ARTICLE 29 DATA PROTECTION WORKING PARTY

00461/13/EN
WP 202

Opinion 02/2013 on apps on smart devices

Adopted on 27 February 2013

Summary

There are hundreds of thousands of different apps available from a range of app stores for each popular type of smart device. It has been reported that more than 1,600 new apps are added to app stores daily. An average smartphone user is reported to download 37 apps. Apps may be offered for little or no upfront cost to the end user and can have a user base of just a few individuals or many millions.

Apps are able to collect large quantities data from the device (e.g. data stored on the device by the user and data from different sensors, including location) and process these in order to provide new and innovative services to the end user. However, these same data sources can be further processed, typically to provide a revenue stream, in a manner which may be unknown or unwanted by the end user.

App developers unaware of the data protection requirements may create significant risks to the private life and reputation of users of smart devices. The key data protection risks to end users are the lack of transparency and awareness of the types of processing an app may undertake combined with a lack of meaningful consent from end users before that processing takes place. Poor security measures, an apparent trend towards data maximisation and the elasticity of purposes for which personal data are being collected further contribute to the data protection risks found within the current app environment.

A high risk to data protection also stems from the degree of fragmentation between the many players in the app development landscape. They include: app developers; app owners; app stores; Operating System and device manufacturers (OS and device manufacturers); and other third parties that may be involved in the collection and processing of personal data from smart devices, such as analytics and advertising providers. Most conclusions and recommendations in this Opinion are aimed at app developers (in that they have the greatest control over the precise manner in which the processing is undertaken or information presented within the app), but often, in order for them to achieve the highest standards of privacy and data protection, they have to collaborate with other parties in the app ecosystem. This is particularly important with regard to security, where the chain of multiple actors is only as strong as its weakest link.

Many types of data available on a smart mobile device are personal data. The relevant legal framework is the Data Protection Directive, in combination with the protection of mobile devices as part of the private sphere of users contained in the ePrivacy Directive. These rules apply to any app targeted to app users within the EU, regardless of the location of the app developer or app store.

In this opinion the Working Party clarifies the legal framework applicable to the processing of personal data in the development, distribution and usage of apps on smart devices, with a focus on the consent requirement, the principles of purpose limitation and data minimisation, the need to take adequate security measures, the obligation to correctly inform end users, their rights, reasonable retention periods and specifically, fair processing of data collected from and about children.

Contents

1. Introduction

Apps are software applications often designed for a specific task and targeted at a particular set of smart devices such as smartphones, tablet computers and internet connected televisions. They organise information in a way suitable for the specific characteristics of the device and they often closely interact with the hardware and operating system features present on the devices.

There are hundreds of thousands of different apps available from a range of app stores for each popular smart device type. Apps serve a wide range of purposes including web browsing, communication (e-mail, telephony and internet messaging), entertainment (games, movies/video and music), social networking, banking and location based services. It has been reported that more than 1,600 new apps are added to app stores daily.[1] An average smartphone user will download 37 apps.[2] Apps may be offered for little or no upfront cost to the end user and can have a user base of just a few individuals or many millions.

The underlying operating system will also include software or data structures that are important for the core services of the smart device, for example, the address book of a smartphone. The operating system is designed to make these components available to apps through Application Programming Interfaces (APIs). Those APIs offer access to the multitude of sensors which may be present on smart devices. Such sensors include: a gyroscope, digital compass and accelerometer to provide speed and direction of movement; front and rear cameras to acquire video and photographs; and a microphone to record audio. Smart devices may also contain proximity sensors.[3] Smart devices may also connect through a multitude of network interfaces including Wi-Fi, Bluetooth, NFC or Ethernet. Finally, an accurate location can be determined through geolocation services (as described in WP29 Opinion 13/2011 on Geolocation services on smart mobile devices[4]). The type, accuracy and frequency of these sensor data varies by device and the operating system.

Through the API, app developers are able to collect such data continuously, access and write contact data, send email, SMS or social network messages, read/modify/delete SD card contents, record audio, use the camera and access stored pictures, read the phone state and identity, modify the global system settings and prevent the phone from sleeping. APIs can also provide information relating to the device itself through one or more unique identifiers and information about other installed apps. These data sources can be further processed, typically to provide a revenue stream, in a manner which may be unknown or unwanted by the end user.
The objective of this opinion is to clarify the legal framework applicable to the processing of personal data in the distribution and usage of apps on smart devices and to consider further

---

1 Report in ConceivablyTech of 19 August 2012, available at www.conceivablytech com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of. Quoted by Kamala D. Harris, Attorney General California Department of Justice, Privacy on the go, Recommendations for the mobile ecosystem, January 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

2 This is a worldwide estimate for 2012 by ABI Research, http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o

3 A sensor that can detect the presence of a physical object without physical contact. See: http://www.w3.org/TR/2012/WD-proximity-20121206/

4 See WP29 Opinion 13/2011 on Geolocation services on smart mobile devices (May 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

processing which might take place outside of the app, such as using the collected data to build profiles and target users. The opinion analyses the key data protection risks, provides a description of the different parties involved and highlights the various legal responsibilities. This includes: app developers; app owners; app stores; device and Operating System manufacturers (OS and device manufacturers); and other third parties that may be involved in the collection and processing of personal data from smart devices, such as analytics and advertising providers.

The opinion focuses on the consent requirement, the principles of purpose limitation and data minimisation, the need to take adequate security measures, the obligation to correctly inform end users, their rights, reasonable retention periods and specifically, fair processing of data collected from and about children.

The scope is applicable to many different types of smart devices but particularly focussed towards apps available for smart mobile devices.

2. Data protection risks

The close interaction with the operating system allows apps to access significantly more data than a traditional internet browser.[5] Apps are able to collect large quantities of data from the device (location data, data stored on the device by the user and data from the different sensors) and process these in order to provide new and innovative services to the end user.

A high risk to data protection comes from the degree of fragmentation between the many players in the app development landscape. A single data item can, in real time, be transmitted from the device to be processed across the globe or be copied between chains of third-parties. Some of the best known apps are developed by major technology companies but many others are designed by small start-ups. A single programmer with an idea and little or no prior programming skills can reach a global audience in a short space of time. App developers unaware of the data protection requirements may create significant risks to the private life and reputation of users of smart devices. Simultaneously, third-party services such as advertising are developing rapidly, which, if integrated by an app developer without due regard, may disclose significant amounts of personal data.

The key data protection risks to end users are the lack of transparency and awareness of the types of processing an app may undertake combined with a lack of meaningful consent from end users before that processing takes place. Poor security measures, an apparent trend towards data maximisation and the elasticity of purposes for which personal data are being collected further contribute to the data protection risks found within the current app environment. Many of these risks have already been examined and addressed by other international regulators, such as the US Federal Trade Commission, the Canadian Office of the Privacy Commissioner and the Attorney General of the Californian Department of Justice.[6]

---

[5] Although desktop web browsers are gaining wider access to sensory data on end user devices, driven by web game developers.

[6] See, amongst others, FTC staff report Mobile Privacy Disclosures, Building Trust Through Transparency, February 2013, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf, FTC staff report Mobile Apps for Kids: Current Privacy Disclosures are Disappointing, Feb. 2012,

- A key data protection risk is the lack of transparency. App developers are constrained by the features made available by Operating System manufacturers and app stores to ensure comprehensive information is made available, at a relevant time, to the end user. However, not all app developers take advantage of these features as many apps do not have a privacy policy or fail to inform their potential users in a meaningful way about the type of personal data the app may process and for what purposes. The lack of transparency is not limited to free apps or those owned by inexperienced developers as a recent study reported that just 61.3% of the top 150 apps provided a privacy policy.[7]

- The lack of transparency is closely related to a lack of free and informed consent. Once the app is downloaded, consent is often reduced to a tick box indicating that the end user accepts the terms and conditions, without even offering a 'No thank you' option. According to a GSMA study from September 2011, 92% of app users want to have a more granular choice.[8]

- Poor security measures may lead to unauthorised processing of (sensitive) personal data, for example if an app developer suffers a personal data breach or if the app itself leaks personal data.

