Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 30 | Issue 1 Article 3

2-25-2014

Here, There and Everywhere: Mobility Data in the EU (Help Needed: Where is Privacy?)

Raffaele Zallone

HERE, THERE AND EVERYWHERE: MOBILITY DATA IN THE EU (HELP NEEDED: WHERE IS PRIVACY?)

Raffaele Zallone†

Abstract

European law on data privacy has not clearly developed the concept of mobility data. The evolution of technology has forced the EU to cope with this reality, but so far its legislation lacks a specific focus on this aspect of technology.

A body composed of representatives from the various data protection authorities, the so-called article 29 Working Party (the name stems from section 29 of the European Data Privacy Directive, that calls for the formation and the task of this body) has coped with various aspects of mobile technology, but the documents and analysis it has produced are general and un-conclusive. This is reflected in the general attitude on the side of industry, which seems to be more concentrated on getting access to as many data as possible, rather than taking European data privacy laws seriously.

The European Commission has published its new proposed Regulation that, in the Commission's plans, are bound to replace the old Data Privacy Directive. The proposed Regulation, again, lacks a definition of mobility data, but its present wording is something the industry should look at very seriously, since lack of compliance with it (assuming it shall be enforced sometime in the not-so-far future) may be extremely costly.

---

† Raffaele Zallone is the founding and managing partner of Studio Legale Zallone, a highly specialized firm in the IT business based in Milano. He was General Counsel for IBM Italy from 1989 until 1997, when he started his law firm. Mr. Zallone has been a professor of IT Law at the Bocconi University in Milano and Chairman of the ITC Committee of the European Lawyers Association (UAE). He is the author of several books on IT contracts, privacy and internet. Mr. Zallone and his firm focus on drafting and negotiating outsourcing contracts, intellectual property issues, e-commerce, and data privacy matters.

TABLE OF CONTENTS

INTRODUCTION

From the very moment of its foundation, the European Union (EU) has tried in every way to eliminate any obstacles to the free circulation of goods, services and people across borders. In fact, the EU is based on what have been defined as the four basic European freedoms; these basic freedoms are: free circulation of goods, free circulation of capital, free circulation of services, and (last, but certainly not the least important) free circulation of people.[1] The elimination of any kind of barriers and the possibility for people to offer their services and goods regardless of their place of origin has been the driving force of the European Commission from the outset. In essence, mobility is at the very heart of Europe; in order to foster growth and freedom, everyone and everything has to be free to move, work, and live wherever they see fit—people have to be able to move freely, and so do goods, services, etc.

Needless to say that whenever people move, their data move along with them. If a European citizen wants to move and work in any country within the EU, his or her data must follow him or her from the country of origin to the country of destination; therefore, making sure mobility is not restrained has always been a top priority for European legislators.

It is for these reasons that the concept of mobility is clearly present and expressly mentioned in the title of the basic and fundamental law of Europe on data protection (the "Data Protection Directive"), which is set to regulate "the protection of individuals with regard to the processing of personal data *and on the free movement of such data*."[2]

It is fair to say that even though the mobility of data was conceived as a requisite at the outset of European legislation on data protection, European legislators could not have known how important mobility would become for data protection law, and most of all, how different the concept of data mobility would be from what it was originally foreseen to be in 1995. For the sake of time, I shall not spend time describing the changes, the improvements, and the different progresses of technology that have increased the amount of mobility data available nowadays; we all know the technology, we all

1. *See* Consolidated Version of the Treaty Establishing the European Community art. 3.1, 1997 O.J. (C 340) 173.

2. Council Directive 95/46, arts. 29-30, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC).

use it and we all have it in front of our eyes. I would rather start with examining the different aspects of mobility that are relevant to data protection law and how European legislators have dealt with it.

I. WHAT PERSONAL DATA ARE MOBILITY DATA?

A. A Possible Definition

When addressing the issues raised by mobility data we need to ask ourselves whether there is a definition of mobility data under European Law that we can use as a reference. The answer is no—as of today, European Law (and, to the best of my knowledge, any data protection law of any other country) has no definition of mobility data. The closest one gets is European Directive 2002/58/EC, in which Article 2(c) defines "location data" as "any data processed in an electronic communication network indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications services."[3]

This definition makes no reference to mobility. Eventually location data will turn out to be mobility data (if one knows the location of a data subject in any given moment and assuming in time the data subject has changed his or her location). This definition is based on a static concept related to an object (the physical location of a terminal device), while mobility data, for the purpose of the analysis I shall carry out in this paper, are something very different.

Importantly, the European Commission has issued the draft of a new Regulation, which shall replace the present data protection directive (Directive 95/46/EC). The present draft of the new Regulation (at least in its present status) gives no definition of mobility data.[4]

Because of a lack of a statutory definition and for the sake of common understanding, I shall refer to "mobility data" as personal data which indicate the physical places (and hence the movements) where a person has been in time and where personal data have been generated.

---

3. Council Directive 2002/58, art. 2, 2002 O.J. (L 201) 37, 43 (EC).

4. *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Draft Proposal*], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited Oct. 31, 2013).

B. The Traditional Notion of Mobility Data

Using this definition, we can now examine the different kinds of mobility data. First, we have the data derived from the physical movement of the data subject, i.e. the person whose data are being processed. As an example, when one person travels or simply moves in different places of the same geographical area, the data derived from the use of his or her credit card shall show charges related to the purchases made in the various places visited. The fact that charges have been generated in location A and in location B show that the data subject has moved from location A to location B. Another example is the passengers' data processed by an airline—to board a plane, one must go through the check-in procedures. These data show that passengers of any given flight were in city A before take-off and (most likely) will be in city B after landing. In this case mobility data are not self-generated by technological devices, but are simply the result of the use of information technology (IT) to perform basic processing related to the business activity of the controller. What has generated the data is just the physical presence of a person in different places in different times.

Another kind of mobility data are data which are generated by a device that is associated to a person. Radio frequency identification devices (RFIDs) are a typical example of these devices;[5] they also are the first example of self-generated data that have been examined under EU law (as we shall see later on in this paper). RFID[6] is the technology that allows one to pay the toll automatically on a freeway or when crossing a bridge without stopping at the pay-toll gate, or that allows employees to access different areas of an office and to open doors with a badge. In all these cases RFIDs are associated with a person; therefore, the data generated from the device indicate the presence of a person in a given place at a given time.

