EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency

Shakila-Bu-Pasha, Anette Alén-Savikko, Jenna Mäkinen, Robert Guinness and Päivi Korpisaari*

Protection of privacy is currently a debated topic with regard to collecting and processing of location data via smartphones. This article seeks to discover whether meaningful protection of privacy is fostered by default location settings and the practice of seeking users’ permission by requiring approval of general terms and conditions, or if these instead cause users to unknowingly share location data. The article also asks whether such practices comply with human rights law and European Union (EU) data protection law. Moreover, the article discusses whether it is feasible to adopt transparent, explicit and specific steps to secure user privacy at all levels of smartphone usage, and argues that users should enjoy some control over personal data associated with smartphone usage, including location, and that this control should be executed under a legal arrangement which also secures users’ privacy and enables app developers’ or operating system providers’ lawful purposes with regard to processing location data.

I. Introduction

1. Topic Overview

Privacy is a critical concern in connection with smartphone applications (apps) and use of mobile devices in general around the world. Location privacy, in particular, is under scrutiny since other private information can be derived from location-related information.1 Location data privacy refers to the right not to be subjected to unauthorised collection, retention, use or distribution as well as processing of individual or organisational location data.2 The concept of location data privacy does not refer to hiding information – rather it safeguards one’s present or past location information from use for commercial or other purposes without one’s knowledge.3

Many smartphone and other mobile device users become reluctant to install apps or uninstall them after realizing that their personal data have been revealed to others due to the installation of certain apps.4 Furthermore, in many cases the mobile operating system (OS) itself collects data which may be considered personal data, and it may be imposs-

* Shakila-Bu-Pasha, Doctoral Student, Faculty of Law, University of Helsinki; Anette Alén-Savikko, Post-doctoral Researcher in Copyright Law, University of Helsinki; Jenna Mäkinen, Doctoral Researcher, Faculty of Law, University of Helsinki; Robert Guinness, Senior Research Scientist, Finnish Geospatial Research Institute, National Land Survey of Finland; Päivi Korpisaari, Professor in Communication Law, University of Helsinki. For correspondence: <shakila.bu-pasha@helsinki.fi>. The work is supported by the MyGeoTrust Project running under Department of Navigation and Positioning, Finnish Geospatial Research Institute, National Land Survey of Finland.


2 Location Forum, Location Data Privacy Guidelines, Assessments and Recommendations (Version 2; 1 May 2013).


ble due to OS restrictions to utilize the full functionality of the device’s hardware without enabling some data collection.

The right to privacy of smartphone users can be invaded in a variety of ways, for example by tracking web habits, monitoring contact lists, tracking location, examining files without the owner’s knowledge,7 and collecting technical information including IP addresses and other transaction data8. This article is focused particularly on privacy issues related to collecting and processing location data of individual users. In fact, many relevant stakeholders including mobile device manufacturers, online platform providers as well as OS and app store9 providers, location service providers, mobile app developers, Internet service providers (ISP), advertisers and governments or legislators can play an active role in collecting and processing user’s location data.8

Determining the location of a smartphone9, often known as positioning, can be accomplished using different methods. Some methods, such as those based on the Global Positioning System (GPS), perform positioning independently within the smartphone. In other methods, radio signals emitted by the smartphone are measured externally, and thus positioning can occur without any indication to the smartphone or user that such determination has taken place.10

At present Global Navigation Satellite System (GNSS)11, Global System for Mobile Communications (GSM)12 base stations and WiFi13 are the three main types of radio signals used for positioning in smartphones. While GNSS can be used as a ‘stand-alone’ positioning signal, typically positioning services based on GSM or WiFi require interaction between the smartphone and a commercial provider. In addition, an enhanced method, known as Assisted GNSS (A-GNSS), requires communication with a system operator, who is typically contracted by the smartphone manufacturer and the communications are routed through its servers. Most smartphone manufacturers refer to their proprietary positioning services based on GSM, WiFi, and A-GNSS as ‘location services’, and therefore this term is used below to refer to proprietary services that are used to determine the location of mobile devices. These interactions between a smartphone and location services prevent potential privacy issues concerning location data.

Although data protection has been discussed intensely in Europe in recent years, legislation on privacy aspects, particularly regarding location data collected via mobile apps and smartphones, is still developing. Analysing the legal aspect of collection, processing and protection of location data of smartphone users and keeping the EU at the core of the discussion, this article investigates the threat of privacy infringement and the efficacy of relevant EU legal provisions in addressing that threat. Aside from discussing relevant provisions of existing legal instruments, it also proposes steps to be taken by mobile app developers, mobile OS providers, Internet platforms and legislators for a transparent and accountable data protection system.