- Another data protection risk is related to disregard (due to ignorance or intention) for the principle of purpose limitation which requires that personal data may only be collected and processed for specific and legitimate purposes. Personal data collected by apps may be widely distributed to a number of third parties for undefined or elastic purposes such as 'market research'. The same alarming disregard is shown for the principle of data minimisation. Recent research showed that many apps abundantly collect data from smartphones, without any meaningful relationship to the apparent functionality of the app.[9]

---

http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf and follow-up report, Mobile Apps for Kids: Disclosures Still Not Making the Grade, December 2012, http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf, Canadian Offices of the Privacy Commissioners, Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps, October 2012, http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf, Kamala D. Harris, Attorney General California Department of Justice, Privacy on the go, Recommendations for the mobile ecosystem, January 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

[7] FPF June 2012 Mobile Apps study, http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf

[8] "*89% [of users] think it important to know when their personal information is being shared by an application and to be able to turn this off or on.*" Source: User perspectives on mobile privacy, September 2011, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf

[9] Wall Street Journal, Your Apps Are Watching You, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

3 Data protection principles

3.1 Applicable law

The relevant EU legal framework is the Data Protection Directive (95/46/EC). It applies in any case where the use of apps on smart devices involves processing personal data of individuals. To identify applicable law, it is essential to first identify the role of the different stakeholders involved: the identification of the controller(s) of the processing carried out via mobile apps is particularly crucial in relation to applicable law. The establishment of the controller is a decisive element to trigger application of EU data protection law, although it is not the only criterion. According to Article 4.1.(a) of the Data Protection Directive, the national law of a Member State is applicable to all processing of personal data carried out "in the context of an establishment" of the controller on the territory of that Member State. Pursuant to Article 4.1(c) of the Data Protection Directive, the national law of a Member State is also applicable in cases where the controller is *not established* on Community territory and makes use of equipment situated on the territory of that Member State. Since the device is instrumental in the processing of personal data from and about the user, this criterion is usually fulfilled.[10] However, this is only relevant where the controller is not established in the EU.

As a result, whenever a party involved in the development, distribution and operation of apps is deemed to be a controller, such a party is responsible, alone or jointly with others, for ensuring compliance with all the requirements set forth under the Data Protection Directive. The identification of the role of the parties involved in mobile apps will be further analysed below in section 3.3.

Additionally to the Data Protection Directive, the ePrivacy directive (2002/58/EC, as revised by 2009/136/EC), sets a specific standard for all parties worldwide that wish to store or access information stored in the devices of users in the European Economic Area (EEA).

Article 5(3) of the ePrivacy directive prescribes that *the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing. (…)*

While many provisions of the ePrivacy directive apply only to providers of publicly available electronic communication services and providers of public communication networks in the Community, Article 5(3) applies to every entity that places on or reads information from smart devices. It applies without regard to the nature of the entity (i.e. whether public or private, an individual programmer or a major corporation or whether it is a data controller, data processor or a third party).

The consent requirement of Article 5(3) applies to <u>any information</u>, without regard to the nature of the data being stored or accessed. The scope is not limited to personal data; information can be any type of data stored on the device.

[10] To the extent that the app generates traffic with personal data to data controllers. This criterion might not be fulfilled if the data are only processed locally, in the device itself.

The consent requirement from Article 5(3) of the ePrivacy directive applies to services offered '*in the Community*', that is, to all individuals living in the European Economic Area, regardless of the location of the service provider. It is important for app developers to know that both directives are imperative laws in that the individual's rights are non-transferable and not subject to contractual waiver. This means that the applicability of European privacy law cannot be excluded by a unilateral declaration or contractual agreement.[11]

3.2 Personal data processed by apps

Many types of data stored on or generated by a smart device are personal data. According to Recital 24 of the ePrivacy directive:

> *"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms."*

They are personal data whenever they relate to an individual, who is directly (such as by name) or indirectly identifiable to the controller or to a third party. They may relate to the owner of the device or to any other individual, such as the contact details of friends in an address book.[12] Data can be collected and processed on the device or, once transferred, elsewhere, on app developers' or third parties' infrastructure, via connection to an external API, in real-time without the knowledge of the end user.

Examples of such personal data that can have a significant impact on the private lives of the users and other individuals are:

- Location
- Contacts
- Unique device and customer identifiers (such as IMEI[13], IMSI[14], UDID[15] and mobile phone number)
- Identity of the data subject
- Identity of the phone (i.e. name of the phone[16])
- Credit card and payment data
- Phone call logs, SMS or instant messaging
- Browsing history
- Email
- Information society service authentication credentials (especially services with social features)

---

[11] For instance, statements that only a law of a jurisdiction outside of the EEA applies.

[12] Data can be (i) automatically generated by the device, on the basis of features pre-determined by the OS and/or device manufacturer or by the relevant mobile telephony provider (e.g. geolocation data, network settings, IP address); (ii) generated by the user through apps (contact lists; notes, photos); (iii) generated by the apps (e.g. browsing history)

[13] International Mobile Equipment **Identity**

[14] International Mobile Subscriber I**dentity**

[15] Unique Device Identifi**er**

[16] Users tend to name their phone with their real name: "John Doe's iPhone".

- Pictures and videos
- Biometrics (eg facial recognition and fingerprint templates)

3.3 Parties involved in the data processing

Many different parties are involved in the development, distribution and operation of apps and each of which can have different data protection responsibilities.

There are four main parties which can be identified. These are: (i) the app developers (including app owners)[17], the manufacturers of the Operating System and device ("OS and device manufacturers")[18]; (iii), app stores (the distributor of the app) and, finally, (iv) other parties involved in the processing of personal data. In some cases the data protection responsibilities are shared, in particular when the same entity is involved at multiple stages, for example where the OS manufacturer also controls the app store.

There is also a role for end users to take appropriate responsibility, to the extent that they create and store personal data through their mobile devices. If such processing serves purely personal or household purposes, the Data Protection Directive would not apply (Article 3(2)) and the user would be exempt from the formal data protection obligations. If users however decide to share data via the app, for instance by making information public to an indefinite number of people[19] using a social network app, they process information beyond the conditions of the household exemption.[20]

3.3.1 App developers

App developers create apps and/or make them available to end users. This category includes private and public sector organisations that outsource the app development and those companies and individuals building and deploying apps. They design and/or create the software which will run on the smartphones and thus decide the extent to which the app will access and process the different categories of personal data in the device and/or through remote computing resources (app developers' or third parties' computing units).
To the extent the app developer determines the purposes and means of the processing of personal data on smart devices, he is the data controller as defined in Article 2(d) of the Data Protection Directive. In that case, he has to comply with the provisions of the entire Data Protection Directive. The key provisions are explained in paragraphs 3.4 to 3.10 of this opinion.

Even when the household exemption applies to a user, the app developer would still be responsible as data controller if he processes the data for his own purposes. This is for example relevant when the app requires access to the entire address book in order to deliver the service (instant messaging, phone calls, video calls).

---

[17] The Working Party uses the common terminology of app developers, but emphasises that the term is not limited to the programmers or technical developers of apps, but includes the app owners, that is, companies and organisations that commission the development of apps and determine their purposes.

[18] In some instances, the manufacturer of the OS overlaps with the device manufacturer, whereas in other cases the device manufacturer is a different company from the OS supplier.

[19] See cases European Court of Justice, Case C-101/01 Criminal proceedings against Bodil Lindqvist, judgment of 6 November 2003 and Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, judgment of 16 December 2008.

