Mobile App Design

Contents

1. SCOPE OF THIS GUIDANCE

This guidance has been written specifically for the context of mobile apps developed and used to conduct research for which University ethics review and approval is required. The same design and privacy principles can be applied to any software developed for research purposes, but this guidance pays special attention to the risks that are most likely for mobile devices like phones and tablets.

Researchers may wish or make use of mobile apps for a variety of uses: the sensors, processing power and flexibility offered by phones, tablets and other mobile devices can unlock a new world of research and data collection. However, these same features can also expose the app users (including research participants), device owners and researchers to different types of risk. The new use of the device may expose the device or user to physical risks (e.g. doing a task one-handed while entering data) or to ethical or privacy risks (e.g. collectin h to create g data on an activity which was not monitored before). For example:

- The app may, without the user realising, have access to data sources or sensors on the phone (location, contacts, camera, microphone, etc.) which are sensitive or private, and must be treated with respect.
- The app developer/ deployer may be exposed to legal risk, e.g. prosecution under Data Protection law in the event of data breach.
- The app may create a software or hardware vulnerability for the device, exposing users to potential data theft or device hijacking by other actors – which may also entail legal liability for the app developer/ deployer.

In the case of apps used for medical research, these issues can be even more complex, and may be subject to the Medical Devices Regulations (see this UK Government guidance for further

details). For guidance on medical research, please contact the Medical Science Research Ethics team, ethics@medsci.ox.ac.uk. This should be done at the intial planning stage.

No app can ever be perfectly secure and private, but the guiding principles in this document are a starting point for responsible app development. It is good practice to document your choices, especially where trade-offs must be made, so you can justify design decisions should any questions arise. For background reading on privacy and security, we highly recommend the UK Information Commissioner's Office guidance for app developers for privacy in mobile apps.

2. HOW TO USE THIS GUIDE

This document is a list of broad principles which should be applied, to help minimise risk to researchers and research participants. It is meant to serve as a prompt: if you come across a concept that is unfamiliar, or you are not sure how it applies to your project, it is a cue that you should seek advice.

You can turn this Guidance document into (part of) your app's documentation, by providing answers for each of the bullet points below. This list is not exhaustive – please add further points as relevant for your project.

3. CONSENT

If you are building a research app which will collect or share data from users, you must ensure you have obtained and have a record of their informed consent. This is often implemented as a click-to-agree page at the start of the app. Ask your local DREC (or IDREC) if you have any questions about acceptable consent processes; Best Practice Guidance 06 on Internet-Mediated Research is a good starting point. You will also need to obtain CUREC approval before you conduct your research.

The COVID symptom study is an example of an app that has managed the consent process well: information is provided within the app, there is an easy-to-complete consent form, and users are emailed a copy of the study information for their records.

- What information do you need to provide to users, so they can make an informed choice about whether to participate? (what the app does, how the data will be used, etc.: see the CUREC consent templates as a starting point)
- How, when and where will you give users this information?
- How will you record participants' consent, and where/ for how long will this be kept?
- Will there be a way for users to contact the developers/ researchers?
    - Will this be through the app, or via email/ another channel?
    - Will this allow user anonymity to be preserved (if necessary)?
    - *(protip: create dedicated contact addresses for each app you make, with separate addresses for research questions vs. tech support)*
- Can participants withdraw their consent if they wish to stop participating?
    - How can they inform you of their wish to withdraw consent?
    - What happens to the app they have installed?
    - What if they uninstall the app first, and then wish to withdraw consent?
    - What happens to any data that has already been shared with the researcher?
    - What happens to any data stored on the participant's device?
- If the app is in an App Store, what will be the experience for people who find it and aren't part of the study? Will you be collecting their data? Access to the app should ideally be limited only to people taking part in the research, e.g. by issuing an activation

code, to be entered into the app, after requesting access (or once consent has been given to take part).
- What is your CUREC approval reference number?

4. BASIC TECHNICAL STANDARDS

Apps must meet acceptable industry technical standards and specific standards set by mobile app distributors, for example:

- Android http://developer.android.com
- Apple https://developer.apple.com

However: these industry standards have insufficient security and privacy requirements, especially in the context of academic research ethics. Simply meeting those standards is not enough.

- Which technical standard(s) will you follow?
- Do these standards have any shortcomings for ethics, privacy or security in your case?
- If so, how will you work around those shortcomings?

5. PRIVACY AND SECURITY

When building your app, you should bear in mind the following security principles. Even if you are well-versed in software security practice, we highly recommend you get an outside opinion on your code. The Computer Science DREC can help you find a second opinion if necessary.

Management of personal data, either directly or via a third party, must comply with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as set out in the University's Guidance on Data Protection and Research. Advice on data protection is also available from the Information Compliance team.