Global Positioning System (GPS)[7] data are other examples of

---

5. For a summary description of RFID technology see Simon Holloway, *RFID: An Introduction*, MICROSOFT DEVELOPER NETWORK (June 2006), http://msdn.microsoft.com/en-us/library/aa479355.aspx.

6. For more on RFID technology see Roy Want, *An Introduction to RFID Technology*, IEEE PERVASIVE COMPUTING, Jan.–Mar. 2006, at 25; s*ee also* LARAN RFID, A BASIC INTRODUCTION TO RFID TECHNOLOGY AND ITS USE IN THE SUPPLY CHAIN (2005) (on file with author).

7. GPS provides location information on objects on the earth. *GPS Definition*, BRITANNICA.COM, http://www.britannica.com/EBchecked/topic/235395/GPS (last visited Nov. 1, 2013). The system is composed of a number of satellites and on ground receivers. *Id*. A GPS receiver calculates its position by precisely timing the signals sent by a satellite. *Id*.

this kind of mobility data. A GPS[8] is, in essence, a satellite-based system that tracks the position and the movements of a given object, be it a car or a mobile phone. In fact, GPS is a basic feature of many mobile phones, in that it allows location of the phone and the cell tower to which it is connected. When the telephone moves along with its owner, the GPS constantly indicates its location and allows one to make/receive phone calls, mail, or messages in any place. GPS is also a basic feature of some (but, probably of all smartphone embedded) digital cameras.[9] It is now customary on the computer, when downloading pictures taken with a phone, to see the different places where every single picture was taken.[10] This feature was used by the FBI to track and arrest a hacker of the "Anonymous" group who had just cracked a strategic military IT system. In order to show off his success in cracking the system, the hacker had taken a picture of the screen and published it, which was enough to locate and arrest him![11]

Most apps available for download and use on our smartphones use location data, for one reason or another.[12] Some applications could not work at all without being able to position the user—for example, one of the main purposes of Google's Maps[13] would be totally useless if it wasn't able to exactly locate the user requesting data. It is hard to conceive how it would be possible for it to indicate

---

8. For more information on GPS technology see *Official U.S. Government Information About Global Positioning System (GPS) and Related Topics*, http://www.gps.gov (last visited Aug. 24, 2013).

9. A feature called "geo-tagging" applies location coordinates to digital objects like photographs and other documents for purposes such as creating map overlays. *See Geotag Definition*, OXFORD DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/geotag (last visited Nov. 1, 2013).

10. Apple's iPhoto under the heading "Places" will show all the locations where the photos loaded on the Mac have been taken, a common feature now in many programs.

11. Photographic geo-coding combines position data with photographs taken with a digital camera, which allows one to look up the location where the photograph was taken. *See* Diomidis D. Spinellis, *Position-Annotated Photographs: A Geotemporal Web*, IEEE PERVASIVE COMPUTING, Apr.–June 2003, at 72, *available at* http://www.spinellis.gr/pubs/jrnl/2003-PC-GTWeb/html/gtweb.pdf (last visited Nov. 1, 2013).

12. The information usually available on Apple's iTunes Store is a brief description of the App, the name of the developer, the category it fits in, the date of the latest update and the version, dimension of memory required, compatibility and an evaluation based on feedback from users. APPLE ITUNES, http://www.apple.com/itunes/charts/free-apps/ (last visited Dec. 16, 2013). No detailed technical information is usually available; in some cases, where a link with the developer is supplied, some more technical information is available.

13. GOOGLE MAPS, https://maps.google.it/maps?hl=it&tab=nl (last visited Aug. 24, 2013).

the road to follow in order to get from a given place of origin to a required destination without knowing the location of the user and his or her movement in space and time. The processing of mobility data generated from our mobile devices (phones, tablets, etc.) is the one thing data protection authorities are presently struggling with most. They haven't come to any solution or proposal; in fact, I know of only one decision related to mobility data in any part of Europe so far, and it is a fairly recent development in the Netherlands. It is a decision against Tom-Tom, a fairly common navigation system used in many cars, that was laid down in December 2011 by the CBP, the Dutch Data Protection Authority, which this Article shall analyze later on.[14]

Again, if we stick to the definition given at the outset of this section, we can make dozens of examples of data that indicate the mobility of persons. However, this definition is not and cannot be exhaustive. The point is that, for all practical purposes, the assumption that mobility data only refer to the mobility of the data subject is fairly conservative since it only considers the physical movement in space of a person or of a device, and it reflects our natural attitude to consider things for their physical characteristics and dimension. Since we live in a three-dimensional world, we consider only the variations of mass that can be noticed in space and time, that are derived from movement of people and devices in space and time—in essence, we stick to what we can see with our eyes (or what can be seen by someone else's eyes).

C. A New Paradigm for Mobility Data

This is a limited way of addressing the issue and so I would like to make the point that technology has put in front of our eyes at least two additional cases to consider: cloud computing[15] and internet navigation data.

So far lawyers have examined the legal implications of cloud computing from many points of view. Right now, for example, many are asking the following question: is there a limitation to the kind of data that can be put into the cloud? Can a government organization

14. COLL. BESCHERMING PERSOONSGEGEVENS, OFFICIAL INVESTIGATION BY THE CBP INTO THE PROCESSING OF GEO-LOCATION DATA BY TOM TOM N.V. (2011), *available at* http://www.dutchdpa.nl/downloads_overig/en_pb_20120112_investigation-tomtom.pdf (last visited Aug. 29, 2013).

15. Cloud Computing allows the use of computing resources, on demand, through a network (usually through the Internet). Peter Mell & Timothy Grance, U.S. Dep't of Commerce, The NIST Definition of Cloud Computing 2-3 (Nat'l Inst. of Standards and Tech. ed., 2011).

use cloud computing in regards to data used to perform the tasks and the activities of public administrations, e.g. data related to the health of its citizens, their financial situation as reflected in their tax returns, data that indicate racial origin and the like? Can a government organization use it for any other kind of data? Public agencies and public administrations are examining what data can be processed using the cloud technologies and offerings that are now available everywhere and from many providers.[16]