For the purpose of the topic, legal aspects can be examined from two angles:

(a) By analysing the related provisions of existing legislations drafted by the public authorities in order to secure the rights of data subjects, and bind with their provisions the private actors which may collect and process location data of data subjects, i.e., the human and fundamental rights and EU data protection regulations; and

---


7 App store refers to online stores for the distribution of software applications generally intended for mobile devices <https://www.techopedia.com/definition/27519/app-store> accessed 8 June 2016.

8 Location Data Privacy Guidelines (n 2) 17.

9 Much of the discussion in this article applies equally well to other mobile devices, such as tablets, but for simplicity we will focus on smartphones in the remainder of the article.

10 Minch (n 1).

11 GNSS refers to any satellite system that provides a global navigation (ie, positioning) service. GPS, operated by the US, is one particular GNSS, but other GNSSs are already operating or are under development by other actors. Most modern smartphones utilize radio signals from multiple GNSS. Importantly, the operator of a GNSS does not receive any information about the devices utilizing its signals.

12 GSM is a default global standard for wireless mobile communications mostly used in Europe and also many other parts of the world: <http://searchmobilecomputing.techtarget.com/definition/GSM> accessed 8 June 2016.

13 WiFi denotes a wireless networking technology that provides wireless Internet and network connections using radio waves: <http://www.webopedia.com/TERM/W/Wi_Fi.html> accessed 8 June 2016.
(b) By examining the *locus standi* of privacy policies and terms and conditions developed by different private actors, eg, OS providers as well as mobile app providers who collect location data.

However, this article includes both the public and private sector and their relationship with data subjects, since both of these two sectors operate to formulate legal obligations which require legal research and collaboration in order to protect location data privacy of smartphone users.

It is legally required of the app publishers to publish privacy policies concerning the possibility, reason and extent of personal data processing including location data.\textsuperscript{14} Legislation in many states demands the inclusion of a privacy policy for a mobile app when it involves access to any kind of personal information.\textsuperscript{15} A survey conducted in 2014 revealed that, among the 110 most popular free Android\textsuperscript{16} and iOS\textsuperscript{17} mobile apps, location data were transmitted via 33\% and 47\% of the apps, respectively.\textsuperscript{18} According to an other survey published in June 2012, almost 56\% of the paid apps and 30\% of the free apps did not have a privacy policy at all.\textsuperscript{19}

It is technically possible to monitor and collect location data secretly, which would constitute a gross violation of privacy.\textsuperscript{20} Tracking and managing location data is often associated with Big Data,\textsuperscript{21} so it is important to keep in mind that location data may be only one type of data within the context of many other types of data being collected about an individual. Fragments of data combined and monitored over time, can result in new personal data, which in many cases can be very sensitive. Along with the possibility of disclosing sensitive and private information, unlawful or unethical collection of location data may facilitate identity theft.\textsuperscript{22} These examples show that the user of location-based services (LBS)\textsuperscript{23}, whether he or she is aware of it or not, is vulnerable to various threats to his or her privacy and well-being.

When online platforms and mobile OSs, app developers or publishers are tending to process users’ location data, they have to do it in compliance with the law. One of the grounds for processing location data is to obtain ‘freely given’ consent as required under several legislations. Consent is an expression of the right to self-determination featured in European data protection law. This article discusses consent as a prerequisite for a transparent data protection system in processing location data.

2. Are Location Data Personal or Sensitive?

It is important to note that by collecting location data, app developers or other actors are able to deduce many types of personal information apart from merely location, such as religious or political affiliation. To give an example, if a person visits a church regularly or goes to a gay bar in the weekends, conclusions can be drawn about that person’s religion or sexual preferences. Because many privacy-protected attributes are uniquely associated with places or events, collecting data that show a person frequently visits a place or attends a particular event represents a powerful means to draw a comprehensive picture of an individual.

Generally, the term ‘location data’ comprises any information implicitly or explicitly referring to geographic or geospatial position.\textsuperscript{24} In order to understand the role of location data under various legal frameworks, it is important to distinguish between cases where location data constitute either personal data or sensitive data (ie, special category of personal data) from those cases where the data are effectively anonymised,\textsuperscript{25} thus not considered personal or sen-

\textsuperscript{14} Article 29 Data Protection Working Party (A29 WP), Opinion 02/2013 on apps on smart devices (27 February 2013), 24.

\textsuperscript{15} Zottola and Brutaker (n 6); see, eg, Press Release of State of California Department of Justice, Office of the Attorney General, Attorney General Kamala D. Harris Files Suit Against Delta Airlines for Failure to Comply with California Privacy Law (6 December 2012).


