Press conference on 9 August 2012

AK: Careful with mobile phone apps--data is big business!

You are being informed by:
Gabriele Zgubic, Head of the Consumer Policy Department, Vienna Chamber of Labour
Daniela Zimmer, Consumer Policy Department, Vienna Chamber of Labour
Jaro Sterbik-Lamina, Study Author

Consumers need more protection: Put a stop to data-hungry mobile phone apps

DEADLINE FRI 9 AUGUST/11:00 A.M.

Smartphones and tablet computers are closely connected to their owners and almost like open books. The AK commissioned the Institute of Technology Assessment at the Austrian Academy of Sciences to carry out a study on this subject. It found that data collectors can use geographic data such as GPS coordinates or WLAN access points to track the location of the mobile device and the places they go. Apps in particular are increasingly causing a frenzy of collection activity. They often serve as facades, masking their actual purpose, which is to collect data. Advertising companies are frequently associated with the app vendors and obtain huge volumes of data.

“The data are real gold mines. There is a lively trade in data,” AK consumer advocates Gabriele Zgubic and Daniela Zimmer explained. “The app vendors sell the data to advertising firms for good money. These firms make intensive use of these data. As for consumers, they are usually not even aware of how they are being used; data transmission is not transparent. Consumers are becoming as transparent as glass in the process. Data protection regulations and privacy are often abused; app developers and device manufacturers often clean up.”

The AK called for more protection for consumers. Equipment and app vendors must provide better information. In addition, reliable protection programs must be installed on mobile phones. On another front, EU-wide standards are needed for data-hungry app collectors as well as measures against violations.

Where are you? Ask your phone!

In 2010 there were about 600 million smartphones in use around the globe and that figure continues to rise constantly. In fact, the annual growth rates are about 20 per cent. The AK commissioned the Institute of Technology Assessment at the Austrian Academy of Sciences to carry out a study entitled “Current Issues regarding Geographic Data Use on Mobile Communication Devices”. The study warns about the risk of being monitored by data-hungry apps. Various data collectors can use geographic data such as GPS coordinates or WLAN access points to track the location of users and the places they go.

Geographic data are getting wise to consumers

Databases (of providers such as Skyhook or Navizon) are employed to ascertain location. The smartphone sensor determines which UMTS mobile communication cells and WLAN points are in the vicinity. It sends this information to the database operators and receives the location data, i.e. longitude and latitude, postal code (district or section of a town, city, state, and country), street and house number in return. With repeated measurements, precise times and movement profiles (tracking; speed measurement) can even be calculated. This can be done, for instance, for emergency or geo-fencing apps in which an alarm is sounded, for example, in the case of car accidents or as soon as people or objects go beyond a prescribed radius.

Geographic data are used for navigation functions, for example, or social networks link geographic data with other information. For instance, Flickr links photos with geographic data or in the event of an emergency, geographic data help response teams to proceed to a certain address quickly, etc., etc., ... Besides smartphone makers and telecom providers, geographic data are also saved by app producers themselves and/or sent to third parties. “All of these services show what a fine line there is between use and the loss of personal liberty,” Zimmer noted.

Apps as data collectors

Apps are often busy collecting data. Along with location data, apps frequently have access to the device ID, e-mail and phone contacts and SIM card number, which they send to analysis service providers without even informing users they are doing so. Basically all “data treasures” in a smartphone are subject to snooping: saved address data, memento photos and all communication by phone.

Data-hungry apps pass data on to countless advertising networks, for example, often without even telling the users about it. The smart devices can be traced back quite accurately to one person and provide an ideal way for advertisers to draw up behavioural profiles. Free apps in particular often serve as facades to mask their actual purpose, namely data collection. For instance, Paper Toss, a simple game requiring no geographic data, transmits the location together with the phone ID to five international advertising networks.

Zimmer: “Many people are not aware that data are transmitted and what consequences that has. They need more protection. The internationally active device manufacturers and app (shop) vendors have to take greater responsibility to ensure modern data protection. It is also extremely difficult to enforce data protection rights. The vendors are often based overseas.”

Transparent consumers

Advertising networks provide app manufacturers with software add-ons that automatically integrate advertising in apps. These modules track not just the location data but also the time the customers spend using an app.
Actually, it is a subtle form of surveillance for more or less useful service and advertising purposes. Zimmer: “Because of the playful nature of apps, consumers do not perceive data collection as monitoring and are willing to reveal a lot about themselves.”

A growing industry is busy linking profiles of mobile phone users with other sets of data. Collectors are mainly concerned about processing, merging, analysing and re-selling additional data for marketing purposes. Zimmer: “The uses to which the collected data are put are very difficult to control–lively trade in data with third-party vendors is now a common practice.”