For what reasons are public authorities interested in examining cloud computing? It is because it is not the data subject that moves in cloud computing technology, rather it is the data that moves! Cloud computing techniques and technologies require data to move dynamically from one server to another, on the basis of the services requested and the availability of storage and/or computing power. In fact, data processed with cloud computing techniques can be stored and/or processed in any given device of an IT infrastructure, regardless of the country that originated the data or where the final customer resides.[17] When the data are required for processing, they may then be moved to any device on the basis of available resources and/or computing power, thus allowing the provider to respond to every specific customer's demand. The servers or the storage devices where the data are moved may be in any given country of the world. The physical location and its nationality, in this technology, is not an issue, rather the issue is to better exploit the technology to better service customers. In our world of cut-throat competition, where industries try to save every possible nickel and dime, servers tend to be located in areas where manpower costs are lower. We have seen the rise in outsourcing capabilities in India and other similar countries; the same is true for cloud computing. In fact, with increase

16. Most recently the Swiss government has issued a bid through the University of Lausanne to ascertain what data held by a Swiss public administration could be stored or processed on cloud computing systems. For additional materials and information on cloud computing and privacy implications, see DIDIER BIGO, ET AL., EUROPEAN PARLIAMENT, POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, FIGHTING CYBER CRIME AND PROTECTING PRIVACY IN THE CLOUD (2012), *available at* http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050 (last visited Aug. 29, 2013).

17. Indeed, this is the main difference between cloud computing and the traditional client-server model. Cloud computing resources are shared by multiple users because the technology allows the users to maximize their resources by allocating them to users in different time-zones. Thus, for instance, during European business hours a given set of resources serve European customers, while the same resources serve North American customers during their business hours.

in competition and with new entrants on the marketplace, price-sensitivity shall increase and the likelihood that servers be placed in remote countries with low manpower costs is going to increase accordingly. This is not a trivial fact—data from rich and wealthy countries may end up in the hands of low-income, less developed countries. This may not be a problem in and of itself, but the issues related to it need to be addressed and resolved from a legal perspective.[18]

But let's go back to mobility; in cloud computing there are no mobility data as I have tried to define them at the outset. The issue is mobility of the data.

The point is that moving data from one country to another is an act that has significant legal consequences,[19] since trans-border data flow (when data moves beyond the boundaries of Europe) is regulated (at least in Europe) and has to follow certain rules.[20] Therefore, regardless of where the data are generated, the fact that they may be moved from one country to another does create a data protection issue to be addressed and resolved. What makes the case of cloud computing difficult to address is that the mobility of the data does depend on the basic operational decision and choices of the supplier of could computing services. The location of data and their movement within the supplier's infrastructure is mostly automatically driven by the software, and is independent from the location of the customer as well as of the location of the data subject. It is probably correct to say that if the question was asked to most suppliers of cloud computing services, "Where are my data today?" very few would be in a position to answer that question quickly and correctly.

Another case to address is internet navigation data. Again, as stated above, I appreciate that we all have a view of the world which is functional to the physical side of our life: things move in space; our bodies are physical objects that move in space; in this very moment, I am writing this paper by hitting the keys disposed in the layout of the keyboard. This is simply to say that our minds conceive movement as

---

18. For the legal issues raised by cloud computing, see W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: Looking at Clouds From Both Sides Now*, 16 STAN. TECH. L. REV. 79 (2012).

19. Council Directive, *supra* note 3, arts. 25-26, at 45-46.

20. A standard contract has been developed to be used when transferring data outside the EU; this contract has been recently updated with the Commission decision of February 5, 2010. Commission Decision 2010/87 of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 5.

a physical act of an object in space. When we surf the web from one site to another in search of information, we are not moving—our bodies remain in the same physical place (at our desk or in front of our tablet). But while we sit and wait for the results of our navigation, the bits generated from our searches migrate from one device to another; electrical impulses hit different devices, bits are arranged in different fashion, and so our data move from one site to another one, with the final aim to give the users the data sought.

Let me be clear: it is not the fact that bits and electrical impulses move from one device to another inside computers that makes the difference—bits, data, and impulses move continuously when we use a computer. The point is that when moving from one site to the next, our data move from one server to another one, thus creating new sets of data (navigation data) that for all practical purposes can be regarded as personal data (remember, the Data Protection Directive defines personal data as "any information related to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to a identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity").[21] In their trip to retrieve the data and the information we were seeking from the destination internet site, our data have moved from one server to another, creating a completely new set of personal data. Once again, in the case of internet navigation data, as in the case of cloud computing, we have mobility of the data as opposed to mobility of the data subject.

The last two examples show that we are facing new and different paradigms where the mobility focus is not on the data subject but on the data itself. After all, the law protects personal data—if mobility of the personal data is induced by reasons different from the movement of the data subject, it's still mobility and it's still data. For this reason navigation data, in my view, do fit within a possible definition of mobility data, upon the condition that we amend the initial definition to include the categories of data indicated above: (A) personal data which indicate the movements and the physical places where a person has been in time and where personal data have been generated; and (B) personal data which indicate Internet navigation of a data subject; and (C) personal data moved, stored, or processed from time to time in different locations.

---

21. Council Directive, *supra* note 2, art. 2, at 38.

II. MOBILITY DATA AND THE DATA PROTECTION PRINCIPLES

Having set the stage in this way, what are the issues related to mobility data under European law?

In order to answer this question, the basic principles of data protection have to be recalled, i.e. what the Data Protection Directive defines as the data protection principles.[22] In essence, these principles are the following:[23]

1. personal data shall be processed fairly and lawfully;
2. personal data can be held for one or more specified lawful purposes and shall not be further processed in any manner incompatible with such purposes;
3. personal data shall be adequate and relevant and not excessive in relation to such purposes;
4. personal data shall be accurate and kept up-to-date;
5. personal data shall be kept for no longer than is necessary for such purposes;
6. personal data shall be processed in accordance with the rights of the data subjects;
7. adequate security measures have to be taken to protect personal data;
8. personal data shall not be transferred to a country or territory outside the EU unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects.[24]

Let's say that, for the purposes of this paper, the most relevant data principles are (A) the transparency principle (point 2): if anyone wants to process personal data, they have to state for which purposes they are going to be processes; (B) the purpose principle (point 2): personal data have to be processed for one or more specific and identified purposes; (C) the data quality principle (point 3): data must be "adequate and relevant," i.e. one has to process data that are consistent with the purposes of the processing; and (D) the location principle (point 8): data can flow freely within the EU, but if they have to go outside the EU it must be into a country where there is a

22. *Id*. arts. 5-6, at 39-40.

23. *Id*. art. 6, at 40.