[20] See WP29 Opinion 5/2009 on online social networking (June 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

The responsibilities of the app developer will be considerably limited if no personal data are processed and/or made available outside the device, or if the app developer has taken appropriate technical and organisational measures to ensure that data are irreversibly anonymised and aggregated on the device itself, prior to any data leaving the device.

In any case, if the app developer gains access to information that is stored on the device, the ePrivacy directive also applies and the app developer must comply with the consent requirement stipulated in Article 5(3) of the ePrivacy directive.

To the extent that the app developer has outsourced some or all of the actual data processing to a third party and that third party assumes the role of a data processor then the app developer must comply with all obligations related to the use of a data processor. This would also include the use of a cloud computing provider (e.g. for external data storage).[21]

To the extent that the app developer allows for the access of user data by third parties (such as an ad network accessing the geo location data of the device in order to deliver behavioural advertising) it must employ appropriate mechanisms to comply with the applicable requirements under the EU legal framework. If the third party accesses data stored in the device, the obligation to obtain informed consent of Article 5(3) of the ePrivacy Directive applies. Furthermore, if the third party processes personal data for its own purposes, it may also be a joint data controller with the app developer and must therefore ensure respect of the purpose limitation principle, and security obligations[22] for the part of the processing for which it determines purposes and means. As different types of arrangements - both commercial and technical - may exist between app developers and third parties, the respective responsibility of each party will have to be established on a case-by-case basis having regard to the specific circumstances of the processing involved.

An app developer may use third party libraries with software that provides common functionalities, such as for example a library for a social gaming platform. The app developer must ensure users are aware of any data processing undertaken by such libraries and if that is the case, that such data processing is compliant with the EU legal framework, including where relevant, by obtaining the consent of the user. In that sense, app developers must prevent use of functionalities that are hidden from the user.

3.3.2 OS and device manufacturers

The OS and device manufacturers should also be considered as data controllers (and where relevant, as joint controllers) for any personal data which is processed for their own purposes such as the smooth running of the device, security etc. This would include user generated data (e.g. user details at registration), data automatically generated by the device (e.g. if the device has a 'phone home' functionality for its whereabouts) or personal data processed by the OS or device manufacturer resulting from the installation or use of apps. Where the OS or device

[21] See WP29 Opinion 05/2012 on Cloud Computing (July 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[22] See WP29 Opinion 2/2010 on online behavioural advertising (June 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf and WP29 Opinion 1/2010 on the concepts of "controller" and "processor" (February 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

manufacturer provides additional functionality such as a back-up or remote locate facility they would also be the data controller for personal data processed for this purpose.

> Apps that require access to geolocation must use the location services of the OS. When an app uses geolocation, the OS may collect personal data to provide the geolocation information to the apps, and may also consider using the data to improve its own location services. For this latter purpose, the OS is the data controller.

The OS and device manufacturer are also responsible for the application programming interface (API) which enables the processing of personal data by apps on the smart device. The app developer will be able to access those features and functions which the OS and device manufacturers make available through the API. Since the OS and device manufacturers determine the means of (and extent of) access to personal data, they must ensure that the app developer has sufficient granularity of control so that access is granted only to those data that are necessary for the functioning of the app. The OS and device manufacturers should also ensure that this access can be revoked in a simple and effective manner.

The concept of "privacy by design" is an important principle which is indirectly referred to already in the Data Protection Directive[23] and which, together with "privacy by default" emerges more clearly in the ePrivacy Directive.[24] It requires from the manufacturers of a device or an application to embed data protection from the very beginning of its design. Privacy by design is explicitly required for the design of telecom equipment, as provided under the radio and telecom terminal equipment directive.[25] Therefore, OS and device manufacturers, together with the app stores have an important responsibility to provide safeguards for the protection of personal data and privacy of app users. This includes ensuring the availability of appropriate mechanisms to inform and educate the end user about what the apps can do and what data they are able to access, as well as providing appropriate settings for app users to change the parameters of the processing.[26]

3.3.3 App stores

Each of the most widely used types of smart device has its own app store and it often is the case that a particular OS is deeply integrated with a particular app store. App stores often process upfront payments for apps and can also support in-app purchases and therefore require user registration with name, address and financial data. These (directly) identifiable data may be combined with data about the purchase and usage behaviour and with data read from, or generated by, the device (such as unique identifiers). For the processing of such personal data app stores are likely to be the data controller, including if they report such

---

[23] See recital 46 and Article 17.

[24] See Article 14(3)

[25] Directive 1999/5/EC of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity. L 91/10 Official Journal of the European Communities, 7.4.1999. Article 3.3 (c) stipulates that the European Commission may decide that end user devices shall be so constructed that they incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.

[26] The Working Party welcomes the recommendations of the FTC in this respect, in the staff report Mobile Privacy Disclosures referred to in note 6 supra, for example on page 15: "(…) *platforms are in a unique position to provide consistent disclosures across apps and are encouraged to do so. Consistent with workshop comments, they could also consider making these disclosures at multiple points in time (…).*"

information back to the app developers. Where the app store processes an end user's app download or usage history or similar facility to restore previously downloaded apps, they would also be the data controller for personal data processed for this purpose.

An app store records login credentials as well as the history of previously bought apps. It also asks the user to provide a credit card number that will be stored with the account of the user. The app store is the data controller for these operations.

On the contrary, websites that allow the download of an app to be installed on the device without any authentication may find that they are not processing any personal data.

App stores are in an important position to enable app developers to deliver adequate information about the app, including the types of data the app is able to process and for what purposes. App stores can enforce these rules by their admission policy (based on either ex ante or ex post controls). In collaboration with the OS manufacturer, the app store can develop a framework to enable app developers to deliver consistent and meaningful information notices (such as symbols representing certain kinds of access to sensory data) and display these prominently in the app store catalogue.

3.3.4 Third parties

There are many different third parties involved in the data processing of data through the use of apps.

For example, many free apps are paid for by advertising which can be, but not limited to, contextual or personalised advertising, enabled by tracking facilities such as cookies or other device identifiers. Advertising may consist of a banner space within the app, out-of-app ads that are delivered by modifying browser settings or placing icons on the mobile desktop or delivered through a personalised organisation of the app content (e.g. sponsored search results).

Advertising for apps is generally provided by advertising networks and similar intermediaries which may be linked with or be the same entity as the OS manufacturer or app store. As outlined in WP29 Opinion 2/2010,[27] online advertising often entails the processing of personal data as defined by Article 2 of the Data Protection Directive and interpreted by Article 29 Working Party.[28]

Other examples of third parties are analytics providers and communications service providers. Analytics providers enable app developers to gain insight in the use, popularity and usability of their apps. Communications service providers[29] may also have an important role in determining the default settings and security updates of many devices and may process data about the use of apps. Their customisation ("branding") might have consequences for the

[27] WP29 Opinion 2/2010 on online behavioural advertising (June 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[28] See also the interpretation of the concept of personal data in WP29 Opinion 4/2007 on the concept of personal data (June 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[29] Communications service providers are also subjected to sector-specific data protection obligations which are outside of the scope of this opinion.

possible technical and functional measures that the user can apply to protect his or her personal data.

Compared to app developers, third parties may have two types of roles: one is to execute operations for the app owner, for example to provide analytics within the app. In that case, when they act exclusively on behalf of the app developer and do not process data for their own purposes and/or share data across developers, they are likely to be operating as data processors.

The second role is to collect information across apps to supply additional services: provide analytics figures at a larger scale (app popularity, personalized recommendation) or avoid the display of the same ad to the same user. When third parties process personal data for their own purposes, they act as data controllers and therefore must comply with all applicable provisions from the Data Protection Directive.[30] In the case of behavioural advertising, the data controller must obtain valid user consent for the collection and processing of personal data, consisting for example of the analysis and combination of personal data, and the creation and/or application of profiles. As explained previously by the WP29 in the Opinion 2/2012 on online behavioural advertising such consent is best achieved through the use of a prior opt in consent mechanism.