Be explicit about your design goals, both at the design stage of the project, and with your users. Which of these best describes your approach?

- You do this at your own risk, it was built by enthusiastic researchers with limited experience in this area.
- This is a research app which is not designed for the general public – we've tried to be robust, contact us with questions.
- This is a serious production-grade project and we will guarantee its performance.

Always seek to put the user's interests ahead of your own: prioritise their security and privacy wherever possible. Remember that intimate partners may be part of the threat model (e.g. abusive partners, housemates or stalkers), as well as criminals.

5.1 Data protection and privacy

Minimise the data you collect and process, and seek to give participants control over this (especially for personal data). Concepts such as anonymisation/ pseudonymisation, unlinkability, transparency, intervenability and enforcement/ demonstration are key: see Chapter 5 of the ENISA report on Privacy and data protection in mobile applications for details. For example:

- Where possible, separate personal data from other research data (through anonymisation, or use of a user ID with the de-anonymisation key stored in a separate location).
- If your methods will give you access to data that you do not need for this research (e.g. you are interested in pictures from the device's camera, but the file also includes metadata such as location): can you strip this data from your records to minimise your

contact with it – better still, can this data be stripped on the device before upload, so you never come into contact with it?

- If you need location data, can you use a coarse indication of location (e.g. ask users for the name of their city or area) rather than direct GPS location data?
- Do not keep any sensitive or personal data longer than absolutely necessary.
- How will you apply the principles above to your project?

5.2 Data handling

Carefully work through your **data handling process**: we highly recommend you draw this out as a diagram. People who are unfamiliar with this process might benefit from using Data Flow Diagram notation. It may (possibly) simplify things if you make your software into an online application, rather than software that must be installed on users' machines.

- Exactly what kinds of data are collected, from where, using what process? (e.g. username, location, responses to daily survey, time of app login…)
- Will your app collect personal data (legal definition)?
- For each type of personal data, who is the Data Controller/ Data Processor?
- What data remains on the user's device?
- What data is shared with the researcher?
- How and where is data moved and stored? (and will this be compatible with firewalls?)
- Who owns those locations? Are cloud providers involved? What are the contractual arrangements?
- Will there be any security/ encryption for data in transit or data at rest? "Data at rest" includes in the users' devices, and their local or cloud backups of those devices; not just the researcher's project server and workstation.
- Who will be able to access the data in each of the locations? (You, Oxford collaborators, external collaborators, the device manufacturer, the app author, third parties like cloud providers…)
- What kinds of data processing will be done, and by whom? This might include "processing" data for research, but the legal definition of Data Processing under the UK Data Protection Act/ GDPR is very broad.
- What anonymisation/ pseudonymisation measures will you take and how easily could individuals or data points be re-identified (e.g. by combining your dataset with other available data)?
- Will your app give you access to personal or sensitive data that you do not need to collect for this research? If so, how will you deal with that data?
- Can the participant independently see (or edit) the information that is shared with you?
- If the participant asked you for a dossier with all of the information that you hold about them, could you provide it?
- If the participant asked you to change or remove any of their data, could you do this?
- How long will the research data be kept (where, and by whom? What happens if current project members leave)?
- How and when will your research data be deleted?
- Will any data be archived or shared (e.g. as a data set for others to use)? If so, under what conditions, and what will you do to ensure that data has been sanitised prior to archival/ sharing?
- Map out your stakeholders: who may come into the orbit of your project? This might include yourself, your research collaborators, the user, the user's contacts (who could be impacted in the event of participant oversharing/ data breach/ poor app design…), the University, regulators…

5.3 Security

Write secure code, considering whether you should apply principles like obfuscation, minification, bug testing, hardening and signing/ tamper detection. The OWASP Foundation keeps a reasonably updated list of top ten mobile risks, which you may find helpful.
Think about authorisation and authentication early in the development process, and explicitly address both topics in your design. If you are not familiar with these concepts, the Oxford Research Software Engineering team may be able to help.

- How will you apply security principles to your codebase?
- Could you enable features like remote log-off or remote wiping of the app (e.g. in case of theft or loss of device)?

You should also consider how you could maintain the authenticity of recorded data against malice or mischance (e.g. hashes computed at collection time that can be verified at processing time, or digital signatures if you need stronger guarantees).

The Infosec community often frames security in terms of three properties: **Confidentiality**, **Integrity**, and **Availability**. For academic research applications, you should add **Anonymity** to this framework. Think about how all four properties apply to what you can achieve, and what trade-offs you will make. For example, improving confidentiality through authentication may result in reduced availability of data, especially in time-critical applications. If you protect the integrity of anonymous data with hashes from per-device keys, you may reduce anonymity by associating the data point with the device it came from. No project can be perfect in all four areas: make sure you understand why and how you have decided where to set the balance.