\textsuperscript{17} iOS is the OS of Apple that is used for the functioning of its mobile devices <http://www.gottabemobile.com/2014/08/09/what-is-ios/> accessed 8 June 2016.


\textsuperscript{20} A29 WP, Opinion 13/2011 on GeoLocation services on smart mobile devices (16 May 2011), 7.

\textsuperscript{21} A huge quantity of data which needs special management tools and includes data collected via different online activities over time: <http://www.pcmag.com/encyclopedia/term/62849/big-data> accessed 8 June 2016.

\textsuperscript{22} Location Data Privacy Guidelines (n 2) 12, 15, 16.

\textsuperscript{23} LBS include ‘applications that depend on the user location to provide a service/information that is relevant to the user’ <http://www.navipedia.net/index.php/Location_Based_Services> accessed 8 June 2016.

\textsuperscript{24} Location Data Privacy Guidelines (n 2) 7.

\textsuperscript{25} When identifying factors are removed from personal data, those become anonymised data. Further discussed in ch II (2).
sitive data. Location data may constitute one of the many types of personal data while, at the same time, location data may become sensitive data, because as discussed above, location data may be used to deduce other extremely extensive personal information, thus becoming sensitive data. In Article 4(1) of the General Data Protection Regulation (GDPR), location data is expressly mentioned as a factor by reference to which a person may be directly or indirectly identified, thus is recognised as an ‘identifier’ of personal data. This article focuses on location data when they constitute personal and/or sensitive data.

II. Location Data under Different Legal Framework

For a lawful purpose, EU law permits the processing of location data following strict and precise conditions, including protection of such data against misuse and respect for other rights of the data subjects, while improper collection and processing of location data could result in invasion of privacy.

1. Human and Fundamental Rights Law

The Charter of Fundamental Rights of the European Union (CFR) was recognised as EU primary law from 2009 by the Lisbon Treaty and accordingly considered legally binding and of similar value to the Treaties (Article 6 TEU). Respect for private and family life and right to personal data protection are guaranteed in Article 7 and Article 8, respectively. Article 8(2) of the CFR ensures the right of data subjects to access and rectify the collected personal data and permits processing of personal data with the consent of the data subjects on fair and specified grounds or for some lawful purposes. Article 52 provides limitations to the rights and freedoms under the Charter as well.

In a landmark judgment in the joined cases of Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärtner Landesregierung (C-594/12) and Others, the Grand Chamber of the Court of Justice of the European Union (CJEU) ruled the Data Retention Directive invalid on 8 April 2014; one of the grounds was infringement of the rights under Articles 7 and 8 of the CFR. The provisions of this Directive permitted mobile app providers to retain location data of individual users.

Article 8 of the European Convention on Human Rights (ECHR) guarantees the right to privacy, which includes privacy of Internet users as well. It has been established by the European Court of Human Rights (ECtHR) that violations of fundamental rights and freedoms guaranteed by the Convention...
occurring in the digital or online world can also be determined by the ECHR.\textsuperscript{41} Hence, the human and fundamental right to privacy enshrined both in the CFR and ECHR should be respected no matter where the threat of invasion comes from, including smartphones or mobile apps – and the same applies to location data.\textsuperscript{42}

However, the right to privacy is not an absolute right under Article 8 of the ECHR, and interference with this right by public authorities is allowed only for lawful reasons, such as for the protection of national security or economic wellbeing, public safety, health or morals, rights and freedoms of others, or prevention of other crimes. In \textit{Uzun v Germany}\textsuperscript{13}, the surveillance via GPS, and thereby processing and use of the applicant’s location data was decided as proportionate interference with the private life under Article 8 of the ECHR. As it was done by the State in order to combat terrorism, the surveillance measure without data subject’s consent amounted to the interests of national security and public safety and was ‘necessary in a democratic society’ in accordance with the exceptions provided in Article 8(2) of the ECHR.\textsuperscript{44}

2. EU Data Protection Law

Until the GDPR comes into effect in May 2018, the prime legislation in the EU targeting the protection of personal data is the Data Protection Directive\textsuperscript{45} (DPD), which is also applicable to smartphone devices and apps involving personal data processing.\textsuperscript{46} In particular, it applies to personal data processing when it is done automatically and constitutes a part of some filing system.\textsuperscript{47} Although the term ‘location data’ has not been specifically stated in the DPD, this piece of legislation is of utmost relevance since its provisions apply to the protection and processing of personal data, including location data regarded as such data, and also to the location data collected via mobile apps and smartphones. However, since the DPD was adopted in 1995, some important recent aspects of digitalised environment have not been sufficiently anticipated to fall within the scope of the legislation.\textsuperscript{48}