A company provides metrics for app owners and advertisers through the use of trackers embedded, by the app developer, within apps. The trackers of the company are therefore able to be installed on many apps and devices. One of its services is to inform app developers what other apps are used by a user, through the collection of a unique identifier. The company defines the means (i.e. trackers) and purposes of its tools before offering them to app developers, advertisers and others and therefore acts as a data controller.

To the extent that third parties access or store information on the smart device they must comply with the consent requirement of Article 5(3) of the ePrivacy Directive.

In this context, it is important to note that on smart devices, users generally have limited possibilities to install software that would control the processing of personal data as it is common in the desktop web environment. As an alternative to using HTTP cookies, third parties often access unique identifiers to single out (groups of) users and serve them targeted services, including advertisements. Since many of these identifiers cannot be deleted or changed by users (such as IMEI, IMSI, MSISDN[31]and specific unique device identifiers added by the operating system) these third-parties have the potential to process significant amounts of personal data without the end user being in control.

[30] WP29 Opinion 2/2010 on online behavioural advertising, p. 10-11.
[31] Mobile Station Integrated Services Digital Network

3.4 Legal ground

In order to process personal data, a legal basis is required as enumerated in Article 7 of the Data Protection Directive. Article 7 distinguishes six legal grounds for data processing: the data subject's unambiguously given consent; the necessity for the performance of a contract with the data subject; to protect the vital interests of the data subject, the necessity for compliance with a legal obligation; (for public authorities) to perform a task carried out in the public interest and the necessity for legitimate (business) interests.

With regard to the storing of information, or the gaining of access to information already stored in the smart device, Article 5(3) of the ePrivacy Directive (i.e. the consent requirement for placing and retrieving information from a device) creates a more detailed limitation/restriction of the legal grounds that may be taken into account.

3.4.1 Consent prior to installation and processing of personal data

In case of apps, the principal applicable legal ground is consent. When installing an app, information is placed on the end-user device. Many apps also access data stored on the device, contacts in the address book, pictures, videos and other personal documents. In all those cases, Article 5(3) of the ePrivacy Directive requires consent from the user, having been provided with clear and comprehensive information, before the placing and retrieving of information from the device.

It is important to note the distinction between the consent required to place any information on and read information from the device, and the consent necessary to have a legal ground for the processing of different types of personal data. Though both consent requirements are simultaneously applicable, each based on a different legal basis, they are both subject to the conditions of having to be free, specific and informed (as defined in Article 2(h) of the Data Protection Directive). Therefore, the two types of consent can be merged in practice, either during installation or before the app starts to collect personal data from the device, provided that the user is made unambiguously aware of what he is consenting to.

Many app stores provide an opportunity for app developers to inform end users about the basic features of an app prior to installation and require a positive action from the user before the app is downloaded and installed (ie click an “install” button). Whilst such an action may, in some circumstances, fulfil the consent requirement of Article 5(3), it is unlikely to provide sufficient information in order to act as valid consent for the processing of personal data. This topic has been previously discussed by the WP29 in its Opinion 15/2011 on the definition of consent.[32]

In the context of smart devices, ‘freely given’ means that a user must have the choice to accept or refuse the processing of his personal data. Therefore if an app needs to process personal data, a user must be free to accept or refuse. The user should not be confronted with a screen containing a single 'Yes I accept' option in order to finish the installation. An option to ‘Cancel’ or otherwise halt the installation must be available.

[32] WP29 Opinion 15/2011 on the definition of consent (July 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

'Informed' means that the data subject must have the necessary information at his disposal in order to form an accurate judgement.[33] In order to avoid any ambiguity, such information must be made available before any personal data is processed. This includes data processing that could take place during installation, for example, for debugging or tracking purposes. The content and form of such information is elaborated in paragraph 3.7 of this Opinion.

'Specific' means that the expression of will must relate to the processing of a particular data item or a limited category of data processing. It is for this reason that simply clicking an "install" button cannot be regarded as valid consent for the processing of personal data due to the fact that consent cannot be a generally formulated authorisation. In some cases users are able to give a granular consent, where consent is sought for each type of data the app intends to access.[34] Such an approach achieves two important legal requirements, firstly of adequately informing the user about important elements of the service and secondly asking for specific consent for each.[35] The alternative approach of an app developer asking its users to accept a lengthy set of terms and conditions and/or privacy policy does not constitute specific consent.[36]

Specific also relates to the practice of tracking user behaviour by advertisers and any other third party. The default settings provided by OSs and apps must be such as to avoid any tracking, to allow users to give specific consent to this type of data processing. These default settings may not be circumvented by third parties, as is currently often the case with "Do Not Track" mechanisms implemented in browsers.

Examples of specific consent

An app provides information about nearby restaurants. To be installed the app developer must seek consent. To access the geolocation data, the app developer must separately ask for consent, e.g. during installation or prior to accessing the geolocation.
Specific means that the consent must be limited to the specific purpose of advising the user about nearby restaurants. The location data from the device may therefore only be accessed when the user is using the app for that purpose. The user's consent to process geolocation data does not allow the app to continuously collect location data from the device. This further processing would require additional information and separate consent.

Similarly, for a communication app to access the contact list, the user must be able to select contacts that the user wishes to communicate with, instead of having to grant access to the entire address book (including contact details of non-users of that service that cannot have consented to the processing of data relating to them).

---

33 Idem, p. 19.

34 Granular consent means that individuals can finely (specifically) control which personal data processing functions offered by the app they want to activate.

35 The need for such granular consent is also expressly endorsed by the FTC staff in its most recent report (note 6 supra), p. 15-16: "(…) *platforms should consider providing just-in-time disclosures and obtaining affirmative express consent for collection of other content that many consumers would find sensitive in many contexts, such as photos, contacts, calendar entries, or the recording of audio or video content.*"

36 Idem, p 34-35: '*General consent without a precise indication of the aim of the processing to which the data subject agrees does not comply with this requirement. That means that the information about the goal of the processing must not be included in the general provisions but in a separate consent clause.*

It is important to note however that even if the consent meets the three elements described above, it is not a license for unfair and unlawful processing. If the purpose of the data processing is excessive and/or disproportionate, even if the user has consented, the app developer will not have a valid legal ground and would likely be in violation of the Data Protection Directive.

Example of excessive and unlawful data processing

An alarm clock app offers an optional feature whereby the user can give a verbal command to silence or 'snooze' the alarm. In this example, the consent for recording would be limited to whilst the alarm is sounding. Any monitoring or recording or audio whilst the alarm is not sounding would likely be considered as excessive and unlawful.

In the case of apps installed on the device by default (prior to the end user taking ownership) or other processing undertaken by the OS which rely on consent as a legal basis, the data controllers must carefully consider whether or not this consent is truly valid. In many cases, a separate consent mechanism should be considered, perhaps when the app is first run, in order to give the data controller sufficient opportunity to fully inform the end user. When the data are special categories of data, as defined in Article 8 of the Data Protection Directive, the consent must be explicit.

Last but not least, users must be given the opportunity to withdraw their consent in a simple and effective manner. This will be elaborated in section 3.8 of this Opinion.

3.4.2 Legal grounds for data processing during usage of the app

As explained above, consent is the necessary legal ground to permit the app developer to lawfully read and/or write information and consequently process personal data. In a subsequent phase, during the usage of the app, the app developer may invoke other legal grounds for other types of data processing, so long as this does not involve processing of sensitive personal data.

Such legal grounds may be the necessity for the performance of a contract with the data subject or the necessity for legitimate (business) interests, Article 7(b) and (f) of the Data Protection Directive.

