Ethics in an App

Table of Contents

An Attempt At A Fundamental Rights Based Proposal

0 Introduction

Our digital society is heavily dependent on mobile technologies. The majority of individuals use smartphones more frequently than desktop computers or laptops. The mobile-first paradigm has become increasingly important for the past 10+ years. These smartphones are often locked-in computers that heavily limit what users and developers can do on the platform. Apps are the dominant interface that people use to interact with technology. App Stores are often overlooked points of control in our modern digital ecosystems. This Manifesto establishes ethical principles for this ecosystem. For us, the human perspective and fundamental rights are center stage for the design and evaluation of technological systems – following the ideas of ‘Digital Humanism’.

This Manifesto is structured according to the principles that ethical Apps, App stores and smartphones need to follow. Principles are defined as follows: What is the problem. Why is it a problem. How can it be resolved. Principle to be followed.

1 Respecting users’ time and attention

Often, digital technologies are introduced with the promise of reducing staff at an organization – after all, the laborious task of filling out forms for a given workflow is outsourced to the user. While on the one hand, digitalization can improve workflows for everyone and thus be a net-gain for both the users and the organization, often enough it is implemented by simply outsourcing the workload to the users. In the long run, this is disrespectful of users’ time and their attention. Users tend to get overloaded by tasks they should now do instead of the clerk who originally would help them. The objective therefore must be that whenever workflows are transformed, possibly supported by an “easy to use” app, great care should be taken to measure if the overall user experience is quick, efficient and lean.

2 Limiting user profiling

Many Apps rely on inferences or conclusions about or profiling of their users. These predictions about a person are often wrong, can be discriminatory, and can have negative consequences for that person. Such processing of personally identifiable information requires prior informed and active consent under European privacy law (GDPR). This right is very often violated by Apps and App Stores. Public authorities should refrain completely from profiling their users through their applications and Apps. Therefore, it shall be a principle of ethical Apps to refrain from user profiling.

3 User-control over sensors

Modern smartphones contain a wide variety of sensors which collect information about their users. Without proper safeguards microphones, cameras, location services, movement tracking, etc. are all ubiquitous surveillance technologies in our pockets. The amount of information that can be accumulated about every aspect of a person’s life undermines the essence of our right to privacy and therefore needs to be regulated both by technological and legal measures. Users have to be in control if, when, why and how information from these sensors is accessed by the operating system or Apps. Therefore, it shall be a principle of ethical Apps to obtain informed user consent for a specified purpose, time, and frequency before sensory information shall be assessed. Subsequently, it shall be a principle of Ethical smartphone operating systems to provide users with functionality to obtain knowledge and exercise control over the use of sensory information. The best way to achieve this is by having hardware switches and control LEDs for the sensor equipment on the device. Lastly, it shall be a principle of ethical App stores to prohibit mandatory consent to access of sensory information for both the installation of Apps and the performance of their primary functions.

4 Privacy-enhancing technologies for access to personally identifiable information

Given the sheer amount of personally identifiable information that our smartphones process and the ways in which this information can be obtained by third party developers via Apps, it is vital that the smartphone operating system has built-in functionality to ensure a responsible ‘privacy by design’ philosophy. Without such design safeguards, consent can become meaningless, because granting access to personal information (sensory data or other data points on the device) will always lead to overly intrusive information obtained by the App. To solve this problem and prevent the erosion of user trust in these systems, users need to have a real choice about the information given to third parties. Therefore, it shall be a principle of Ethical smartphone operating systems to provide for technical safeguards of the principles of privacy by design and by default. In practice, these principles entail that a smartphone operating system has to offer functionality to only give access to address books in a form which conceals personally identifiable information (e.g. hashed telephone numbers). Access to address books and photo libraries should be fine granular to only allow an App to access a sub-set of these data points. Consent for obtaining location information from the device needs to be limited to a single use or a specified period of time, instead of indefinite, and it is also required to be fine granular to allow for fuzzy approximations of detailed locations (e.g. whole districts instead of streets). Subsequently, it shall be a principle of ethical Apps – following the GDPR – to distinguish between personally identifiable information that is required for the primary functionality of the app and ask for further access once freely given informed consent was given by the user.

5 Accessibility

Often users with disabilities face exclusion and hardship when accessing Websites/Apps. Especially for Apps/Websites which serve public needs and provide public services, the goal should be to leave no one behind, serve everyone and think about possible user challenges when planning the project. Therefore, it shall be a principle of ethical Apps to follow established best technical practices for accessibility.

