Bar Council response to the public consultation on the safety of apps and other non-embedded software

1. This is the response of the General Council of the Bar of England and Wales (the Bar Council) to the European Commission – Digital Single Market's consultation paper entitled "Public consultation on the safety of apps and other non-embedded software not covered by sector-specific legislation – such as medical devices or radio equipment".[1]

2. The Bar Council represents over 15,000 barristers in England and Wales. It promotes the Bar's high quality specialist advocacy and advisory services; fair access to justice for all; the highest standards of ethics, equality and diversity across the profession; and the development of business opportunities for barristers at home and abroad.

3. A strong and independent Bar exists to serve the public and is crucial to the administration of justice. As specialist, independent advocates, barristers enable people to uphold their legal rights and duties, often acting on behalf of the most vulnerable members of society. The Bar makes a vital contribution to the efficient operation of criminal and civil courts. It provides a pool of talented men and women from increasingly diverse backgrounds from which a significant proportion of the judiciary is drawn, on whose independence the Rule of Law and our democratic way of life depend. The Bar Council is the Approved Regulator for the Bar of England and Wales. It discharges its regulatory functions through the independent Bar Standards Board.

3.1 For individuals or representatives of a public authority / organisation / business.

Question 1: What type of apps or other non-embedded software pose safety risks? Please give examples.

4. As the market matures, app developers are looking to distinguish themselves with data-rich features that allow for a deeper, more personalised user experience. Apps which use deep personal information particularly in categories such as:

(a) Health & Fitness
(b) Lifestyle
(c) Finance
(d) Business

[1] European Commission – Digital Single Market (2016) Public consultation on the safety of apps and other non-embedded software. Available here: https://ec.europa.eu/digital-single-market/en/news/public-consultation-safety-apps-and-other-non-embedded-software

are likely to pose greater safety risks.

5. Examples of how and why app developers are seeking to use personal data include:

(a) App usage data—the ability to know where users look, for how long, and where they go next is crucial in increasing value-add in an app, decreasing clutter and increasing performance. Then there is the further use of health apps which collects users' personal health information such as age, weight, blood pressure, sleep patterns, exercise performance, etc.

(b) Geo-location—using a smartphone's built-in geo-location hardware is helpful in many apps, from finding the nearest supermarket to allowing the user to see how fast they have run or the distance travelled. The location data that this produces can constitute personal data, and so data protection rules must be followed in relation to such use and retention.

(c) In-app purchases—the rise of 'freemium' content, where the basic app is free but extra content must be purchased, is continuing to accelerate. Such business models may lead to a developer handling payment information for its users, which leads to a whole host of compliance requirements, including in the data protection field.

(d) Commercialisation of data lists—where a developer decides to take on lists of personal data, such as login details, personal preferences and others, it may decide to make money from that data itself, for example by selling customer lists. This can be very fruitful, but must be done in compliance with relevant laws.

Further to the above, there has to be strong security of data which is stored in order to protect the user's financial loss and liability.

Question 2. What risks can apps or other non-embedded software pose?

- ☑ **Economic damage**
- ☑ **Physical damage to individuals**
- ☑ **Physical damage to property**
- ☑ **Non-material damage (pain and suffering)**
- ☑ **Other**

Please explain.

6. Security and privacy concerns are prime concerns and apply to app developers including strict rules relating to how data is collected (e.g. via cookies), how consent is obtained and how the data is onwardly processed; however app developers may be ignorant as to the likely breaches.

7. Given this complex web of legislation in data protection and privacy, it is no surprise that, in 2014, Global Privacy Enforcement Network found that 85% of 1,211 mobile apps

reviewed were non-compliant with data protection laws[2]. This will be of concern for app developers as the regulatory system tightens and the consequences of non-compliance become more serious.

8. The Article 29 Working Party has identified the lack of transparency and awareness of the types of processing an app may undertake, and a lack of meaningful consent from end-users before processing takes place, as the main risks for end-users of apps[3].

9. The main risks include security, breach of data protection and privacy laws, and/or unclear methods to obtain consent from the user.

Question 3: Please give your opinion on the following options:

	No risk	**Low risk**	**High risk**	**Very high risk**
***Economic damage**	○	○	○	◉
***Physical damage to individuals**	○	◉	○	○
***Physical damage to property**	○	○	◉	○
***Non-material damage (pain and suffering)**	○	○	○	◉
***Other**	○	○	○	◉

Please explain.

10. As well as the above, reputational damage is a very high risk.

3.2 For representatives of a public authority / organisation / business.

Question 4: In your professional experience have you already identified unsafe apps or other non-embedded software or have consumers approached you because they encountered problems with unsafe apps or other non-embedded software?

[2] Information Commissioner's Office Website: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/09/global-survey-finds-85-of-mobile-apps-fail-to-provide-basic-privacy-information/

[3] Article 29 Data Protection Working Party: Opinion 03/2013 on apps on smart devices: the lack of transparency and awareness

- (●) **Yes**
- ( ) **No**

Please specify:

11. Barristers who practice in this field are regularly approached by consumers on these issues. As stated the main risks identified are:

(a) Security concerns and storage (including use through the application programming interfaces (APIs)),

(b) Lack of transparency and awareness of the types of processing an app may undertake, and

(c) A lack of meaningful consent from end-users before processing takes place.