These legal grounds are limited to the processing of non-sensitive personal data of a specific user, and can only be invoked to the extent a certain data processing is strictly necessary to perform the desired service or, in the case of Article 7(f), only if such interests are not overridden by the interests for fundamental rights and freedoms of the data subject.

Examples of contractual legal ground

A user consents to the installation of a mobile banking app. In order to fulfil a request to make a payment the bank does not have to ask for the separate consent of the user to disclose his name and bank account number to the recipient of the payment. This disclosure is strictly necessary in order to perform the contract with this specific user, and therefore the bank has a legal ground in Article 7 (b) of the Data Protection Directive. The same reasoning applies to communication apps; when they provide essential information such as an account name, e-mail address or phone number to another individual that the user wishes to communicate with, the disclosure is obviously necessary to perform the contract.

3.5 Purpose limitation and data minimisation

Fundamental principles underlying the Data Protection Directive are purpose limitation and data minimisation. Purpose limitation enables users to make a deliberate choice to trust a party with their personal data as they will learn how their data are being used, and will be able to rely on the limitative purpose description to understand for what purposes their data will be used. The purposes of the data processing therefore need to be well-defined and comprehensible for an average user without expert legal or technical knowledge.

At the same time, purpose limitation requires that app developers have a good overview of their business case before they start to collect personal data from users. Personal data may only be processed for fair and lawful purposes (Article 6(1)a of the Data Protection Directive) and these purposes must be defined before the data processing takes place.

The purpose limitation principle excludes sudden changes in the key conditions of the processing.

For example, if an app originally had as purpose to allow users to e-mail each other, but the developer decides to changes its business model and merges the e-mail addresses of its users with the telephone numbers of users of another app. The respective data controllers would then have to individually approach all users and ask for their prior unambiguous consent for this new purpose of their personal data processing.

Purpose limitation goes hand-in-hand with the principle of data minimisation. In order to prevent unnecessary and potentially unlawful data processing, app developers must carefully consider which data are strictly necessary to perform the desired functionality.

Apps can obtain access to many of the functionalities in the device, and are therefore capable to do many things like sending a stealth SMS, accessing images and the entire address book. Many app stores support (semi) automated updates where the app developer can integrate new features and make those available with little or no interaction by the end user.

The Working Party emphasises at this point that third parties obtaining access to the user data through the apps must respect the principles of purpose limitation and data minimization. Unique, often unchangeable, device identifiers should not be used for the purpose of interest based advertising and/or analytics, due to the inability of users to revoke their consent. App developers should ensure that function creep is prevented by not changing the processing from one version of an app to another without giving the end users appropriate information notices and opportunities to withdraw from either the processing or the entire service. Users should also be offered the technical means to verify statements about declared purposes, by allowing them access to information about the amounts of outgoing traffic per app, in relation to user-initiated traffic.

Information and user controls are the key features to ensure the respect of the principles of data minimisation and purpose limitation.

Access to the underlying data on the device through the APIs gives OS and device manufacturers and app stores an opportunity to enforce specific rules and offer appropriate information to end users. For example, the OS and device manufacturers should offer an API

with precise controls to differentiate each type of these data and ensure that app developers can request access to only those data that are strictly necessary for the (lawful) functionality of their app. The types of data requested by the app developer can then be clearly displayed in the app store to inform the user prior to installation.

In this regard, control over the access to data stored in the device relies on different mechanisms:

a. OS and device manufacturers and app stores define **rules** that apply to submit apps in their app store: app developers must respect these rules or risk not being available in these stores.[37]
b. Operating Systems' **APIs** define standard methods to access the data stored in the telephone to which apps have access. They also have an impact on the collection of data on the server side.
c. **Ex-ante controls** - controls in place before installing an app.[38]
d. **Ex-post controls** - controls implemented after having installed an app.

3.6 Security

Following article 17 of the Data Protection Directive data controllers and processors must take the necessary organisational and technical measures to ensure the protection of the personal data they process. As a result, measures have to be taken by all actors identified in section 3.3, each according to their role and responsibility.

The goal of compliance with the security obligation is twofold. It will empower users to more stringently control their data, and enhance the level of trust in the entities that actually handle users' data.

In order to comply with their respective security obligations as data controllers, app developers, app stores, OS and device manufacturers and third parties have to take the principles of privacy by design and by default into account.. This requires an ongoing assessment of both existing and future data protection risks, and implementation and evaluation of effective mitigating measures, including data minimisation.

App developers

There are many publicly available guidelines regarding the security of mobile apps published by OS and device manufacturers and independent third parties, for example from ENISA.[39]

It is outside of the scope of this opinion to review all best security practices in the development of apps; however the Working Party takes this opportunity to review those that have a potentially grave impact on app users' fundamental rights.

---

[37] Jailbroken devices allow installation of apps outside official stores; Android devices also allow installation of apps from other sources.
[38] With the particular case of pre-installed apps.
[39] ENISA "Smartphone Secure Development Guideline": http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

An important decision before designing an app is the decision where the data will be stored. In some cases user data are stored on the device, but app developers may also use a client-server architecture. This means personal data are transferred or copied to the service provider's systems. Storing and processing data on the device gives the end users the greatest control over those data, for example allowing them to delete the data if they withdraw consent to its processing. However, securely storing data in a remote location can assist in data recovery following the loss or theft of a device. Intermediate methods are also possible.

App developers must identify clear-cut policies on how the software is developed and distributed. There is also a role for the OS and device manufacturers to promote secure processing by apps, which will be elaborated below. Secondly, app developers and app stores must design and implement a security-friendly environment, with tools to prevent malicious apps from spreading and allow each app to be installed/uninstalled easily.

Good practices which can be put in place during the design of an app include that of minimizing the lines and complexity of code, and implementing checks to exclude that data might be unintentionally transferred or compromised. In addition, all inputs should be validated to prevent buffer overflow or injection attacks. Other security mechanisms which are worth mentioning include adequate security patch management strategies, and performing regular, independent system security audits. Additionally, app design criteria should include the implementation of the principle of the least privilege by default, whereby apps are enabled to access only the data they really need to make a functionality available to the user. App developers and app stores should also encourage users, with warnings, to complement these good design practices by virtuous user practices, such as updating their apps to the latest available versions, and reminders to avoid the reuse of passwords across different services.

During the design stage of the app, app developers must also take measures to prevent unauthorised access to personal data by ensuring that data are protected both in transit and when stored, when applicable.

Mobile apps should run in specific locations within the memory of the devices (sandboxes[40]), in order to reduce the consequences of malware/malicious apps. In close collaboration with the OS manufacturer and/or app store, app developers must use available mechanisms that allow users to see what data are being processed by which apps, and to selectively enable and disable permissions. The use of hidden functionalities should not be allowed.

App developers must carefully consider their methods of user identification and authentication. They should not use persistent (device-specific) identifiers, but, instead, use low entropy app-specific or temporary device identifiers to avoid tracking users over time. Privacy-friendly authentication mechanisms should be considered. When authenticating users, app developers must give special care to the management of user-ids and passwords. The latter must be stored encrypted and securely, as a keyed cryptographic hash value. Making a test available to users on the robustness of chosen passwords is also a useful technique to encourage better passwords (entropy check). When appropriate (access to sensitive data, but also access to paid-for resources) re-authentication could be envisaged, also by means of multiple factors and different channels (e.g. access code sent by SMS) and/or the use of authentication data linked to the end user (rather than to the device). Also, when selecting

[40] A sandbox is a security mechanism to separate running programs.

session identifiers, unpredictable strings should be used, possibly in combination with contextual information such as date and time, but also IP address or geo-location data.