Hence, the Directive will be replaced by the GDPR, published in the Official Journal in spring 2016. The Regulation will secure a uniform data protection law for the EU Member States after a two-year transition period from its entry into force [20th day after official publication, cf Article 99(1)].\textsuperscript{49} This article makes references to the GDPR mainly in issues of particular relevance to the subject. No overall assessment of the reform is sought.\textsuperscript{50}

At the same time, some provisions of the Directive on privacy and electronic communications\textsuperscript{51} (e-Privacy Directive) as amended by Directive 2009/136/EC of the European Parliament and of the Council\textsuperscript{52} are very significant in addressing the location privacy issues of smartphone users. Aiming to protect personal data in the field of electronic communication networks and services, the e-Privacy Directive differentiates between traffic data and location data.\textsuperscript{53} According to the amended Article 3, the applicability of the e-Privacy Directive includes public communica-

\textsuperscript{41} See eg, Ashby Donald and others v France App no 36769/08 (ECHR, 10 January 2013).
\textsuperscript{42} See eg, Uzun v Germany App no 35623/05, IHRL 1838 (ECHR, 2 September 2010), 105a, note 816a Law Review 1701(1 data protection system when the GDPR comes into force where cell connected with the termina
\textsuperscript{43} ibid.
\textsuperscript{44} Council of Europe/European Court of Human Rights, Research Division, Internet: case-law of the European Court of Human Rights (2011, Updated: June 2015), 7.
\textsuperscript{46} A29 WP, Opinion 02/2013 (in 14) 7.
\textsuperscript{48} eg, AG Jääskinen, C-131/12 Google Spain et al v AEDP; Costaia Gonzales (CEU, 13 May 2014) ECJ1EU:C:2014:317, points 27, 30, 31, 61; C-103/01 Bodul Lindqvist ECJ1EU:C:2003:596, para 68; COM (2012) 9 final, 3.
\textsuperscript{50} Dimov (n 47).
\textsuperscript{52} OJ L 317/11.
\textsuperscript{53} Dimov (n 47).
tions networks that support personal data collection and processing, and identification devices. For instance, most tracking systems resort to public communications networks in their functions, and individuals may be directly targeted or tracked via personal devices, such as smartphones, which rely on public communications networks.

The e-Privacy Directive becomes relevant, for example, when a device manufacturer wants to upload data stored in a user’s device to its servers. According to Article 5(3) of the e-Privacy Directive, this means that the controller needs the user’s consent. But once the data are already uploaded on the controller’s servers and an application requires access to this information, it is not subject to the e-Privacy Directive but to the provisions of the DPD instead (further processing, Article 7 DPD). As per Recital 10 of the e-Privacy Directive, the applicability of the DPD extends to all perspectives relating to the protection of fundamental rights and freedoms in the electronic communications sector, all of which are not within the scope of applicability of the e-Privacy Directive. According to Article 1(2) of the latter, the provisions of the e-Privacy Directive ‘particularise and complement’ the relevant provisions of the DPD.\(^\text{54}\)

In pursuance of Recital 24 of the e-Privacy Directive, terminal equipment, such as smartphones, or any information stored in a mobile device should be considered as ‘private’ and be protected under the ECHR. Thereby, unauthorised tracking of location either through mobile carriers, mobile apps or mobile phone application programming interfaces (APIs)\(^\text{55}\) are considered a violation of the right to respect for private life protected under Article 8 of the ECHR.

When data are ‘processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service’, they are defined as ‘location data’ in Article 2(c) of the e-Privacy Directive. In addition, according to Recital 14, such data includes the ‘latitude, longitude and altitude of the user’s terminal equipment’.

As per Article 2(a) of the DPD, when a natural person is identified or identifiable via so-called identifiers specific to, for example, their identity of body, mind, economy, culture, society, the (accompanying) pieces of information are ‘personal data’ [see also Article 4(1) GDPR]. Many activities performed on smartphones, such as downloading applications or using web-based services, require registration with the user’s name, email address, physical address, or account number, which are identifying personal data. If those data are combined with location data, then location data easily become also personal data. Additionally, every smartphone has one or more unique identifiers, for example, the International Mobile Equipment Identity (IMEI)\(^\text{56}\), which can be used in the development of location services. Because of such identifiable and identifying pieces of information, users’ ‘personal location data are being disclosed with or without their knowledge.\(^\text{57}\)

Normally, national laws of the respective EU Member States are applicable in defining the activities of a data controller according to Article 4(1)(a) of the DPD with regard to processing personal data, and those provisions must be ‘pursuant to’ the DPD. The GDPR will provide a more uniform instrument. App developers can be defined as data controllers within the meaning of Article 2(d) of the DPD when the purposes and means of processing of personal (including location) data on smartphones are determined by them and thereby the provisions of the whole Directive are applicable to them\(^\text{58}\) [see Article 4(7) GDPR].