6 User control over App access to information on the smartphone

Most smartphones contain a wide variety of data points about a person’s life. The photo library on a smartphone can contain thousands of personal photographs. The address book on a smartphone can contain personal information (like home address, birthdays, or occupations) about third parties who have not given consent to the processing of their information on somebody else’s smartphone (although such uses on a private phone might not fall under the GDPR). Music libraries can contain specific information about musical tastes and character traits. Smartphone operating systems need to regulate access to this information with a focus on transparency and user control. Therefore, it shall be a principle of ethical Apps to provide the user with detailed and comprehensible information about the purpose and consequence of any request for access to data points on the smartphone. Subsequently, it shall be a principle of Ethical smartphone operating systems to provide the user with transparency functions detailing which App has accessed which data points at what time and allow the user to grant or revoke access to these data points. Lastly, it shall be a principle of ethical App stores to prohibit mandatory consent to access of data points on the smartphone for the installation of Apps or for the performance of their primary functions.

7 Configurability of smartphones and deletion of all pre-installed Apps

An annoying habit of smartphone vendors and carriers is to pre-install Apps that cannot be uninstalled by the user. Often these Apps are then also the default for certain functionalities, or the configuration of the device limits the users’ ability to change the defaults. A good example are Maps and Messaging Apps which the user is often tied to whenever they click on an address or want to send a text message. This problem can be solved if users were given the choice to uninstall all pre-installed Apps and change all defaults about associations with Apps (e.g. address links, telephone links, etc.). Therefore, it shall be a principle of Ethical smartphones to empower users to uninstall all Apps and change all settings.

8 Disentanglement of smartphones from manufacturer cloud services

Almost all modern smartphones can only be operated with their full functionality when the user agrees to the terms of service of a proprietary cloud service from the manufacturer. Customers acquire the hardware of their smartphones including the operating system, yet they are barred from fully utilizing it. Untying smartphones from the manufacturer’s cloud empowers users to have full choice about how they want to use their devices and to whom they entrust their data. Therefore, it shall be a principle of ethical smartphones to allow the full functionality of the device (hard- and software) without the necessity of any communication to cloud infrastructure.

9 Quality labels for Apps in App stores

We acknowledge the enormous bottleneck of App Stores in the distribution of Apps. This necessity can become a virtue for the transparency towards consumers. Right now, App reviews in App stores are mostly focused on their compliance with the terms of service of the store. Information provided is of very limited usefulness for making informed consumer choices. Establishing third party hallmarks that help identify Apps with a particularly good adherence to high data protection standards or to the criteria of this ethical App Manifesto would be as useful as automatically generated labeling of Apps that contain tracking and spying functionality and connect to the servers of Facebook, Google, Amazon or other dominant market players.

Therefore, it shall be a principle of ethical App stores to enable third party hallmarks from established consumer protection or data privacy initiatives with the goal of informing consumer decisions about the outstanding positive or negative characteristics of the App.

10 Resetability and security expiration date

Today consumers can buy a new smartphone from the store and within a few months might find themselves in the situation of no longer receiving vital security updates from the manufacturer. While the hardware is still perfectly fine and could be used for many years, the manufacturer might choose to no longer invest in the security maintenance of this particular device. This is both a challenge for the users' security, as well as an ecological problem. A solution for this issue that will empower consumers is that smartphones should be sold with a "best before date" for security updates. After this date has expired and the manufacturer chooses not to extend it, they must release the drivers of all hardware components of the smartphone as free software to allow third party operating systems and community projects to continue sustainable and secure use of the device. Therefore, it shall be a principle of ethical smartphones to be only sold with a clearly communicated date until which the manufacturer is obliged to provide (security) updates for the device and after this date has expired, the manufacturer needs to release the drivers for all hardware components of the smartphone under a free license.

11 Alternative App stores & side-loading

Distribution of Apps on Apple iPhone smartphones is only allowed via the Apple App store. This bottleneck severely limits the choice of users how to use their devices, the innovative capacity of App developers and cements the monopoly position of Apple in control of 'their' iPhones. A proven solution to this problem is to allow the installation and execution of Apps from App stores of third parties or the installation of Apps via external storages or websites (aka: Side-Loading). Therefore, it shall be a principle of Ethical smartphones to allow for third party App stores and side-loading of Apps.