App developers should also be mindful of the requirements set forth in the ePrivacy directive with regard to personal data breaches and the need to proactively inform users. Whilst these requirements currently only apply to providers of publicly available electronic communications services it is expected that the obligation will be extended to all data controllers (and data processors) by way of the future Data Protection Regulation as per the Commission's proposals (COM 2012/0011/COD). This further reinforces the need to have and continuously evaluate a thorough "security plan" covering the collection, storage and processing of any personal data, to prevent such breaches from occurring and avoid incurring the heavy pecuniary penalties envisaged in such cases. The security plan, among others, must also provide for vulnerability management and for timely and secure release of reliable bug fixes.

The responsibility of app developers for the security of their products does not end with the delivery of a working version to the market. Apps may, as any software product, suffer from security flaws and vulnerabilities and app developers must develop fixes or patches for these and provide them to those players that can make them available to the users or do this themselves.

App stores

App stores are an important intermediary between end users and app developers and should include a number of robust and effective checks on apps before admitting them to the marketplace. They should provide information on the checks they are actually performing, and include information on what type of data protection compliance checks they carry out.

While this measure is not 100% effective in eliminating the dissemination of malicious apps, statistics show that this practice greatly reduces the occurrence of malicious functionalities in "official" app stores.[41] In order to cope with the large number of apps that are submitted on a daily basis this process might benefit from the availability of automatic analysis tools as well as from implementing information exchange channels between security experts and software professionals and effective procedures and policies to deal with reported issues.

In addition to the review of apps before admittance to the app store, apps should also be subjected to a public reputation mechanism. Apps should not just be rated by users for how "cool" they are, but also on the basis of their functionalities, with specific reference to privacy and security mechanisms. Also, reputation mechanisms should be engineered to prevent false ratings. Qualification and reputation mechanisms for apps can also prove effective in building mutual trust between the various entities, especially if data are exchanged through a long chain of third parties.

App stores often have implemented a method to remotely uninstall malicious or insecure apps. This mechanism, if not properly designed, might constitute a hindrance to empowering users to keep tighter control of their data. A privacy friendly means for an app store to remotely uninstall apps should therefore be based on information and user consent. Moreover,

[41] *"Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets"*, Y Zhou et al., Network and Distributed System Security Symposium (NDSS) 2012

from a more practical standpoint, feedback channels should be given to users to report security problems with their apps and on the effectiveness of any remote removal procedure.

Like app developers, app stores should be aware of future personal data breach notification obligations, and work closely together with app developers in order to prevent those breaches.

OS and device manufacturers

OS and device manufacturers are also an important player in the definition of minimum standards and best practice amongst app developers, not only in the security of the underlying software and APIs but also in the tools, guidance and reference material they make available. OS and device manufacturers should make available strong and well known encryption algorithms and support appropriate key lengths. They should also make strong and secure authentication mechanisms available for app developers (e.g. the use of certificates signed by trusted certification authorities to verify the authorisation of a remote resource). This would also avoid the need for app developers to develop proprietary authentication mechanisms. In practice this is often poorly implemented and may represent a serious vulnerability.[42]

The access to and processing of personal data by apps should be managed through API built-in classes and methods providing proper checks and safeguards. The OS and device manufacturers should ensure that methods and functions allowing access to personal data include features aiming to implement granular consent requests. Similarly, action should be taken in order to exclude or limit access to personal data by using low-level functions or other means that could circumvent controls and safeguards incorporated into APIs.

OS and device manufacturers must also develop clear audit trails into the devices such that end users can clearly see which apps have been accessing data on their devices.

All parties must respond quickly to security vulnerabilities in a timely fashion such that end users are not unnecessarily exposed to security flaws. Unfortunately, some OS and device manufacturers (and telecom operators when they distribute branded devices) fail to provide long-term support to versions of the OS leaving users unprotected against well-known security vulnerabilities. OS and device manufacturers, together with app developers, must provide end users with upfront information about the length of time they might expect regular security updates. They should also inform users as soon as possible if a security issue requires an update to fix.

Third parties

The above security features and considerations must also be applied by third parties when they collect and process personal data for their own purposes, foremost advertisers and analytics providers. This includes secure transmission and encrypted storage of unique device and app user identifiers and other personal data.

---

[42] It has recently been pointed out that the lack of visual security indicators for SSL/TLS usage and the inadequate use of SSL/TLS can be exploited to launch Man-in-the-Middle (MITM) attacks. The cumulative installed base of the apps with confirmed vulnerabilities against MITM attacks includes several million users according to recent research. "*Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security"*, Bernd Freisleben and Matthew Smith, 19th ACM Conference on Computer and Communications Security (ACM CCS 2012).

3.7 Information

3.7.1 The obligation to inform and the content required

According to Article 10 of the Data Protection Directive, each data subject has a right to know the identity of the data controller who is processing their personal data. Additionally, in the context of apps, the end user has the right to know what type of personal data is being processed and for what purpose the data are intended to be used. If the personal data of the user are collected from other actors in the app ecosystem (as described in section 3.3 of this Opinion), the end user, according to Article 11 of the Data Protection Directive, nonetheless has the right to be informed about such data processing, in the same manner as described. Therefore, if processing personal data the relevant data controller must inform potential users at the minimum about:

- who they are (identity and contact detail),
- the precise categories of personal data the app developer will collect and process,
- why (for what precise purposes),
- whether data will be disclosed to third parties
- how users may exercise their rights, in terms of withdrawal of consent and deletion of data).

Availability of this information on personal data processing is critical in order to obtain consent from the user for the data processing. Consent can only be valid if the person has first been informed about the key elements of the data processing. Providing such information only after the app has started to process personal data (which often starts during installation) is not deemed sufficient and is legally invalid. In agreement with the FTC staff report, the Working Party underlines the need to provide information at the point in time when it matters to consumers, just prior to the collection of such information by apps. Being told what data are being processed is particularly important given the broad access apps generally have to sensors and data structures on the device, where such access in many cases is not intuitively obvious. Adequate information is also of vital importance when the app processes special categories of personal data, e. g. on health condition, political beliefs, sexual orientation, etc. Finally, the app developer should clearly differentiate mandatory and optional information and the system should allow the user to refuse access to optional information using privacy friendly default options.

With regard to the identity of the data controller, users need to know who is legally responsible for the processing of their personal data and how that controller can be contacted. Otherwise they cannot exercise their rights, such as the right to access data (remotely) stored about them. Due to the fragmented nature of the app landscape, it is crucial that every app has a single point of contact, taking responsibility for all the data processing that takes place via the app. It must not be left to the end user to research the relations between app developers and other parties processing personal data through the app.

With regard to the purpose(s), end users must be adequately informed which data are collected about them and why. Users should also be made aware in clear and plain language whether the data may be reused by other parties, and if so, for what purposes. Elastic purposes such as 'product innovation' are inadequate to inform users. It should be plainly stated if users will be asked to consent to data sharing with third parties for advertising and/or analytics purposes. There is an important responsibility for the app stores to ensure that this information is available and easily accessible for each app.

There is an important responsibility for app stores to ensure appropriate information. The use of visual signifiers or icons regarding data uses is strongly recommended to make users aware of the types of data processing.

In addition to the above minimum scope of information, necessary in order to seek consent from the app user, the Working Party in view of fair processing of personal data strongly advises that the data controllers also provide to the users information on:

- proportionality considerations for the types of data collected or accessed on the device,
- retention periods of the data,
- security measures applied by the data controller.

The Working Party also recommends that app developers include information in their privacy policy dedicated to European users, how the app complies with European data protection law, including possible transfers of personal data from Europe to for example the USA, and whether and how the app, in that case, complies with the Safe Harbor framework.

3.7.2 The form of the information

The essential scope of information about data processing must be available to the users before app installation, via the app store. Secondly, the relevant information about the data processing must also be accessible from within the app, after installation.

As a joint controller with the app developers with regard to information, app stores must ensure that every app provides the essential information on personal data processing. They should check the hyperlinks to included pages with privacy information and remove apps with broken links or otherwise inaccessible information about the data processing.