How will you handle encryption and/ or other security measures for:

- Data held on the user's device?
- Data held on your server?
- Data in transit from the phone to your server?
- Can you achieve end-to-end data integrity protection?

Note: the University can issue TLS certificates: contact your local departmental IT team or the IT Services helpdesk. Alternatively, if you are using your own domain for the server, https://letsencrypt.org can provide certificates for free. You may wish to use certificate pinning to help prevent man-in-the-middle attacks.

Be careful when using **third-party libraries**: some have known security and privacy vulnerabilities, and others are simply not maintained, making it difficult to maintain the security of any app built on top of them. On the other hand, commercial or open-source packages may be better implemented than "a random graduate student's" code. This article is a useful starting place for auditing third-party libraries.

- Which third-party libraries will your project use, and how will you address risks regarding long-term support or known vulnerabilities?

Think about **session-handling**: use tokens rather than device authentication where possible. Many devices have secure enclaves available for creating and using cryptographic material, giving hardware level protection. These should be used where possible.

- How will you address session handling?

For **cryptographic key storage**: use containers wherever possible; try to avoid storing keys on the user's device (although it may be necessary sometimes, e.g. device-specific keys for anonymisation). Use up-to-date schemes: https://www.keylength.com aggregates recommendations from NIST, BSI, and other sources.

- Which encryption scheme will you use?
- How and where will you store cryptographic keys?
- How and when will keys get rotated (periodically replaced), and how will cryptographic breaches (accidentally shared private keys, weaknesses discovered in algorithms/ implementations) be handled?

Think about Application Programming Interfaces (**APIs**): use authorised APIs for your own work, and do not open your API unless you understand the security/ privacy risks this may entail for the user.

- Will you use an API? If so, will the API be open?

5.4 Lifecycle

Think about the whole lifecycle of your app:

- Might it be worthwhile to make a 'beta release' to get feedback on bugs? (and if so, who should use the beta version, and what might the consent process look like?)
- How (and for how long) will you maintain the codebase and roll out patches?
- What happens to the app/ any data held on the participant's device, when their participation has ended?
- What happens to the app at the end of your research project?
- What happens if the lifecycle of the app is longer than the post of the person in charge of the codebase (or participant support)?

6. ACCESSIBILITY

You should consider the needs of potential users with poor vision, hearing, manual dexterity and other impairments.

For web design (and related app features), you should aim to meet Level-AA standard of WCAG 2.1. This includes elements such as:

- Alt text for all images and providing non-visual alternatives where appropriate.
- All essential audiovisual information is captioned, described as necessary or provided in alternative formats.
- Content can be navigated with just a keyboard or speech recognition tools.
- The website can be used with a screen reader.
- Content is structured, ordered and labelled appropriately.

The Digital Communications team at the University provide guidance for how you can maintain accessibility standards. The BBC mobile accessibility guidelines are also useful.

- How will you address accessibility considerations for your app?

7. BRANDING

You may wish to include the University's logo or name on your app. If the app is for a research project which is covered by University of Oxford research ethics clearance, use of the University logo should be straightforward. For apps which you wish to release to the general public (for non-research purposes), it is difficult to provide blanket guidance: be careful who you are

claiming to represent. Please ask your local DREC/ IDREC, and/ or Communications Office, or Public Affairs for guidance (see https://www.ox.ac.uk/public-affairs/branding-toolkit).

8. INTELLECTUAL PROPERTY

If you plan to put your app into an App Store, you should think about Intellectual Property: contact the Intellectual Property Rights Management team and Oxford University Innovation for advice. For licensing and Free and Open-Source Software questions, the Research Data Oxford team is an invaluable resource. Even if you do not plan on a general release, we recommend you investigate this: IP considerations will come into play if the person who developed the code moves to a new institution, for example.

Note also that App Store Terms and Conditions are not a good fit for University of Oxford processes. It might be worthwhile for you to investigate departmental or organisational developer accounts rather than attempting to release software in your own name.

9. USEFUL TOOLS LIBRARIES

- If you are developing on iOS, using Testflight allows you to invite specific users to use an app, allowing for limited release, only giving access to research participants etc. This also allows you to prompt for updates and automatically expires your app after a set amount of time. It also allows you to stop the app from being used, which is useful should a security or ethics issue arise. Google Play has some similar functionality.
- The Alamofire swift library (for iOS) contains all networking functionality you should need. It also has support for SSL and certificate pinning.
- If you need to store Cryptographic material, on many iOS devices this can be stored in the secure enclave, a hardware layer that helps protect keys.
- The android developer docs contain best practice guides for network security.
- Android enables encrypted file storage.

10. CHANGE HISTORY

Version No.	Significant Changes	Previous Version No.
1.0	New document.	N/A