24. *Id.* Most European statutes on data protection have the same data principles. *See e.g*. Data Protection Act, 1998, c. 29, § 4, sch. 1 (Eng.); *see also* Decreto Legislativo, 30 Giugno 2003, in D.Lgs., n. 196 (It.).

reasonable expectation that the data shall receive an adequate level of protection, comparable to the protection they receive within the EU.[25] This means that any entity processing mobility data must inform the data subject about two things: that the entity processes personal data of the data subject and for what purposes the entity is processing the data. The data subject, depending on the circumstances (and on the law they are subject to) has to agree with such processing.

There is no legal requirement under EU law to indicate what data shall be processed; therefore, it is irrelevant to indicate if one shall collect and process mobility data. Nevertheless, since the relevance of data is one of the data protection principles, one must ensure that there is a fair and lawful reason to collect mobility data. A phone company needs mobility data to provide its services and connect the customers wherever he or she may be. In this case the processing is consistent with the scope of providing the services agreed upon and fulfilling the contract between the parties.

On the other hand, an application called "Mirror,"[26] which simply transforms the screen of a smartphone into a mirror (sort of), sends a warning stating: "Mirror wants to access your location data" (which means that as one moves, the app shall be collecting mobility data). Under the data quality principle above, what is the relevance of mobility data to an application that is only supposed to transform my screen into a mirror? What is the purpose of such processing and how does it relate to the function performed by the application?

The fact is that nowadays, it is quite common to open an app and receive the message, "This app wants to use your location data." This means that the app, no matter what its purpose is and what function it is supposed to perform, shall collect mobility data of the data subject. Under the data protection principles highlighted above and European law, one has to ascertain the relevance of mobility data for such an application. The question is not moot, because if the location data are not necessary and consistent with the purpose principle and/or the data quality principle, i.e. the data are not necessary to perform the function that the app is supposed to perform, collecting and processing these data could be against EU law. Checking the processing of mobility data against the data principles, in the light of the function performed by an app, is fundamental to position it under EU Law and to decide how to proceed, whether or not consent of the

25. Council Directive, *supra* note 2, arts. 25-26, at 45-46.

26. ITUNES, https://itunes.apple.com/us/app/mirror/id390949350 (last visited Aug. 25, 2013).

data subject is needed.[27]

III. MOBILITY DATA IN THE EU

Mobility data has been examined by several EU authorities. Article 29 of the European Data Privacy Directive has established a Working Group, known as the Article 29 Data Protection Working Party (WP29);[28] it is composed of representatives of the national Data Protection Authorities. The WP29 has a consulting function, not a legislative or a judiciary function; however, it exercises a significant role in data protection in Europe, because its document highlights the common position of the various authorities established in every member state. In 2005 the WP29 published four documents that deal with mobility data. The first one on RFIDs (WP 105)[29] was followed by a public consultation on the subject and resulted in a second

---

27. Case law shows several cases where the processing was blocked because the data sought was totally unrelated to the purpose that apparently being pursued. The website of the Italian Authority has almost ten pages of decisions and documents on the matter; for example, a company that supplies business information through a central database of all companies, as well as on individuals, was required to eliminate certain records from its files, since they were not considered pertinent under the law. For more information, see GARANTE, www.garanteprivacy.it (search "pertinenza") (last visited Aug. 25, 2013).

28. The directive provides as follows:

> (1) A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up. It shall have advisory status and act independently. (2) The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies. (3) The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities. (4) The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable. (5) The Working Party's secretariat shall be provided by the Commission. (6) The Working Party shall adopt its own rules of procedure. (7) The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Council Directive, *supra* note 2, arts. 29-30.

29. Article 29 Data Protection Working Party *Working Document on Data Protection Issues Related to RFID Technology*, 2005 10107/05 (WP 105) (EN), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf (last visited Aug. 25, 2013).

document (WP 111).[30] The third document (WP 115) deals with the use of location data in the context of supplying value added services.[31] The most recent document was adopted on February 27, 2013 (WP 202).[32]

WP 105 highlighted a heated debate between industry representatives, consumer groups, universities, think tanks, and trade organizations. WP 105 set out some examples of processing personal data using RFIDs, for example a supermarket that tags loyalty cards or similar devices (which identify the holder by name) to learn consumer habits while in the store.[33] Another example made by the WP29 was related to products which have been tagged with RFIDs—a customer enters a shop wearing a product (a wrist watch) bearing an RFID, albeit not originally inserted by that shop; the customer's RFID is scanned by the reading station of the shop which starts a profile of the customer so that when he or she returns to the store he or she is identified and the profile is updated with details of sections visited, products bought, etc. Even though the store may not know the customer's name (since the RFID was inserted in the wrist watch by someone else) the WP29 believed these were personal data.[34] These examples have been strongly criticized by industry representatives,

---

30. Article 29 Data Protection Working Party, *Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology*, 2005 1670/05 (WP 111) (EN), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp111_en.pdf (last visited Aug. 25, 2013).

31. Article 29 Data Protection Working Party, *Working Party 29 Opinion on the Use of Location Data with a View to Providing Value-Added Services*, 2005 2130/05 (WP 115) (EN), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf (last visited Aug. 25, 2013).

32. Article 29 Data Protection Working Party, *Opinion 02/2013 on Apps on Smart Devices*, 2013 00461/13 (WP 202) (EN), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (last visited Aug. 25, 2013).

33. Article 29 Data Protection Working Party, *supra* note 29, at 5-6 ("one can consider the case where supermarket tags loyalty cards or similar devices, which identify individuals by their name to learn and record consumer habits while consumers are in the store").

34. The WP29 explained:

> Take the hypothesis when person Z walks into shop C with a bag of RFID-tagged products from shops A and B. Shop C scans his bags and the products in it are revealed. Shop C keeps a record of the numbers. When person Z returns to the shop the next day, he is rescanned. Product Y that was scanned yesterday is revealed today; the number is for the watch he always wears. Shop C sets up a file using the number of product Y as a key. This allows them to track when person Z enters the shop, using the RFID number of his watch as a reference number for him.