The Working Party recommends that information about personal data processing is also available, and easy to locate, such as within the app store and preferably on the regular websites of the app developer responsible for the app. It is unacceptable that the users be placed in a position where they would have to search the web for information on the app data processing policies instead of being informed directly by the app developer or other data controller.

At the very least, every app should have a readable, understandable and easily accessible privacy policy, where all the above mentioned information is included. Many apps do not meet this minimum transparency requirement. According to the June 2012 FPF study, 56% of the paid apps do not have a privacy policy, and almost 30% of the free apps.

Apps which do not, or are not intended for the processing or personal data, should clearly state this within the privacy policy.

Of course, there are limitations to the amount of information that can be presented on a small screen, but this is no excuse to not adequately inform end users. Several strategies can be followed to ensure users' awareness of key elements of the service. The Working Party sees benefits in the use of layered notices as detailed by WP29 in Opinion 10/2004[43], where the

[43] WP29 Opinion 10/2004 on More Harmonised Information Provisions (July 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf

initial notice to the user contains the minimum information required by the EU legal framework, and further information is available through links to the whole privacy policy. The information should be presented directly on screen, easily accessible and highly visible. Next to comprehensive information suitable for the small screen of mobile devices, users must be able to link through to more extensive explanations, for example in the privacy policy, how the app uses personal data, who the data controller is and where a user can exercise his rights.

This approach may be combined with the use of icons, images, video and audio, and make use of contextual real time notification when an app accesses the address book or photos.[44] These icons have to be meaningful, i.e. clear, self-explaining and unambiguous. Clearly, the OS manufacturer has an important joint responsibility to facilitate the use of such icons.

In fact, app developers excel in programming and designing complex interfaces for small screens, and the Working Party calls on the industry to use this creative talent to deliver more innovative solutions to effectively inform users on mobile devices. In order to ensure that the information really is understandable to users without a technical or legal background, the Working Party (in line with the FTC staff report) strongly recommends consumer testing of chosen information strategies.[45]

3.8 Data subject's rights

Following Articles 12 and 14 of the Data Protection Directive, app developers and other data controllers in the mobile app ecosystem must enable app users to exercise their rights of access, rectification, erasure and their right to object to data processing. If a user exercises the right to access, the data controller has to provide the user with information about the data are being processed and on the source of those data. If the controller takes automated decisions based on the compiled data, the controller must also inform the user about the logic behind those decisions. This might be the case when users' performance or conduct is evaluated, for example based on financial data or health data, or other profile data. Subject to user request the app data controller also must enable rectification, erasure or blocking of personal data if they are incomplete, inaccurate or processed unlawfully.

In order for users to be able to exercise control over the processing of their personal data, apps must clearly and visibly inform their users about the existence of these access and correction mechanisms. The Article 29 Working Party recommends the design and implementation of simple but secure online access tools. Access tools should preferably be available within each app, or by offering a link to an online feature, where users can get instant access to all the data being processed about them and the necessary explanations thereof. Similar initiatives have been employed by online service providers, such as different dashboards and other access mechanisms.

The need for easy online access is especially high in case of apps that process rich user profiles, such as networking, social and messaging apps, or apps that process sensitive or financial data. Of course, access should only be granted if the identity of the data subject has been established, in order to prevent data leakage to third parties. However, this obligation to

[44] For example, the warning icon for geolocation processing used on iPhones.
[45] FTC staff report, note 6 supra, p. 16.

verify the correct identity should not lead to an additional, excessive collection of personal data about the data subject. In many cases, authentication could suffice, instead of (full) identification.

Additionally, users should always be provided with the possibility to withdraw their consent in a manner which is simple and not burdensome. A data subject may withdraw consent for data processing in a number of different ways and for a number of different reasons. Preferably the option of consent withdrawal should be available through the above mentioned easily accessible mechanisms. It must be possible to un-install apps and thereby remove all personal data, also from the servers of the data controller(s). In order to allow users to have their data deleted by the app developer, there is an important role for the OS manufacturer to provide a signal to the app developer once a user uninstalls the app. Such a signal could be provided through the API. In principle, after the user has uninstalled the app, the app developer does not have a legal ground to continue processing of the personal data relating to that user, and therefore has to delete all data. An app developer that wishes to keep certain data, for example in order to facilitate reinstallation of the app, has to separately ask for consent in the uninstall process, asking the user to agree to a defined extra retention period. The only exception to this rule is the possible existence of legal obligations to retain some data for specific purposes, for example fiscal obligations relating to financial transactions.[46]

3.9 Retention periods

App developers must consider the retention of data collected with the app and the data protection risks these pose. The specific timescales will depend on the purpose of the app and the relevance of the data to the end user. For example, a calendar, diary or photo sharing application would place the retention schedule into the control of the end user where for a navigation app it may suffice to store only the last 10 recently visited locations. App developers should also give consideration to the data of those users who have not used the app for an extended period of time. These users may have lost their mobile device, or switched to another device without actively uninstalling all apps on the initial device. App developers should therefore predefine a time period of inactivity, after which the account will be treated as expired and ensure that the user is informed of such a timescale. Upon expiry of this time period, the data controller should alert the user and give the user a chance to retrieve personal data. If the user doesn't respond to the alert, personal data relating to the user and usage of the app should be irreversibly anonymised or deleted. The reminder period depends on the purpose of the app and the location where the data are stored. If it concerns data stored on the device itself, for instance a high score in a game, the data may be kept as long as the app is installed. If it concerns data that are only used once per year, such as information on a ski resort, the reminder period could be 15 months.

[46] The Working Party reminds all information society services, such as apps, that the European data retention obligation (Directive 2006/24/EC) does not apply to them and therefore cannot be invoked as a legal ground to continue to process data about app users after they have deleted the app. The Working Party takes this opportunity to highlight the especially risky nature of traffic data, which deserve special precautions and safeguards *per* se – as highlighted in the WP29's Report on the enforcement of the Data Retention Directive (WP172) – where all the relevant stakeholders were called upon to implement the appropriate security measures.

3.10 Children

Children are avid users of apps, either on their own devices or on shared devices (e.g. those of their parents, siblings or in an education setting) and there is clearly a large and diverse market for apps targeted at children. But at the same time children have little or no understanding of and knowledge about the extent and sensitivity of the data to which apps may gain access, or the extent of data sharing with third parties for advertising purposes.

The Working Party has dealt with the issue of child data processing extensively in Opinion 2/2009 on the protection of children's personal data and only addresses a number of app-specific risks and recommendations in this paragraph.[47]

App developers and other data controllers should pay attention to the age limit defining children or minors in national legislation, where parental consent to data processing is a precondition to lawful data processing by apps.[48]

When consent can legally be obtained from a minor, and the app is intended to be used by a child or a minor, the data controller should pay attention to the minor's potentially limited understanding of and attention for information about data processing. Because of their general vulnerability, and taking into account that personal data must be processed fairly and lawfully, data controllers aiming at children should even more strictly respect the principles of data minimization and purpose limitation. Specifically, data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing.

The Working Party shares the concerns expressed by the Federal Trade Commission in its staff report on mobile apps for kids.[49]

App developers, in collaboration with app stores and OS and device manufacturers, should present the relevant information in a simple manner, in age specific language. The data controllers should also specifically refrain from any collection of data relating to the parents or family members of the child user, such as financial information or information about special categories of information, such as medical data.

---

[47] WP 160, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) (11 february 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf

[48] In the EU Member States the age limits spans from 12 to 18 years old.

[49] FTC staff report Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (Feb. 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf. "*While staff encountered a diverse pool of apps for kids created by hundreds of different developers, staff found little, if any, information in the app marketplaces about the data collection and sharing practices of these apps.* "

4 Conclusions and recommendations

Many types of data available on a smart mobile device are personal data. The relevant legal framework is the Data Protection Directive, in combination with the specific consent-requirement contained in Article 5(3) of the ePrivacy directive. These rules apply to any app targeted to app users within the EU, regardless of the location of the app developer or app store.