12. Key issues to be considered before data is processed include:

(a) Consent

i. Was there a valid meaningful consent for use and for the purposes given?

ii. Plain understandable language must be used at the time consent is captured, to explain what data is to be collected, how it will be processed, and by whom.

(b) Privacy Policy

i. Is the privacy policy clear, transparent and up-to-date? It should cover all current uses of data. If a new function is added to the app, and that function involves processing of personal data, the policy should be updated.

ii. Is key information easily read on a device? Bearing in mind the different screen sizes and resolutions available on different devices such as phones, tablets and smart watches.

(c) Cookies

i. Is the notification clear, both in terms of the language it uses and its visibility on-screen?

ii. Is the cookie policy easily accessible? Consider placing it along with the web terms and conditions at the bottom of every page template.

(d) Security

i. Are passwords used appropriately before data can be accessed? This relates to the user-facing level (appropriate logon security, for example,

with mobile wallets or online banking) and back-end security for the servers on which personal data is stored

ii. Are appropriate encryption methods used when data is in transit?

iii. Is data stored securely?

Question 4.1: If yes: What did you do to solve these problems?

13. Clients are provided with advice and representation before the Courts whose role it is to ensure enforcement of legislation and determine rights.

Question 5: Are existing EU or national safety rules and market surveillance mechanisms sufficient to monitor and withdraw, where necessary, unsafe apps or non-embedded software from the market?

- (●) **Yes**
- ( ) **No**

***Please explain:**

14. Key changes arising from the GDPR which would affect app developers include:

(a) Increased fines of up to 4% of a company's annual global turnover or up to €20m for non-compliance,

(b) Privacy by design—requiring developers and others to conduct regular audits of their processing strategy and to implement a strategy that suits their business (not just, for example, implementing a precedent privacy policy from the internet),

(c) Data protection officers, responsible for data protection compliance within the company and interaction with the regulators. Those working in the public sector as well as private sector organisations engaged in 'large scale', regular systematic monitoring will be required to appoint a data protection officer. This may present companies with a new cost initially but, in the long run, may save on large non-compliance fines through ensuring that the company operates in accordance with the rules throughout its operations, and

(d) Extra territorial reach—the GDPR is set to have a wide span, too as it catches not only data processing 'in the context of the activities of a controller or processor in the EU', but also to non-EU entities targeting, or monitoring the behaviour of, EU data subjects.

Question 6: Have you been held accountable for damage caused to consumers because of unsafe apps or other non-embedded software?

- ( ) **Yes, as manufacturer of the device the software runs on or controls**

- ○ **Yes, as an app or software manufacturer/developer**
- ○ **Yes, as an intermediary/distributor (e.g. app store)**
- ○ **Yes, other**
- ◉ **No**

Question 6.1: If yes: What did you do?

15. Not Applicable

Question 7: Do you think that existing horizontal and sector-specific EU legislation (e.g. General Product Safety Directive, Market Surveillance Regulation, Medical Device Directive, Radio Equipment Directive) taken together sufficiently cover the safety of all types of apps or other non-embedded software available on the market?

- ◉ **Yes**
- ○ **No**

Please explain:

16. Provided there is sufficient will and resources to enable enforcement by authorities tasked with providing enforcement, the legislation exists.

Question 8: Have you considered opening up an Application Programming Interface (API) of a device you manufactured or a service you provide to app and software developers to link their app to your device/service and use its functionalities? If so, have you taken into consideration safety aspects?

- ○ **Yes**
- ○ **No**
- ◉ **Not applicable**

Question 9: Has the legal framework on safety influenced your decision on whether to invest in developing apps or software?

- ○ **Yes**
- ○ **No**
- ◉ **Not applicable**

Question 10: In the EU Member State where you operate, are there specific rules on safety requirements for apps or other non-embedded software?

- ◉ **Yes**

No

17. The Information Commissioner's Office also provides guidance:

(a) ICO guidance on privacy in mobile apps

(b) ICO guidance on personal information online

(c) ICO guidance on personal information online—small business checklist

(d) ICO guidance to consumers on using apps safely and securely on their mobile

(e) ICO guidance to consumers on keeping their mobile devices secure

18. However, as technology develops (e.g. with 3D printing, and radio frequency identification) it is likely that legislation and guidance will have to be reformed more frequently with sector-specific knowledge.

Question 13: Do you have any further comments?

19. No.

Bar Council[4]
September 2016

For further information please contact
Melanie Mylvaganam, Policy Analyst: Legal Affairs, Practice and Ethics
The General Council of the Bar of England and Wales
289-293 High Holborn, London WC1V 7HZ
Direct line: 020 7092 6804
Email: MMylvaganam@BarCouncil.org.uk

[4] Prepared for the Bar Council by the Information Technology Panel