Article 29 Data Protection Working Party, *supra* note 29, at 7.

who, in response to the public consultation, made the point that these were not to be considered personal data. The WP29 did not issue a decision on the matter (since it has no decision power) but reported the dissent and concluded that data controllers using RFIDs should check the data protection principles and comply with them. Highlighting the importance of checking the processing of the data gathered with the RFID, the purpose principle, and the data quality principle,[35] WP29 continued stating that consent was the legal ground to carry out such kind of processing of personal data.[36] If consent is necessary, consent must be informed and as such information requirements must be met (i.e. the customer must be aware of the presence of an RFID tag on the product bought and of the entity that would process the related data and for what purposes).[37] The public consultation highlighted that there was consensus as to the fact that the RFID's should embed technical solutions (e.g. privacy enhancing technology or PET) to allow easy deactivation of the RFIDs by the retailers at the cash register level (i.e. the cashier should deactivate the RFID at moment of purchase).[38] Needless to say that retailers and standard bodies for retailers "strongly disagreed" that the cashier should perform the de-activation of the RFID.[39] Also, there was harsh criticism of WP 105 due to the fact that it did indeed stretch the notion of personal data in some of its examples,[40] as well as the fact that some of the examples were not taken from real life, but mere hypotheses.[41]

WP 115 on location data gathered in performance of value added services is quite interesting; it is a short document (11 pages, cover

35. *Id*. at 9 ("Data controllers collecting data in the context of RFID applications must comply with several data protection principles.").

36. *Id*. at 10 ("Under most scenarios where RFID technology is used, consent from the individuals will be the only legal ground available to data controllers to legitimize the collection of information through the RFID.").

37. *Id*. at 9 (Data controllers "must provide the following information to data subjects: identify the controller, the purposes of the processing as well as, among others, information on the recipient of the data and the existence of a right of access.") (footnote omitted).

38. Article 29 Data Protection Working Party, *supra* note 30, at 3 ("As concerns technical solutions that some consider should be in-built in [sic] RFID applications, respondents agree about the need for easy deactivation of RFID tags by retailers at the point of sale must be mandatory.").

39. Article 29 Data Protection Working Party, *supra* note 30.

40. *Id*. at 3 ("In particular, a number of respondents think that the various hypotheses described in point 3.3 of the Working Party 29 paper do not entail a processing of personal data.").

41. *Id*. ("A repeated criticism of the paper is that the examples of RFID applications given in the paper do not represent reality.").

and standard openings included) and it really is the first official document that addresses the world of smartphones, although the title does not explicitly state so.[42] The technologies considered by the document are: devices used in the transport sector, GPS, credit cards, and mobile phones.[43] The document distinguishes traffic data (data to locate the user and allow it to call or receive calls, as well as all data relate to phone calls made) that are considered necessary to supply the phone services, from location data that "provide key information about an individual" and have been quickly "viewed as a potential source of revenue."[44] After having addressed the legal framework under which these applications had to be evaluated—Directive 95/46/EC and Directive 2002/58/EC[45]—as well as the issues related to applicable national law, the WP29 highlighted that in order to process data other than traffic data, it is necessary to obtain consent, but only after the user has been duly informed pursuant to Section 6 and Section 9 of the Data Privacy Directive.[46] Consent is not required when traffic data are processed in order to perform the services offered.[47] However, it must be noted that WP 115 is quite fuzzy and confusing when addressing the issue of consent, in that at the very outset of addressing the issue of consent, it states that consent is required when sensitive data are processed.[48] Although the statement in itself is correct,[49] the point is that WP 115 does not indicate what sensitive data could be processed by using location data. But most of all, after having made such an ominous statement, WP 115 does not address the issue of whether consent is required when sensitive data *are not* being processed. It is therefore a significant disappointment to read a document from such a prestigious group and find such a grey area. The result is that the document raises some issues that

42. Article 29 Data Protection Working Party, *supra* note 31.

43. *Id*. at 2 ("Generally speaking, there are many ways of locating individuals, primarily using 'traces' left by the use of new technologies: automatic ticket machines in the transport sector, GPS, bank cards or electronic purses, or, in the case at issue, mobile telephones.").

44. *Id*. ("[L]ocation data, insofar as they provide key information about an individual (in short, who is where), quickly came to be viewed as a potential source of revenue.").

45. Council Directive, *supra* note 3.

46. Article 29 Data Protection Working Party, *supra* note 31, at 4-6.

47. *Id*. at 6 ("Offering a service that requires the automatic location of an individual . . . is acceptable provided that users are given full information in advance about the processing of their location data.").

48. Article 29 Data Protection Working Party, *supra* note 31.

49. *Id*. at 5 ("In accordance with standard practice for personal data protection when sensitive data are [sic] processed, European legislation requires prior consent to be obtained for processing location data other than traffic data.").

appear to have little connection with the subject matter; and in doing so creates other questions and issues that are not addressed.

IV. GEOLOCATION SERVICES OFFERED BY SMARTPHONES

A. The WP29 on Geo-Location Services

More interesting and more to the point is the document adopted by the WP29 on May 16, 2011, WP 185.[50]

This document has ups and downs, so to speak. It starts with a description of the technologies involved (base station data, GPS, and Wi-Fi).[51] The document then, per the standard format used in these cases, summarizes the legal risks of this technology, stating that geo-location services can help gain "an intimate overview of habits and patterns of the owner."[52] But most disturbing is when WP 185 (similar to WP 115) again makes the point that such location data may also include sensitive data.[53] The examples made are vague, amazingly generic, and plainly wrong and misleading. Is the mere presence of an individual in a hospital a sign of him or her being sick? Certainly not—one may visit a hospital for a dozen reasons, which have nothing to do with the health status of the data subject, just as one may go to a church for the wedding of a friend, without there being an indication about his or her religious belief.

But let's leave this example aside for a moment. The WP29 highlights what it believes are the main risks of a given technology or situation in a section of its published documents titled "privacy risks." Let's then look at what risks are pointed to in WP 185. First, since mobile phones are constantly linked to an individual (people keep them in their pocket or in their purse), they allow "provider[s] . . . to gain an intimate view of habits and patterns of the owner and build extensive profiles."[54] Second, "[t]he technology of smart mobile

50. Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices*, 2011 881/11 (WP 185) (EN), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf (last visited Aug. 25, 2013).

51. *Id*. at 4-6.

52. *Id*. at 7 (After noting that most people are indeed aware that mobile devices contain extensive intimate information, WP 185 states that "[t]his allows the providers of geolocation [sic] based services gain an intimate overview of habits and patterns of the owner of such a device and build extensive profiles.").

53. *Id*. ("A behavioural [sic] pattern may also include *special categories of data*, if it for example reveal visits to hospitals and religious places, or presence at political demonstrations or presence at other specific locations revealing data about for example sex life.").

