fieldfisher

Mental Health Apps and Privacy Notices

16 May 2022

Lorna Cropper/Alexandra Hague/Minhaal Datoo

Mental Health Apps and Privacy Notices

How is the wellbeing of your Privacy Notice?

Last week was mental health awareness week in the UK, which this year had an overarching theme of loneliness. May, is also mental health awareness month in the US. The coronavirus pandemic has impacted everyone, regardless of socioeconomic background and global location, although certain groups of individuals and sectors have fared much worse than others. Whilst conversations around mental health were gathering pace pre pandemic, the impact of the last two years has put the mental health of all front and centre.

Health services and mental health resources are under pressure and there is a shortage of available therapists, even if you can afford to pay privately. In recent years to add to the library of self help books available, there has been an increasing number of mental health apps introduced to the market. These apps can be used in isolation or in conjunction with therapy and/or other wellbeing techniques. To some they can provide an absolute lifeline and they certainly enable users to feel calmer and more able to take control of their life when it otherwise seems hopeless, terrifying, chaotic ... Given the importance that these apps have in society, it was somewhat alarming to see the results of the Mozilla Guide on Mental Health Apps recently, which raised concerns about the privacy protections of mental health and prayer apps.

The Irish Data Protection Commissioner's (DPC) decision on WhatsApp and accompanying EUR 225m fine in August 2021 (DPC WhatsApp Decision) is heavily focused on transparency, i.e., the information that should be given to individuals and showcases what needs to be provided in a privacy notice. As we approach the fourth anniversary of the EU and UK GDPR (General Data Protection Regulation) and non compliance data protection matters make headlines across the media, now is an ideal opportunity for every organisation to reflect on the wellbeing of its own privacy notice and determine if it needs a refresh. To assist with that task, we take a look at the concerns the Mozilla Guide expressed, the key factors stemming from the DPC WhatsApp Decision and the UK's proposal for a voluntary Code of Practice for apps stores and developers.

Mozilla **Privacy Not Included* buyer's guide

Known for creating the Firefox web browser almost 20 years ago, Mozilla has since turned its attention to the goal of keeping the internet open, accessible and healthier for all. In an effort to give individual users real agency online and to ensure tech providers are held accountable, the Mozilla Foundation created the **Privacy Not Included* guide (the 'Mozilla Guide') in 2017 and a most informative user guide. The objective of the Mozilla Guide is to empower individual consumers to shop smartly and safely for products that connect to the internet and be able to identify privacy-related issues such as:

- whether their personal data will be shared or sold;
- the app developer's track record of protecting an individual's personal data; and
- how secure or vulnerable the product is.

The latest iteration of the Mozilla Guide focused on 32 mental health and prayer apps. Mozilla's verdict was that the majority of apps, 26, i.e., 81% fell below par and were given a **privacy not included* warning sign. Of great concern to Mozilla is how those apps, lacking in privacy protections, "track, share, and capitalise on users' most intimate personal thoughts and feelings". Another key finding was how the apps are a "data harvesting bonanza" to such an extent it was "more than Mozilla researchers have even seen from apps and connected devices"! We invite readers to consider the Mozilla Guide for themselves and take the opportunity to click on an assortment of apps to observe the most detailed information about the apps researched, including their privacy and security features. To filter through the good, the bad and the ugly, we took an example in each category - the best in class, i.e., those without the **privacy not included* warning sign; those with the warning sign; and one of the "six worst offenders" to determine what the worst offenders are doing wrong and what the non-offending apps are doing well.

Mental Health Apps and Privacy Notices

The good, the bad and the ugly

Data protection area under focus	The Good	The Bad	The Ugly
Privacy Notice	Not commented on explicitly.	Alarming given its content about how much data it collected.	Found to have many shortcomings with key information missing.
User friendly privacy information	No.	No.	No.
Collection of data	Some common points such as name, email address and app usage data. Facebook ID (if given by the user). Far less data in comparison to other applications.	Personal information. Information from third party sources including "consumer research platforms, and/or business contact databases". Tracking data. Targeted advertising data.	Name, contact details, details in case of emergency, sexual orientation. Mental health symptoms and observations.
Data Sharing	With Google and Facebook for targeted advertising and personalisation.	With ad and analytic service providers. The fact the app shares "aggregated" data prompted Mozilla to remind readers about the relative ease to de-anonymise data.	With advertising partners and service providers. With affiliates across the corporate group.
Use of machine learning	In development to allow an individual's data to be used to offer new, personalised content in real-time.	No.	Researchers unable to determine.
Data retention	Accounts inactive for two years – data is anonymised.	Provided for Californian and EU residents.	No details mentioned.
Mozilla recommendations for protecting your privacy	Check out the app's own tips to protect your account from a data breach. Disconnect the app from any social media site you are logged in to.	Do not log in to the app via your social media account. Choose a strong password.	Do not connect via Google, social media or third party tools and do not share medical data when connected to these accounts. If messaging within this app, delete each message if you do not want it to be retained in your account.