Location data can be processed by the mobile apps collecting it via smartphones independently from OS developers or the location infrastructure controllers.\(^\text{59}\) In this process, location data might be conveyed to apps after the OS collects it. If any OS uses that data to improve its own location services, then the OS would be considered as a data controller according to the definition of Article 2(d) of the DPD.\(^\text{60}\) Similarly, an app store will be deemed as the data controller when it keeps records of formerly bought apps with login credentials or credit card numbers of account holders of the apps.\(^\text{61}\) Thus the provisions of the DPD bind app developers, OSs and app stores,

---


\(^{55}\) APIs refer to a set of routines, protocols and tools in order to develop software applications <http://www.wikipedia.com/TERM/API.html> accessed 8 June 2016.

\(^{56}\) An IMEI is a number used by GSM networks to uniquely identify mobile devices <https://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity/> accessed 8 June 2016.

\(^{57}\) A29 WP, Opinion 13/2013 (n 20) 9, 10.

\(^{58}\) A29 WP, Opinion 02/2013 (n 14) 9.

\(^{59}\) A29 WP, Opinion 13/2013 (n 20) 12.

\(^{60}\) A29 WP, Opinion 02/2013 (n 14) 11.

\(^{61}\) ibid 12.
when they become data controllers within the definition of the DPD.

The principle of data minimization is prescribed in Article 6(1)(c) of the DPD and Article 5(1)(c) of the GDPR respectively in collecting and processing of personal data. Article 17 of the DPD and Article 32 of the GDPR respectively require the app developers and OS providers to arrange security measures for the protection of such data.62

At the same time, EU data protection laws also permit some exceptions to the right to data protection. If data are disclosed to the controller and data processing is necessary for the basic functionality of the apps, Article 7(f) of the DPD permits data processing based on legitimate interests so long as the fundamental rights of the data subject are ensured [see Article 6(1)(f) GDPR].

Although according to the aforementioned definitions of EU law, location data of individual users are ‘personal data’, anonymous location data is treated differently (see pseudonymous data63). When data are effectively anonymised so that they cannot be used to identify an individual, then normally such location data are not regarded as personal data.64 According to Recital 26 of the DPD, when a particular smartphone user is not identifiable, it is indeed not a legal requirement to apply ‘the principles of protection’.65 But it is important to note that even so-called anonymised location data, when combined with other types of information, may be possible in some cases to ‘reidentify’ and ‘deanonymise’ and be used to uniquely identify an individual, therefore it is not straight-forward to determine an appropriate level of anonymization.66 Recital 26 DPD clarifies that ‘to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.’ A similar view is also expressed in Recital 26 of the GDPR.

According to Article 3(2) of the DPD, its provisions regarding processing of personal data will not be applicable in case of public and state security, defence, and criminal law proceedings by a state [see also Article 2(2) GDPR]. Article 13(1) of the DPD also provides exemptions and restrictions to the right to personal data protection on similar grounds, as well as some additional grounds as those mentioned above. Following this provision, or to prevent ‘unauthorised use of the electronic communication system’, Article 15 of the e-Privacy Directive allows restrictions to the scope of the rights and obligations concerning location data, based on largely similar grounds.

III. Transparency and Consent: The Most Contested Requirements

Although many multinational technology companies have their own privacy policies, developer distribution agreements and end-users license agreements (EULAs), a lack of transparency exists about the nature, amount and purpose of and sometimes even threat concerning personal (including location) data processing of smartphones and mobile apps users.67

For example, there are strict procedures that app developers must follow before they qualify to sell their apps in the Apple App Store.68 Users of iPhones69 do not have any option but to agree with the terms and conditions of Apple, and in most cases the users do not know about the nature and volume of their personal data that is processed when installing and using apps on their iPhones.

In case of iOS, it is only possible to turn location services ON or OFF. If location services are turned OFF, then (according to Apple) no location data is collected by Apple (GPS, WiFi, or GSM), nor made available to apps. Where the user has turned location services to ON, then Apple receives anonymous location and WiFi data, and also chooses whether to determine location by GPS, WiFi, GSM, or some other means. There is no way to ‘opt out’ of this data processing when location services are turned on.