Who with whom

One of the biggest advertising networks is AdMob, which Google acquired in 2010. It and the two major platforms iOS and Android are all found on webOS and Windows Phone 7 as well. AdMob also collects data from an especially large number of data categories. In its terms and conditions regarding data privacy, for example, AdMob explains that it also records geographic data, phone IDs and, if transmitted by the network operator, phone numbers. In other words, users have to expect that apps using AdMob transmit concrete personal data.

Mobclix, for its part, is a company that connects advertisers with app producers. Phone IDs are recorded and criteria such as which apps people download, how much time people spend with an app, etc. are used to categorise users into various stakeholder groups.

Apps on smartphones have different ways of processing geographic data. Apps can access data produced by WLAN, UMTS and GPS recipients either only if the program is running and the data inquiry is needed to perform the desired service or always if the user starts the app or always if the app is running in the background and is recording the data.

Houston, do we have a problem?

Shop operators—Apple, Google & Co—tend to be quite relaxed about the data protection problem associated with their ranges of apps. For instance, Google does not usually check the apps and believes the app producers themselves bear responsibility for how apps handle user information. If a consumer complains, individual apps are checked and if need be, removed from the range.

Apple is more restrictive in its handling of apps. Although Apple says it checks programs uploaded by developers, this check is not done thoroughly enough because of the huge numbers of apps involved.

Studies on apps show that more than half of the apps tested transmitted the phone ID, for example. The second data category most frequently transmitted involves the various forms of location data (GPS data, but also postal code, for example). Free apps in particular are active data transmitters—they contact one or more servers in advertising networks. With many apps, it is not clear at first glance why they need the data.

Better information and greater transparency for consumers

Zgubic summed up the situation: “We cannot expect each consumer to delve into the technical and legal aspects of how apps work, which data they process and transmit. Users have too little technical knowledge and it is insufficiently clear to them how their data are subsequently used, where they are stored, who has access to them and how money is earned on them in the process.” The AK therefore has the following demands:

1 Mobile phone and app vendors must provide greater consumer protection.

+ Terminals that protect personal privacy.
There is a lack of “privacy-friendly” models for end users on the smartphone market. A user has to be able to prevent possibilities for monitoring on the mobile phone. There are certain modest beginnings, such as aSpotCat. It sorts installed apps according to the rights they are granted, thus making it easier to maintain an overview and control.

+ Quality mark for apps
“Consumer-friendly” app programmers should be subject to the European Privacy Seal and acquire it as a mark of quality.

+ Better information
App vendors and data collectors must provide substantially better information about the purpose of data processing, about the duration, scope and type of data used. They must also explain to the users involved how they can enforce their rights to information, correction and deletion of their data.

2 Clear-cut laws at EU level

+ Uniform regulations throughout the EU for data-hungry apps
There are data privacy regulations but they have to be expanded. Because of the lack of data and consumer protection for geographic data services, apps, etc. … uniform standards are needed across the EU to protect consumers from data-hungry mobile phone apps, e.g. reliable methods of preventing access. Smartphones can usually only apply a blanket ban on data access for apps while the apps are being installed. Users should be able to decide freely whether and when they want to make data accessible, which data are involved and to whom they are to be sent. There are generally no ways of subsequently erasing data tracks.

+ Rules for vendors
Statutory provisions are needed for equipment vendors because of the complete lack of transparency regarding the processes involved in data processing. People less technically well versed should be given ready access to understandable information. Mobile phones should have a function that is always clearly visible and that tells them the moment location data are being processed.

New approaches to the enforcement of rights also have to be used. There are millions of apps and only a handful of international equipment and app shop vendors. Given this situation, national data privacy authorities and the EU Commission will have to cooperate closely to enforce European data privacy standards.

What to watch out for in apps

+ Install apps only if they come from trustworthy sources. Read evaluations of the apps first (e.g. in an app shop and in Internet forums).

+ Check the access authorisations when installing the app. You usually find them under “Settings”. In Android mobile phones and tablets you can do this even before clicking on “Install”. The same is true of Apple devices. After that, you can deactivate tracking services, for example, under “Settings”. It is better not to install an app that obviously requires too many authorisations for its scope of functions.

+ Be especially cautious with free apps. Do not click on advertising links.

+ Be careful when children play with the device. Since May you have had the power to disable data services on mobile phones. This step also eliminates the possibility of abuse by apps.

+ Delete apps you no longer need. This step will ensure that undesired data can no longer be transmitted in the background.