54. *Id*.

devices allows for the constant monitoring of location data" so that "from a regular travel pattern in the morning, the location of an employer may be deducted."[55] Third, "the unlimited global access creates new risks ranging from theft to burglary, to even physical aggression and stalking." And finally, a major risk is regarded to be the so called "function creep, i.e. the fact that based on the availability of a new type of data, new purposes are being developed that were not anticipated at the time of the original collection of data."[56]

Having stated in this fashion the most significant risks, WP 185 clarifies that the legal framework to look at is the Data Protection Directive 95/46/CE, but if a telecom operator offers geo-location services processing base station data, these services are qualified as public electronic communication services, thereby also falling under Directive 2002/58/EC of July 12, 2002 (the so-called "e-Privacy Directive"), later amended in November 2009 by Directive 2009/136/EC.[57]

On the other hand, companies that provide location services and applications based on a combination of technologies (e.g. base station, GPS, and WiFi) are "information society services," and as such outside the application of the e-Privacy Directive.[58]

Given the number of players in this scenario, WP 185 focuses on the subject to whom the legislation applies and who, hence, has the duty to comply with the law. Since location data are a combination of data collected through Wi-Fi access points, GPS, and base stations, whoever collects these data processes' personal data should be regarded as the controller and, therefore, must comply with the requirements of the Directives.[59] In addition, application providers that offer applications capable of offering geo-location services are to be regarded as the controller and, as such, have the duty to comply with the law.[60] Examples of these applications are weather forecast

55. *Id*.

56. Article 29 Data Protection Working Party, *supra* note 50. As mentioned above, the risks are listed in paragraph 3.

57. Council Directive 2009/136, 2009 O.J. (L 337) 11, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:en:HTML (last visited Aug. 25, 2013).

58. Article 29 Data Protection Working Party, *supra* note 50, at 8 ("[C]ompanies that provide location services and applications on a combination of base station, GPS and WiFi [sic] data are *information society services*. As such they are explicitly excluded from the e-Privacy directive.").

59. *Id*. at 11-12.

60. *Id*. at 12 ("Such applications can process the location data (and other data) from a smart mobile device independently from the developer of the operating system and/or the

applications or applications that offer information on near-by places of interest, stores, restaurants, etc.

Also the developer of the operating system of a smartphone, "when it interacts directly with the user and collects personal data (such as requesting initial registration and or collecting location information for the purpose of improving services)" can be a controller of data.[61] These controllers are required to use privacy by design principles to help minimize the possibility of secret monitoring.[62]

As far as the legal ground for processing, the WP 185 is quite sharp—the only ground for a controller to supply a value added service based on the processing of personal location data (independently if the controller is a telecom operator, application provider, or the developer of the operating system) is to seek and obtain prior consent, which must be informed and specific for all purposes for which data are being processed.[63] The consent is also needed because when the default setting of the operating system allows for the transmission of location data, lack of intervention by the user does not imply consent.[64] WP29 warns as to the lack of transparency that may exist and the lack of consistency with the data principles,[65] specifically, that data can be processed only for the typical purpose of the application.[66] In this respect, the different controllers "must make sure the owners of the smart devices are adequately informed about the key elements of the processing in conformity with Article 10 of the Data Privacy Directive."[67] If the purposes of the processing change, new information must be given

---

controllers of the geolocation [sic] infrastructure.").

61. *Id*.

62. *Id*. at 12 ("As a controller the developer must employ privacy by design principles to prevent secret monitoring, either by the device itself or by the different applications and services.").

63. *Id*. at 13.

64. Article 29 Data Protection Working Party, *supra* note 50, at 13 ("[T]echnical capacity should not be confused with . . . lawfulness.").

65. Council Directive, *supra* note 2, at 40 (stating that personal data shall be processed fairly and lawfully, that personal data can be held for one or more specified lawful purposes, and that it shall not be further processed in any manner incompatible with such purposes).

66. Article 29 Data Protection Working Party, *supra* note 50, at 15 ("The controller must make it very clear if his service is limited to providing an answer to the voluntary question 'Where am I right now?', or if [his or her] purpose is to create answers to the questions 'Where are you, where have you been and where will you be next week?' In other words, the controller must pay specific attention to consent for purposes a data subject does not expect, such as for example profiling and/or behavioural [sic] targeting.").

67. *Id*. at 17.

and new consent sought; in fact, WP 185 suggests that a good practice may be to ask renewal of consent at periodic intervals.[68] Data subjects must be able to withdraw their consent in an easy fashion, without negative consequences regarding the use of the device.[69] Finally, the controllers must grant access rights to the data subject who, in principle, should have the capability to find out what location data have been gathered and the profiles that have been created on the basis of these data.[70] Specific attention must be given by the controllers to the retention period.[71] In this respect, the WP 29 is quite flexible, making a point and offering a way out to controllers; far from indicating a maximum retention period, the WP29 simply suggests that a retention period for the data be established.[72] I know very well that this is a sensitive spot for many operators, but the whole point is that the law does not impose a given number; it simply asks that a period be determined. It would be unwise to simply say, "Oh, well, we need those data forever;" yet, if this is the case, there must be a bulletproof legal rationale on which to base such a decision. This legal rationale must always be at the basis of whatever the decision is as to the period of retention. It may very well be that the legal rationale is justified by technical reasons (i.e. my system would simply not work otherwise), but the technical grounds must be sound and bulletproof.

B. A Recent Approach to Smartphones

As mentioned above, the fourth and last document is very recent and deals specifically with the privacy implications of apps on smart devices.[73] The document is quite articulate and specifically focuses its attention on consent, data principles, security of the data, information, and retention period.[74]

---

68. *Id*. at 15 ("The Working Party recommends that providers of geolocation [sic] applications or services seek to renew individual consent . . . after an appropriate period of time.").

69. *Id*.

70. *Id*. at 17-18.

71. *Id*. at 18.

72. Article 29 Data Protection Working Party, *supra* note 50, at 18.

73. Article 29 Data Protection Working Party, *supra* note 32, at 1 (the format of the document is the same as per the previous documents: the indication of the data protection risks, applicable law, legal grounds. In this case the document is quite articulate, in that includes many other sections that deal with purpose limitation, security, information, the data subject rights and the retention period, ending with conclusions and recommendation).