12 Respecting the intent

Big tech has been very successful at evading any regulation of their services. Examples are legal evasion such as hiding disclaimers (“must be older than 13 years for this service”) in long EULAs which no one reads (in this example: especially not children). This can be seen as a way of complying with laws “on paper” but actually ignoring them in practice – an evasion technique. Apart from legal evasion techniques, technical evasion techniques exist, which slightly modify a service / app or piece of software so it does not quite fall under a particular set of regulations

A third form of evasion is the nudging of users to accept certain (non-)privacy settings by simply repeatedly asking them until they give in. One example are cookie banners on web sites which pop up repeatedly. Or asking if a setting should be activated every time you open the app. A “No” shall be a “No”, the intent of the user must be respected. Dark patterns such as nudging users to accept detrimental privacy settings must be avoided.

Ethical apps and operating systems shall respect the intention of regulations (GDPR, etc.) and the intent of users and not try to circumvent it. Parallel to this, the legal system must adapt to identify the intent of a modification of a service/app or operating system behavior and compare it with the intent of the relevant regulation.

We already apply this principle in criminal law, where intent is taken into consideration.

A corollary of respecting the intent of the GDPR is that tracking for advertising purposes or similar should be absolutely minimized, with a clear opt-in only strategy (for example by explicitly having to go to settings and actively enabling marketing tracking) and great care should be taken to not track personally identifiable information in any form.

13 Simple explanations of the intent and possible consequences

Where an app (or operating system) makes use of a user’s data or metadata, the intent of that usage must be explained in simple terms and/or graphically at a level that a child can understand quickly. Possible consequences of the data being sent to some server for processing must be mentioned. Compare with cigarette package warnings.

Users shall be given a choice to disable selected functionalities from apps/operating systems, where specific behavior is unwanted (and this intent shall be respected without further nudging of users. See above).

14 No geoblocking in App stores

Geoblocking, that is providing or denying content based on location, is a widespread practice. Neither where the request comes from nor the IP address disclose any information about the actua location of the request, not even about any legal attributes such as the nationality of the user. If services are only provided or denied because of the user’s location, this establishes a power imbalance, based on location or user competence and IP address. It basically excludes some people and favors others. The original, scientific Internet knows no nationality or location as an exclusion criterion. All people must have the opportunity to participate in processes, only in this way can the interests of all be safeguarded. Therefore, it shall be a principle of ethical App Stores not to distinguish between users based on their geo location and not to have Geo-blocking in app stores. In principle, access must be granted to everyone. In addition, the user must be able to decide which app version they want to use if different country versions are available.

15 Independent audits

Smartphone vendors and App Store providers are often circumventing existing legislation and regulatory goals of the jurisdictions they operate in. Such circumventions become even more easy when the vendors are big multi-national cooperations that have a strong market position. Ethical apps and operating systems shall undergo independent audits, to certify that they conform with the relevant regulations and respect their intent and whether the app or operating system follows this Manifesto. Therefore, it shall be a principle of ethical smartphones to publish such audits, and their methodology should be clear and repeatable.

16 Market transparency & no undue interference in App Stores

For the whole of the App ecosystem in modern smartphones the dominant vendors of the devices are also in control of the App Stores and hence they are the gatekeepers for the majority of software developers on these platforms. This form of vertical integration creates a monopoly situation for bringing Services and Apps to the devices. Over the past years we have witnessed the abuse of this power by Apple and Google by copying popular Apps from independent SMEs, using their knowledge from the App Stores to fine-tune their own services and in general tilting the market place in their favor. Meaningful regulation of this field needs to allow for the enforcement of anti-trust rules on App Stores – so as to prevent undue interference in the market place –, oblige App Store providers to offer comprehensive statistical overview about the market from a macroscopic perspective, due process in App Store review processes, as well as dispute settlement and legal redress for App vendors, and the possibility of App developers to interact directly with their customers. The Digital Markets Act of the EU and other European legislation are addressing some of these problems.

Therefore, it shall be a principle of ethical App Stores to provide macroscopic transparency about their market places, offer App providers due process for the review of their Apps with binding dispute resolution mechanisms and legal redress, while also not excluding the possibility of direct interaction between App providers and their users. Consequently, existing competition and anti-trust regulation needs to be enforced vigorously against App Stores.