Mental Health Apps and Privacy Notices

Since it is a requirement of an app store that any app submitted has a privacy notice, with respect to those apps selected for the Mozilla Guide, the devil is perhaps in the detail (or lack of it in certain cases). It was extremely difficult to find an app with the Mozilla Guide that is considered to have "user-friendly privacy information"! It is beneficial to know that a minimum of eight hours was spent researching each app and often the greatest alarm generated for researchers appears to be the data collected and/or shared with an array of third parties beyond advertisers. It is common practice for data to be shared with advertisers although users can configure their browser and device settings as well as be savvy in their cookie / similar tracking technology selection, in order to maintain their privacy with respect to advertising. Conversely, the user is less in control, other than by consciously choosing the product they wish to use, when controllers share data with other stakeholders.

Minimum requirements for your privacy notice

The information that must be provided in a privacy notice is set out under **Article 13** of the EU and UK GDPR. The aim of these requirements is to ensure that individuals are properly informed about how their personal data will be used and why. The content a notice needs to provide includes, amongst other details, the purposes for which the app provider will use personal data collected via the app and the legal bases that will be relied on to process that information. To accompany the GDPR, the European Data Protection Board (EDPB) issued guidelines on transparency, which provided examples on how information should be presented to data subjects. The DPC WhatsApp Decision was equally noticeable for the fact that it concerned information that should be given to non users but who contact(s) was a user of WhatsApp.

As mentioned at the outset of this blog, the DPC WhatsApp decision and accompanying fine of EUR 225 million fine has taken matters to a whole new level. The DPC in its 266 page decision has made clear its expectations and those of the EDPB (the DPC's initial proposal, you may recall, was a fine for EUR 50 million). The DPC had a number of issues with the level of transparency that WhatsApp had provided to its users both in terms of how the privacy notice was presented as well as the level of detail it included. Key takeaways from the WhatsApp decision include:

- a far higher level of detail than what up to the date of the DPC WhatsApp decision was standard practice;
- a notice that is easily accessible;
- a notice that does not use multilinked documents so that information is not buried and it is clear to the user when the have exhausted all sources of detail;
- the need to specify the legal basis and purpose of processing for each processing activity by reference to the particular types of personal data collected; and
- details about data sharing arrangements need to be as precise as possible.

A requisite of the DPC WhatsApp Decision was that WhatsApp needed to provide the information found lacking within three months of the decision. WhatsApp published a modification of its privacy policy on 22 November 2021, which has been updated most recently in March 2022. WhatsApp's privacy notice is undoubtedly the platinum standard although such a comprehensive notice may not be pragmatic for every business, especially if the product is not a global one, in a family of related apps, with a user base in its billions.

UK's proposal for a Voluntary Code of Practice

The use of apps today is pervasive and given the spectrum of developers and devices across which apps can operate, the UK government has launched a consultation on its proposal for a voluntary Code of Practice for all app store operators and developers. Essentially the government wants to increase the standard of apps and protect users from "malicious and insecure apps", which it has persistently seen available during a review from December 2020 to March 2022. The code would set minimum security and privacy requirements. Interestingly the code proposes that privacy information would need to explain why an app needs access to users' contacts and their location. The consultation is open until 29 June 2022 and opinions are sought on the interventions the government is proposing to limit the number of bad actors in this space. Developers, in particular, are asked to contribute about their experiences "on the review and feedback processes" they have had when submitting apps to the different app stores.

The 'win-win' of privacy compliance

The DPC WhatsApp Decision is not an isolated case about the deficiencies in a privacy notice. There have been several other recent cases involving privacy notices among regulators such as Klarna Bank AP and Brussels Airport Company NV/SA, which have similarly been subject to fines in relation to failures in their privacy notice practices.

Privacy and data protection today is proving to be a market differentiator and it is apparent from the Mozilla Guide that organisations that respect users' privacy will be promoted. The UK's Information Commissioner's Office has for some time championed the notion that the public needs to be able to trust companies with how their personal data is used. Trust as the saying goes has to be earned and there are certainly ways data controllers can do that. App providers should also note that it is not just regulators taking action on the lack of privacy protections. Cisco's 2021 Consumer Privacy Survey demonstrated that consumers are taking action to protect their personal data, including by switching providers or companies as a result of their data protection practices or policies.

It is clear that the makeup of a privacy notice is under the spotlight from regulators, civil society and users. The concerns too go beyond the content and accessibility of the notice itself. Improving a privacy notice though may in fact increase the amount of data an individual is prepared to disclose when a transparent notice is readily available to inform them about how their personal data is used, shared and safeguarded.

For example, a mental health app provides users with the option to complete a monthly tracker on a daily basis about their mental health whilst the app tracks their interaction with the app's services. However, due to users' concern about the app's privacy protections, a significant number of users do not engage with this survey. To alleviate the users' concern, the app provider introduces a new privacy notice, additional privacy settings and encourages users to create strong passwords. Confident of how their data will be used and shared, users begin to engage with this survey that provides visible results that demonstrate how continued use of the app brings great benefits and improvement their users' mental health. Such a data set will equally be valuable to the app providers and mental health experts who could research the value and effectiveness of particular courses or meditations within the app. With increased consumer confidence, more valuable data sets are achievable as well as increased user numbers for the app provider due to user trust and visible benefits of using the app.

There is no better time to review, update and enhance your privacy notice in accordance with the new level of what is accepted compliance. Do also consider how else your notice can be presented beyond a static, written document. The investment of time, resources and finance will undoubtedly bring dividends for app providers.