---

62 Kamala D Harris, Attorney General, California Department of Justice, Privacy on the Go, Recommendations for the Mobile Ecosystem (January 2013) 9, 10.
63 The GDPR expressly includes the concept of pseudonymisation (eg, arts 4, 25). Personal data are pseudonymised when identifying elements are replaced with some pseudonyms.
64 Handbook on European data protection law (n 33) 44.
67 Årenes and Nes (n 28) 5.
68 ‘Android vs. iOS vs. Windows Phone’ (mobidev, 8 February 2013) <http://mobidev.biz/blog/android_vs_ios_vs_windows_phone> accessed 8 June 2016.
69 iPhones are smartphones projected and marketed by Apple Inc. running special mobile OS of Apple <http://www.webopedia.com/TERM/iPhone.html> accessed 8 June 2016.
For its part, the Android OS provides different ‘modes’ for accessing location. In the mode ‘High accuracy’, Android uses either GPS, WiFi, or mobile networks (e.g., GSM) to estimate the location. In ‘Power saving’ mode Android uses only WiFi and mobile networks to estimate location (i.e., no GPS). In the mode ‘GPS only’ Android uses only GPS. In most Android phones, in order to use either the most ‘High accuracy’ or ‘Power saving’, the user must enable ‘Google’s location service’ while in order to enable Google’s location service, the user must consent to the collection of ‘anonymous location data’. Also, this process of requiring consent, may differ from phone to phone. Lastly, in Android there is a setting, buried in the ‘Advanced’ settings for WiFi, which says, ‘Always allow scanning: Let Google Location Service and other applications scan for WiFi networks, even when WiFi is off’. This setting is enabled by default and it is very probable that the majority of users are unaware that it exists.

The use of LBSs on smartphones is increasingly popular, with large market revenues fostering data collection, which exposes the user to various threats to privacy. Different mobile apps offer LBSs using different mobile OSs, accessing location data of the users. LBS includes diverse services, including navigation services, crowdsourced location information services, tagging location of content (e.g., photos) posted on the Internet, personal location history tracking and advertising based on location data.

Besides, by collecting other types of data, such as ID data, calendar data, accessing users’ cameras or microphones, using hardware in mobile phones like gyroscopes and accelerometers, the probability of being able to track users’ location without the use of GNSS, WiFi, or GSM is high. The total system for monitoring and processing location data involves ambiguity and lack of transparency and accountability, keeping it based on trust from the users’ side to the OSs and app developers as to the nature, extent and means of the whole process.

The app approval process of multinational technology companies, such as Apple and Google, and their EULAs are based on one-sided terms and conditions irrespective of international or regional data protection principles. This raises the question on how giant technology companies can disregard international and regional norms of privacy and data protection in their collection of user data. These OSs, using infrastructures such as GPS or WiFi to provide location services, should also be held legally responsible if they violate European data protection law. Such aspects require that the international community collaborate to ensure a transparent and safe electronic communication system.

1. Legal Provisions on Consent

Pursuant to Article 10 of the DPD, in case of personal location data processing, smartphone users are entitled to be informed about the identity of the OS provider, app publisher, or app developer as controller, the purposes of the data processing, and the recipients of that data, with the right to access and rectify the data. Article 7 of the DPD provides six lawful grounds under which personal data might be processed including when consent by the user is given ‘unambiguously’. Article 2(h) of the DPD states that, such consent shall be ‘freely given specific and informed’. Processing sensitive data, including cases where location data are considered sensitive data is to be prohibited but exceptions apply for instance where the data subject explicitly consents to the processing (Article 8 DPD).

The amended e-Privacy Directive also requires mobile network operators to follow the legal obligations, including to inform and take prior consent in providing particular services requiring base station data. Under Article 5(3) of the e-Privacy Directive, consent has to be obtained by providing ‘clear and comprehensive information’.

Article 9 of the e-Privacy Directive appears as an extensive provision addressing the processing of lo-
cation data. Consent is required regarding the type, purpose, extent and duration of data processing, and transmission of such data to third parties in relation to public electronic communications systems. According to Article 9(2), users or subscribers may refuse the processing of their location data for all separate connections or communications to the network or transmission.

Article 13 of the e-Privacy Directive states that the prior consent of subscribers is required in case of direct marketing using automatic calling machines, fax or emails. According to its Recital 40, the scope of intrusion to ‘privacy by unsolicited communications for direct marketing purposes’ has been extended with inclusion of SMS messages requiring the recipients’ ‘prior explicit consent’.

Being one of the most contested provisions, the GDPR intends to unify some aspects relating to consent and bring about some changes to the concept of consent by data subjects as well as accountability of data controllers or processors, even when sensitive data are not concerned. The GDPR notes that consent must be given by ‘clear affirmative’ action, and an electronic request must be clear and undisruptive (Recital 32). Along with Recital 32, Article 4(11) of the GDPR defines consent of the data subject which implies a ‘freely given, specific, informed and unambiguous’ sign of wishes, and will be in the nature of an agreement between the data processor and data subject concerning personal (incl. location) data processing with either a written statement or ‘clear affirmative action’. In the GDPR, consent is regarded as a justification both for processing in general [Article 6(1)(a)] and with regard to sensitive data, as in special categories of personal data on the condition of ‘explicitness’ (Article 9).