17 Planned obsolescence

Smartphones make up a significant part of electronic waste. The normal lifespan of a smartphone is 2.5 years. Smartphones also contribute to approximately 10% of global e-waste, a number that was estimated to weigh more than 50 million tons in 2019. The potential value of raw materials in e-waste was valued at USD 57 million in 2019. Meanwhile, recycling rates across electronics stood at only 17% in 2019, meaning the vast majority of this value is not being reaped. Hence, it is vital to increase the lifespan of smartphones and in particular reverse the incentive structure of vendors to plan for obsolescence of their devices in order to sell a new generation of devices. From a privacy perspective it also makes sense to stop using one singular, general device for all aspects of life and move towards several, separate devices for particular fields or areas of life. Therefore, it shall be a principle of ethical Smartphones to publish information about the resources used in the production of the device, in order to allow for environmental benchmarking of devices, and to publish circuit diagrams, in order to allow for repairability benchmarks of the devices. Should the manufacturer not offer proper e-waste recycling or intentionally design their smartphones with an excessively short lifespan (planned obsolescence) or reduced repairability, then he should be held accountable via class action suits for environmental damage with incremental fines for repeat offenses.

18 Archivability

Smartphones increasingly become our exterior brains and reflect many aspects of our daily lives. The short-lived nature of this information in App Containers on smartphone Operating systems represents a huge long-term problem. Without the possibility to archive this information users are stripped of control over their information and locked into one particular App or App Ecosystem. Archivability is already enshrined in the right to data portability under the GDPR and can be implemented without conflicting with principles of data minimization and in commonly accepted formats. Therefore, it shall be a principle of Ethical Apps to ensure the Archivability and data export of user data from Apps in practice.

19 Public money, public code, public space

Public authorities increasingly offer Apps to interact with their citizens and provide public service information. Yet, almost all of these Apps are neither open source nor free software. This creates a problem for the transparency of these government functions due to a lack of auditing capacity of proprietary software. Terms of Service restrictions can in some cases limit the democratically desired functionality of the software. The future development and distribution of the software is often restricted by licensing regimes that are following the interests of private vendors more than public authorities. Licensing costs are recurring items in the budget, whereas free software is always in the public domain and can be maintained by a multitude of developers without lock-in effects. Similarly, the public spaces for discussion and interaction provided by public authorities should not be maintained or mediated by private corporations or proprietary software, because terms for citizen interactions should be defined democratically and not by commercial contracts with a vendor.

Therefore, it shall be a principle of ethical Apps from public authorities that they should be under a free and open source license. They should be distributed in App Stores specialized in free software (e.g. F-Droid) and limit the use of proprietary libraries (Google Play Services).

20 Participatory decision making when designing Apps from public authorities

A positive example of a transparent planning process with community participation is the data protection-friendly, German Corona Warn App, which is widely accepted by citizens exactly because of the transparency in its planning process.

App developers should learn from this example and take onboard some principles of community involvement in designing transparency with respect to data handling. In addition, this will lead them to properly develop the use cases together with the app's users, therefore further increasing acceptance of the app.

This participatory bottom-up citizen involvement aspect is also well known in urban planning and has already shown its merits there as well. Open Data is another example for the non-discriminatory, open-for-all,free-to-use approach which benefits all. Therefore, it shall be a principle of ethical Apps from government entities to include community and expert participation during all steps of development and maintenance.

21 Freedom & fairness in payment systems

The Internet has produced a completely new level in the freedom of the flow of information. The same freedom is also possible for the flow of money. With the advent of decentralized, protocol based money, the current App store limitations seem highly inappropriate unhinged and overly intrusive. App stores should not be allowed to dictate payment processes within the App or in other aspects of the underlying service. Developers should be free to innovate – within existing laws – the ways in which business models, donation systems and micro loans are offered to users. Therefore, it shall be a principle of ethical App stores to refrain from any restrictions of payment systems, going beyond the price of the software itself or potential in-App purchases via the App store.

A project by Aaron Kaplan, Hans Christoph Steiner , epicenter.works - Plattform Grundrechtspolitik, Widerhofergasse 8/2/4, 1090 Wien, Austria.
Made possible with the financial support of the Ma7 Kulturabteilung der Stadt Wien.
Code and text source available on Gitlab.
Download this proposal as PDF.
Contact us at ethicsinapps@epicenter.works.
Version: 1.0