include a simple, easy to use option for consumers to report bugs and vulnerabilities to the App store and to App developers. App stores should monitor such reports and be prepared to remove Apps with critical vulnerabilities. This will also greatly strengthen the Code of Practice principle that developers must keep Apps updated to protect users.

Principle: Provide important security and privacy information to users in an accessible way.

The Code of Practice needs to make it clear it is essential that methods for provision of security and privacy information to users are implemented so that they are as consistent as possible across different Apps and across different App stores. Further, a public education campaign is advised to ensure that the general public are supported to engage with these policies.

Principle: Promote security and privacy best practice to developers

In identifying and promoting best practice the Code of Practice needs to be aligned with existing globally recognised skills standards on information technology, such as for example SFIA. SFIA[3] is a global employer led skills frameworks for information technology which, for example, has been adopted in Australia, New Zealand, Canada, Japan, and Saudi Arabia, etc. It is also licenced by global standards bodies, such as for example the IEEE. SFIA is used by BCS and other professional bodies around the world (such as the Australian Computer Society) to underpin standards for professional registration.

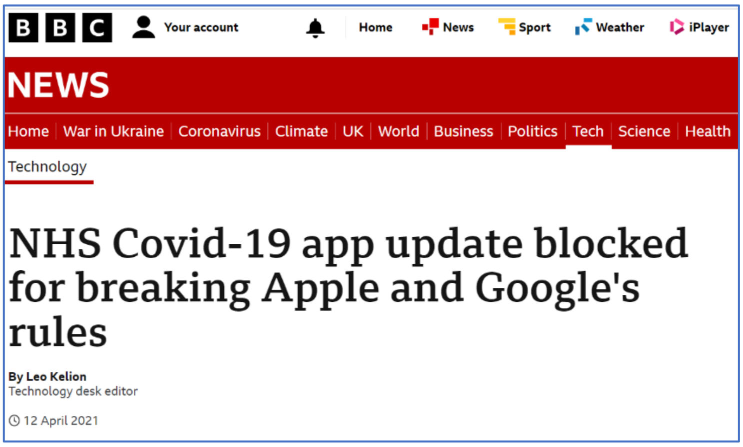
[3] https://sfia-online.org/en

3 Tensions between commercial and public policy priorities

Currently App stores unilaterally mandate that Apps provided through the App store must comply with all App store policies, whether these cover privacy, security, or purely commercial requirements. A review processes will supposedly check those policies are fully adhered to and if they are not an App will be rejected. A future Code of Practice might endorse this approach as good practice.

- An unintended consequence of a Code of Practice would be facilitating an App store to unilaterally impose a policy developed by a corporate entity that contradicts a pubic policy objective developed through a democratic political processes.

The initial version of the NHS Covid-19 App highlights where this kind of contradiction between corporate concerns and public policy concerns can happen. Public Health England initially asked for the NHS Covid-19 App to allow users to report their location through the App to improve the App's track and trace capabilities. Both the Google and Apple App stores stated this was a breach of their privacy policies and did not allow the NHS App update on their stores[4]. This is an example of a conflict between consumer privacy requirements, as defined by a corporate entity, and public health requirements, as defined by a national public health authority mandated through a democratic political process.



NHS Covid-19 app update blocked for breaking Apple and Google's rules

By Leo Kelion
Technology desk editor

12 April 2021

Figure 1: example of conflict of interest as reported by BBC

BCS has no position on whether Google and Apple should or should not have acted unilaterally in that way or whether Public Health England should or should not have asked for such a requirement. What is of note for this consultation is that the technology companies were able to unilaterally block the NHS App without the NHS, UK policy makers, or the general public in the UK having a say in the matter.

This highlights a possible unintended consequence where a Code of Practice makes it easier for commercial App stores to unilaterally mandate privacy or security policies of their choosing, without regard for whether they are consistent with public policy requirements. That might mean in future some public policy objectives can not be delivered through Apps

[4] https://www.bbc.co.uk/news/technology-56713017

deployed on major App stores, because they are deemed to be in contravention of corporate defined App store policies.

We recommend an in depth evaluation of mechanisms to determine when there may be possible overlaps and inconsistencies between App store privacy and security policies and possible public policy objectives. Further consideration should be given to how these mechanisms can then be referenced within a Code of Practice.

4 Software supply chain vulnerabilities

Our expert professional membership raised the issue of dealing with software supply chain vulnerabilities as of particular concern.

It is very common for an App to provide additional functionality by API calls to third party software located outside of the App store ecosystem, whether that be the Apple, Google, Microsoft, Robox, or some other App store. This means the App relies on a software supply chain where the actors in that chain may be located anywhere and where updates/patches and bug fixes are constantly being applied to the third party software after the App has been downloaded.

It is not clear what checks or what requirements App stores place on App developers to verify and audit the security of their software dependencies through third parties. This is a serious issue that needs further consideration, because malware threats in the wider third party software ecosystem may not be so well regulated or detected as they are on App stores.

Requiring reviewing of the software supply chain will have significant implications for App developer communities and likely to add to development and maintenance overheads. Highly popular and benign Apps can be developed by individuals doing it as a hobby. Are hobbyists going to be in a position to ‘audit’ their supply chain? Similarly, are charities or other third sector organisations going to have sufficient capabilities to audit their software supply chains? It seems highly unlikely.

Given the financial resources of major App stores it seems reasonable they take responsibility for verification and assurance of the extended ‘deep services’ on which their App developers depend. As part of being responsible technology stewards App stores should be transparent and open about their ‘deep services’ verification and assurance capabilities and capacity, which they provide on behalf of every participant on their platform, whether an App developer or App user.

Who we are

BCS is the UK’s Chartered Institute for Information Technology. The purpose of BCS as defined by its Royal Charter is to promote and advance the education and practice of computing for the benefit of the public.

We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 60,000 members including practitioners, businesses, academics and students, in the UK and internationally.

We also accredit the computing degree courses in over ninety universities around the UK. As a leading information technology qualification body, we offer a range of widely recognised professional and end-user qualifications.