74. *Id*. at 5 ("The opinion focuses on the consent requirement, the principles of purpose limitation and data minimisation, [sic] the need to take adequate security measures, the

Initially the document briefly describes some of the main characteristics of the functioning of smart devices and the fact that many apps, through the application programming interface (API), have access to many of the sensors available on the devices and collect data continuously and perform a significant number of tasks.[75] The data collected in this fashion can be a base for additional processing of personal data.[76] The risks are identified first in the fragmentation of the subjects involved and in the lack of knowledge of data protection.[77] Four more risks are highlighted, such as first, the lack of transparency—users are unaware of the processing of their data which is taking place due to the simple fact of having downloaded an app![78] The other risks include the immediate and direct consequence of the lack of transparency: the lack of free and informed consent; poor security measures; and finally, the disregard of the purpose limitation principle.[79] As to the applicable law, the document is quite clear—since the requirement for an informed consent applies to services offered in the community, applicable law is European privacy law.[80] The personal data that are processed by the apps are quite significant and the list is quite impressive: location, contacts, unique device identifiers, identity of the data subject and of

---

obligation to correctly inform end users, their rights, reasonable retention periods and specifically, fair processing of data collected from and about children.").

75. The WP29 describes the data collection process:

> 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 content, record audio, use the camera and access the stored pictures, read the phone state and identify, modify the global system settings and prevent the phone from sleeping.

Id. at 4.

76. *Id*. at 4 ("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.").

77. *Id*. at 5 ("App developers unaware of the data protection requirements may create significant risks to the private life and reputation of users of smart devices.").

78. *Id*. at 6 ("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.").

79. Article 29 Data Protection Working Party, *supra* note 32, at 6 ("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 [sic].").

80. *Id*. at 8 (referring to Direct 95/46/EC and Directive 2002/58/EC, as revised by Directive 2002/58/EC, the WP29 stated, "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.").

the phone, credit card and payment data, phone calls, logs, SMS and instant messaging, browsing history, pictures and videos, biometrics, email and various types of access credentials.[81] The four parties involved are: the developers of the apps, the developer of the operating system of the device, the app distributors (app stores) and the other parties involved in the processing of personal data. In some cases the app store and the developer of the operating system tend to coincide. End users may also play a part if they decide to share some information and data, for instance, to a social network, and thereby incur duties under data protection law if personal data are involved.[82] App developers may outsource some of the processing to third parties or share the information collected to third parties. In these cases the mechanism to lawfully do so must be used to comply with the law, and if third parties are allowed access to data, they have to obtain consent from the user.[83] Operating system developers and device manufacturers are also controllers for data processed to ensure smooth running of the device and since they develop the APIs, they have to apply the "privacy by design"[84] concept.[85] As for the app stores, they process payment history for apps and other purchases and as such require user registration, with all related data.[86] Third parties have two kinds of roles: to execute operations for the app owner, or to collect information across apps and provide additional services. Depending on the capacity in which they act, they may be processors or controllers, and to the extent they have access or store information on the device, prior consent is required.[87] As to the legal ground for processing, it is obvious that consent is required, and the main issues here are the transparency of the processing of personal data and the fact that the data subject must be informed of all processing carried

81. *Id*. at 8-9.

82. *Id*. at 9.

83. *Id*. at 10 ("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.").

84. Privacy by design is a concept that has been developed by Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada. The concept is based on a set of principles which aim at embedding privacy tools in the design and architecture of any given product, making it easier for users to gain awareness of their choice and protect their rights. For more information, see PRIVACY BY DESIGN, http://www.privacybydesign.ca (last visited Aug. 29, 2013).

85. Article 29 Data Protection Working Party, *supra* note 32, at 11 ("OS and device manufacturers . . . have an important responsibility to provide safeguards for the protection of personal data and privacy of app users.").

86. *Id*. at 11-12.

87. *Id*. at 12-13.

out; this is necessary so that informed and specific consent is given. "Implicit" consent may not be allowed and may not constitute a valid basis for processing.[88] Another issue is the practice of tracking users behavior by advertiser or third parties. The operating systems must avoid such tracking and avoid circumvention by advertisers.[89] Another section of WP 202 deals with the purpose limitation and data minimization.[90] The purposes must be well-defined and consistent with the functions offered to the user, and the apps have to use only those data that are strictly necessary to pursue these functions.[91] Several suggestions are made to minimize security risks,[92] but the key section is related to the information.[93] The natural consequence of all the issues raised is that adequate information must be given to the user. Now, what is to be considered "adequate information" in this context? We have seen that there is potentially more than one controller[94] in any given scenario, and so the identity of the controllers must be known; the purposes for which the data are collected must be spelled out clearly, as well as the fact that third parties may be involved in the processing of the user's data, and what role and in which capability they are indeed involved. This obligation is not merely on the developer of the app, but also on the app store.[95] The information may be given at the time the user decides to buy or download the app at the app store.[96] If such identities are not known,

88. *Id*. at 15 ("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 [sic].") .

89. *Id*. ("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.").

90. *Id*. at 17 (Users have to "learn how their data are being 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.").

91. Article 29 Data Protection Working Party, *supra* note 32, at 17 ("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.").

92. *Id*. at 18-21.

93. *Id*. at 22-23.

94. *See supra* p. 78.

95. Article 29 Data Protection Working Party, *supra* note 32, at 22 ("There is an important responsibility for the app stores to ensure that this information is available and easily accessible for each app.").

96. *Id*. at 23 ("The essential scope of information about data processing must be available to the users before app installation, via the app store."). "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." *Id*.

there is little possibility for the data subjects to exercise their rights.[97] And, again, retention period must be defined. In this document the WP29 seems to be more restrictive in that it does give some examples of possible retention periods,[98] but I once again underline the fact that the important factor is not merely the time of retention, but the establishment of a reasonable period of time. The document's conclusions draw some three pages of recommendations;[99] it would be useless to list them all here. The main point is that for the first time the WP29 has come with a significant document, which has addressed many of the issues that the previous document had apparently forgotten or overlooked.

V. FROM THEORY TO PRACTICE

A. A Glance Into the Future: The Proposed EU Regulation Approach

From the short summary of the documents published by the WP29 before WP 202 of February 27, 2017,[100] I hope it is clear that there was little substance and a lot of theory. The WP29 had issued documents that were very general in their nature and had failed to address any real issue. Anyone who has bought a smartphone and/or has downloaded an application, for example, knows that real life is quite different from what the WP29 had depicted; there is very little information to data subjects (if any) and disproportionate use of location data (as I said above,[101] why in the world does the "mirror" app[102] or a "translate" app want to use my location data? Why do they need it? What use are they going to do with it?). Unfortunately, the marketplace is dominated by US based companies, who leverage the fact that they are based in the US to avoid any of the duties under European law.