The fragmented nature of the app ecosystem, the wide range of technical access possibilities to data stored in or generated by mobile devices and the lack of legal awareness amongst developers create a number of serious data protection risks for app users. These risks range from a lack of transparency and lack of awareness amongst app users to poor security measures, invalid consent mechanisms, a trend towards data maximisation and elasticity of data processing purposes.

There is an overlap of data protection responsibilities between the different parties involved in the development, distribution and technical capabilities of apps. Most conclusions and recommendations are aimed at app developers (in that they have the greatest control over the precise manner in which the processing is undertaken or information presented within the app), but often, in order for them to achieve the highest standards of privacy and data protection, they have to collaborate with other parties in the app ecosystem, such as the OS and device manufacturers, the app stores and third parties, such as analytics providers and advertising networks.

App developers must

- Be aware of, and comply with, their obligations as data controllers when they process data from and about users;
- Be aware of, and comply with, their obligations as data controllers when they contract with data processors such as if they outsource the collection and processing of personal data to developers, programmers and for example cloud storage providers;
- Ask for consent before the app starts to retrieve or place information on the device, i.e., before installation of the app. Such consent has to be freely given, specific and informed;
- Ask for granular consent for each type of data the app will access; at least for the categories Location, Contacts, Unique Device Identifier, Identity of the data subject, Identity of the phone, Credit card and payment data, Telephony and SMS, Browsing history, Email, Social networks credentials and Biometrics;
- Be aware that consent does not legitimise excessive or disproportionate data processing;
- Provide well-defined and comprehensible purposes of the data processing in advance to installation of the app, and not change these purposes without renewed consent; provide comprehensive information if the data will be used for third party purposes, such as advertising or analytics;
- Allow users to revoke their consent and uninstall the app, and delete data where appropriate;
- Respect the principle of data minimisation and only collect those data that are strictly necessary to perform the desired functionality;
- Take the necessary organisational and technical measures to ensure the protection of the personal data they process, at all stages of the design and implementation of the app (privacy by design), as defined in in section 3.6 of this Opinion;
- Provide a single point of contact for the users of the app;

- Provide a readable, understandable and easily accessible privacy policy, which at a minimum informs users about:
  — who they are (identity and contact details),
  — what precise categories of personal data the app wants to collect and process,
  — why the data processing is necessary (for what precise purposes),
  — whether data will be disclosed to third parties (not just a generic but a specific description to whom the data will be disclosed),
  — what rights users have, in terms of withdrawal of consent and deletion of data;
- Enable app users to exercise their rights of access, rectification, erasure and their right to object to data processing and inform them about the existence of these mechanisms;
- Define a reasonable retention period for data collected with the app and predefine a period of inactivity after which the account will be treated as expired;
- With regard to apps aimed at children: pay attention to the age limit defining children or minors in national legislation, choose the most restrictive data processing approach in full respect of the principles of data minimization and purpose limitation, refrain from processing children's data for behavioural advertising purposes, either directly or indirectly and refrain from collecting data through the children about their relatives and/or friends.

The Working Party recommends that app developers

- Study the relevant guidelines with regard to specific security risks and measures;
- Proactively inform users about personal data breaches along the lines of the requirements of the ePrivacy Directive;
- Inform users about their proportionality considerations for the types of data collected or accessed on the device, the retention periods of the data and the applied security measures;
- Develop tools to enable users to customise retention periods for their personal data based on their specific preferences and contexts, rather than offering pre-defined retention terms;
- Include information in their privacy policy dedicated to European users;
- Develop and implement simple but secure online access tools for users, without collecting additional excessive personal data;
- Together with the OS and device manufacturers and app stores use their creative talent to develop innovative solutions to adequately inform users on mobile devices, for example through a system of layered information notices combined with meaningful icons.

App stores must

- Be aware of, and comply with, their obligations as data controllers when they process data from and about users;
- Enforce the information obligation of the app developer, including the types of data the app is able to access and for what purposes, as well as whether the data is shared with third parties;
- Give special attention to apps directed at children to protect against the unlawful processing of their data, and especially enforce the obligation to present the relevant information in a simple manner, in age specific language;
- Provide detailed information on the app submission checks they actually perform, including those aimed to assess privacy and data protection issues.

The Working Party recommends that app stores

- In collaboration with the OS manufacturer, develop control tools for users, such as symbols representing access to data on and generated by the mobile device;
- Subject all apps to a public reputation mechanism;

- Implement a privacy friendly remote uninstall mechanism;
- Provide feedback channels to users to report privacy and/or security problems;
- Collaborate with app developers to pro-actively inform users about personal data breaches;
- Warn app developers about the specificities of European law before submitting the application in Europe, for example about the consent requirement and in case of transfers of personal data to non-EU countries.

OS and device manufacturers must

- Update their APIs, store rules and user interfaces to offer users sufficient control to exercise valid consent over the data processed by apps;
- Implement consent collection mechanisms in their OS at the first launch of the app or the first time the app attempts to access one of the categories of data that have significant impact on privacy;
- Employ privacy by design principles to prevent secret monitoring of the user;
- Ensure security of processing;
- Ensure (the default settings of) pre-installed apps are compliant with European data protection law;
- Offer granular access to data, sensors and services, in order to ensure that the app developer can only access those data that are necessary for his app;
- Provide user-friendly and effective means to avoid being tracked by advertisers and any other third party. The default settings must be such as to avoid any tracking;
- Ensure the availability of appropriate mechanisms to inform and educate the end user about what the apps can do and what data they are able to access;
- Ensure that each access to a category of data is reflected in the information of the user before the app's installation : the categories presented must be clear and comprehensible;
- Implement a security-friendly environment, with tools to prevent malicious apps from spreading and allow each functionality to be installed/uninstalled easily.

The Working Party recommends that OS and device manufacturers

- Enable users to uninstall apps, and provide a signal (for example through the API) to the app developer to enable deletion of the relevant user data;
- Systematically offer and facilitate regular security updates;
- Ensure that methods and functions allowing access to personal data include features aiming to implement granular consent requests;
- Actively help develop and facilitate icons alerting users to different data usage by apps;
- Develop clear audit trails into the devices such that end users can clearly see which apps have been accessing data on their devices and the amounts of outgoing traffic per app, in relation to user-initiated traffic.

Third parties must

- Be aware of, and comply with, their obligations as data controllers when they process personal data about users;
- Comply with the consent requirement determined in Article 5(3) of the ePrivacy Directive when they read or write data on mobile devices, in cooperation with the app developers and/or app stores, which essentially provide user with the information on the purposes of data processing;
- Not circumvent any mechanism designed to avoid tracking, as it currently often happens with the "Do Not Track" mechanisms implemented in browsers;

- Communications service providers, when they issue branded devices, must ensure the valid consent of users for pre-installed apps and take on board relevant responsibilities when contributing to determining certain features of the device and of the OS, e.g. when limiting the user's access to certain configuration parameters or filtering fix releases (security and functional ones) provided by the device and OS manufacturers;
- Advertising parties must specifically avoid delivering ads outside the context of the app. Examples are delivering ads by modifying browser settings or placing icons on the mobile desktop. Refrain from the use of unique device or subscriber identifiers for the purpose of tracking;
- Refrain from processing children's data for behavioural advertising purposes, either directly or indirectly. Apply appropriate security measures. This includes secure transmission and encrypted storage of unique device and app user identifiers and other personal data.

The Working Party recommends that third parties

- Develop and implement simple but secure online access tools for users, without collecting additional excessive personal data;
- Only collect and process data that are consistent with the context where the user provides the data.

Done at Brussels, on 27 February 2013

For the Working Party
The Chairman
Jacob KOHNSTAMM