According to Article 7 of the GDPR, data controllers are required to be able to demonstrate that the data subjects have given the consent [Article 7(1)]. Consent must also be clearly distinguishable and easily accessible [Article 7(2)]. Moreover, consent must be withdrawable as easily as given [Article 7(3)], thus consent is assumed not to be freely given if there is no genuine free choice and no possibility of refusal or withdrawal. The same applies where no appropriate separation for different data processing operations exists or if the performance of a contract depends on the consent despite it being unnecessary for such performance [Article 7(4), Recitals 42, 43 GDPR].

2. Providing Notice and Seeking Consent

The first step to ensure a meaningful consent is to provide notice to the users about the way, extent and possibility of collection and processing of their location data. Such notice will enable them to take free and informed decisions, and guarantee meaningful control (Recital 7 GDPR) over that data. It is the responsibility of LBS providers to demonstrate users’ consent in an open and unambiguous way, and location data can only be collected as the notice prescribes. This ensures that users can get the feeling of confidence and control over their location data. LBS providers should arrange the notice in clear, understandable and standard language (Recital 42 GDPR), so that it remains applicable irrespective of the technology or devices that the customers use or the business policies that the different OSs adopt. Moreover, data protection should be taken into account early on in the development of LBS and implemented by design and by default (Article 25 GDPR).

The users should be informed with clear and adequate information to what purpose their location data would be used, and with whom the data would be shared including advertisers or any other third parties (see Articles 10, 11 DPD; Article 12-14 GDPR, etc).

The settings of the application should not be such that they expose location or other personal data by default. There must be some option provided by the mobile apps or OSs for the users either to accept or decline, thus to express their actual choice regarding processing of their location data. Failure to provide any option other than accepting the terms to complete the installation process and afterwards processing personal (including location) data would not be consonant with freely given consent.

Instead of formulating and conveying general comprehensive privacy policies and terms and conditions, describing data practices of those apps, and

---

80 GSMA, Privacy Design Guidelines for Mobile Applications (Mobile & Privacy, February 2012) 4 and A29 WP; Opinion 02/2013 (n 14) 15.
81 GSMA, Privacy Design Guidelines (n 80) 20.
82 A29 WP, Opinion 02/2013 (n 14) 14.
compelling the users to agree on certain default settings, there should be arrangements to provide distinct and ‘specific’ notification from the apps which may collect sensitive location data. In other words, because of the special characteristics of location data it is necessary to arrange them as a different set of terms, or at least, when combined with other terms, they should be kept conspicuously distinct and easily identifiable.\(^8\) Checklists can be prepared identifying the types of personal data which the particular app would collect to fulfil the purpose of its operations (Recital 32 GDPR). Terms and conditions, especially regarding these particular types of data processing, should be precise and short instead of long and descriptive.\(^4\) Every new and different use of location data not covered under the introductory notice should provide separate notice to the users asking their consent. The retention period of location data [Article 13(2)(a) GDPR] and possible extension of data retention should be disclosed to the users.\(^5\)

With respect to social media platforms, a request for permission regarding the disclosure of location-related information to other users, as well as a periodical reminder thereof by a notice with a simple statement, would be convenient for the users to express their consent. Also in case of irregular use of a LBS, the app should renew consent or remind users about the availability of their location data once a year. A reminder sent with some image or sign could be more expeditious and time-saving than a descriptive notice.\(^6\) The users should also be able to share their location data with a particular group of people.\(^7\)

Consent, once given, should not be regarded as consent forever. The data subjects should be able to withdraw their consent in a convenient way [Article 7(3) GDPR] and also delete previous location data permanently as prescribed by law (Article 12 DPD; Article 17 GDPR).\(^8\) Since the data subjects have rights over personal data, users should enjoy the liberty to terminate the LBS and their consent accordingly at any time.\(^9\)

In summary, informed consent is essential to ensure a fair and transparent system of location data processing.\(^10\)

3. Example

As an example, if an indoor mobile application is developed providing a location information service, more particularly information relating to nearby chain-stores, the following steps would be considered as standard practice in collecting and processing location data:

- In the course of installation of the app and when accessing the location of the users, there would be an arrangement to ask the consent separately;
- The app must mention the particular purpose, eg, making suggestions to the users about nearby chain-stores or other related information individually, and the location data from the mobile phone should only be collected when the app is used by the user for that specific purpose;
- Such consent would not authorise the app publishers to collect location data from the mobile phone repeatedly;
- In case of successive processing, informing the user distinctly for separate consent is required;
- If the app intends to access the contact list of the mobile phone of the user, there must be an option for the user to select particular contacts with whom he/she intends to communicate or share his/her location.\(^11\)

If a user makes available an important piece of information including account name, email address or phone number to other users in a mobile application that uses location, processing the data without asking a separate consent in certain circumstances [eg, to perform a contract under Article 7 (b) DPD] would be lawful.\(^12\) However, the form, content and methodology to get consent may differ depending upon the policies of different OSs and nature of LBSs.\(^13\)

Even after taking consent to access location data, the OSs and LBS providers should not retain location

\(^8\) CTIA, Best Practices and Guidelines (n 79) 3.
\(^4\) Harris, Privacy on the Go (n 62) 6-8.
\(^5\) CTIA, Best Practices and Guidelines (n 79) 3.
\(^6\) ibid 4.
\(^7\) ibid 6.
\(^8\) A29 WP, Opinion 13/2011 (n 20) 16.
\(^9\) CTIA, Best Practices and Guidelines (n 79) 4.
\(^11\) A29 WP, Opinion 02/2013 (n 14) 15.
\(^12\) ibid 16.
\(^13\) CTIA, Best Practices and Guidelines (n 79) 5.
data indefinitely [Article 6 DPD; Recital 39, Article 5(1)(e) GDPR]. If the business consideration is fulfilled, then such data should be destroyed or converted as unreadable or in special circumstances as anonymised data. There should be a convenient opportunity for users to report any abuse of their location data and proper redress against such abuse. 94 Most importantly, by complying with the relevant provisions of existing data protection laws, data processors can secure and process users’ location data lawfully. 95

IV. Conclusion

Without informing the users (or requiring them to ‘take it or leave it’), collecting their location data and monitoring personal activities on the Internet via smartphones – whether done by the State, mobile OS providers or mobile app developers – pose a serious threat to the right to privacy and personal data protection guaranteed under EU legislation. Unlawful and unfair interference with location data has a direct negative impact on privacy, which has a significant effect on the private lives of smartphone users and also of other individuals.

In order to secure and protect the location data and privacy of smartphone users from unauthorised access, use, disclosure or retention, some administrative, regulatory and technical procedures are required. 96 Privacy issues relating to location data obtained via mobile apps and mobile devices have not been sufficiently covered by existing EU data protection laws, despite the fact that smartphones are more vulnerable compared to other networking devices. 97 Most legal scholars tend to apply existing legal frameworks to deal with location data, even though the special nature of such data would require special legal consideration. The present privacy measures are not sufficiently consistent, broad and effective to handle, protect or manage smartphone users’ location data. 98

The processing of location data can be accomplished in a lawful and transparent way. In case of invasion of privacy, the role and responsibilities of different parties should be easily deduced from legal documents, which are unfortunately not yet comprehensive. 99 It is a matter of concern that most smartphone users are not well informed about the recipient, controller or processor of their location data as well as the nature and purpose of the data processing. It is neither unavoidable nor necessary to monitor smartphone users’ every activity, especially if it has no connection to the running of the respective apps. On the contrary, it is reasonable for people to expect that not all of their personal and location data are available and unsecured via their very personal smartphones.

Hence, it is high time to determine clear legal obligations about the availability of users’ location data when using apps and other functionalities on their smartphones. Few users read the terms and conditions of their smartphone apps thoroughly, and fewer understand the complex documents before installing apps on their devices. A transparent, accountable and interconnected legal system, involving both the terms and policies of mobile platforms and apps as well as EU data protection legislation, is essential for the promotion of secure online public participation via smartphones. In addition to the existing legal instruments designed to protect location data in association with other personal data or to protect location data in different electronic communication devices, there is a need to set up specific legal standards for the location data privacy in smartphones. All the responsible parties and stakeholders should be obliged to follow those standards when drafting their own privacy policies, terms and conditions, and laws. However, we can hope for a better data protection system under the GDPR (eg. fines, explicit processor duties, etc).

The GDPR has taken technological and other developments into account by adding more detail with respect to the previous framework from 1995. In the two years between now and the applicability of the Regulation [25 May 2018, see Article 99(2)], a huge amount of preparation needs to be done by the Member States and multinational technology companies,
and only the future will show whether it will have the intended effect.

Since the future of the new digitalised society is uncertain, it is impossible to foresee, whether the GDPR will solve the underlying data protection issues, such as truly increasing transparency and enhancing the data subject’s position. Although the benefit of greater certainty may be offered by specific definitions, they can also be criticised for being rigid and incapable of responding to new developments.