This is not an advisable course of action to take. If a company wants to do business in any given part of the world, it cannot avoid the responsibility and the duties that derive from such a decision. For

97. *Id*. at 24.

98. *Id*. at 25 (The retention period for "data that are used once" per year could be 15 months, while a navigation app could "store only the last 10 recently visited locations.").

99. *Id*. at 27-30.

100. Article 29 Data Protection Working Party, *supra* note 32.

101. *See supra* p. 68.

102. *See supra* note 26.

instance Ferrari, the sport car maker,[103] in order to sell its cars around the world, has to comply with each law of each country it decides to do business in and so does any other seller of any material goods. The fact that small (or not so small) companies refuse to adopt a simple, logical legal standard is certainly not a badge of honor for any such company. Complying with the law should not be an optional feature, but a fundamental way of doing business. The last document from WP29 clearly addresses most of these issues. First of all, European law applies, which has been clearly stated and is a remark that many data protection authorities and many local European courts may decide to apply.[104] Second, there is too little transparency with respect to these applications. The consequence is already apparent—the proposed draft Regulation on data protection[105] addresses many of the issues highlighted by the WP29. Section 5 of the Regulation has significantly changed one of the key sections of the data principles: personal data should be processed "lawfully, fairly and in a transparent manner in relation to the data subject,"[106] which is a significant change compared to the present wording of the Data Privacy Directive,[107] which states that personal data not be "further processed in a way incompatible with such purposes."[108] Compared to the Data Privacy Directive 95/46/EC[109] the change is very significant and speaks loudly to whoever wants to listen. When it comes to consent, it is up to the controller to prove that the data subject has expressed his or her consent.[110] A new section called transparency and modalities has been added,[111] which did not exist in the Data Privacy Directive. It requires the controller to provide "any information relating to the processing of personal data" and that such information has to be given "in an intelligible form, using clear and

103. FERRARI, www.ferrari.com (last visited Oct. 31, 2013).

104. Article 29 Data Protection Working Party, *supra* note 32, at 8 ("[T]he applicability of European privacy law cannot be excluded by a unilateral declaration or contractual agreement.").

105. *See Draft Proposal*, *supra* note 4.

106. *Id*. at 43.

107. Council Directive, *supra* note 2, at 40 (Art. 6, Sec. 1(a) states that data must be "processed fairly and lawfully.").

108. *Id*. (Art. 6, Sec. 1(c) simply states that personal data should be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.").

109. Council Directive, *supra* note 2.

110. *Draft Proposal*, *supra* note 4, at 45 ("The controller shall bear the burden of proof for the data subject's consent to the processing of personal data for specified purposes.").

111. *Id*. at 47-48.

plain language."[112] And finally, the section related to the information to the data subject has been amended as to include the obligation to inform the data subject as to "the period for which the personal data will be stored."[113] Finally, the controller has the duty to inform the data subject as to any further information necessary to guarantee fair processing."[114] It is clear that all these changes and new requirements, in one way or the other, are the consequence of the new technological scenario and that the issues addressed in WP 202 cannot be ignored anymore. Of course, we are talking about a draft legislation, whose approval and implementation is still to come (if at all, for this matter), and there are a significant number of amendments proposed and waiting to be discussed and voted on at the European Parliament. Regardless, these changes are the sign of a clear change in attitude from European legislators.

B. Recent Cases on Mobility Data

And, indeed, things are starting to change. In Italy, the Data Protection Authority (Italian DPA) has examined several cases where the issues are related to geo-location services. Italian Law[115] has a specific procedure, the so-called "prior-checking procedure,"[116] which allows companies to file a request with the Authority to examine and evaluate certain proposed processing of personal data. The Italian DPA has the power to examine the cases submitted to its attention, to decide if the processing falls under the law, if it shows any issue of any relevance, and, in such a case, either to forbid or to prescribe the precautions or the measures to adopt.[117] In this way any controller has an official seal on specific processing submitted to the Garante for prior checking and can negotiate specific instances and measures.[118]

---

112. *Id*. at 47.
113. *Id*. at 48.
114. *Id*. at 49.
115. Decreto Legislativo, 30 Giugno 2003, in D.Lgs., n. 196 (It.).
116. *Id*. § 17.
117. *Id*.
118. *Id*. The relevant text states:

> 1. Processing of data other than sensitive and judicial data shall be allowed in accordance with such measures and precautions as are laid down to safeguard data subjects, if the processing is likely to present specific risks to data subjects' fundamental rights and freedoms and [sic] dignity on account of the nature of the data, the arrangements applying to the processing or the effects the latter may produce.
>
> 2. The measures and precautions referred in paragraph 1 shall be laid down by the Garante on the basis of the principles set out in this Code within the

One such case (probably the first one related to mobility data) regarded the use of GPS and other monitoring devices on buses. The management of a bus company active in central Italy wanted to implement a GPS-based system that would have allowed the possibility to check the location of each bus, as well as provide information on a number of selected of items. The system would have provided information as to speed, necessity of maintenance, degradation of specific parts, etc. It was mainly a safety-oriented system, which the Italian DPA approved without significant limitations or requested measures.[119] This was the first decision on such matters,[120] and other similar decisions on similar cases have been subsequently adopted by the Italian DPA.[121]

In another case, the Italian DPA simply issued a document stating that the system for which prior checking had been requested had no implications under the law.[122] It was a request filed by the Alpine Rescue Organisation (Alpine Rescue), an organization which intervenes in cases of avalanches and the like. The Alpine Rescue wanted to be able to have access to telephone GPS data, if available, in case of accidents, such as when GPS would be necessary to rescue people. In light of the public interest of such operations, the Italian DPA stated that no consent was needed and that the proposed processing could be carried out without any issue.[123]

In the Netherlands, at the end of 2012, an investigation was completed by the local data protection authority on Tom-Tom, the maker of navigation systems.[124] It appeared that Tom-Tom was selling or somehow making available to third parties the navigation data of its users, without giving any notice to the users. The Dutch Data Protection Authority (Dutch DPA) concluded that Tom-Tom had not been selling its customer data, but it had violated the local privacy

---

> framework of a check to be performed prior to start [sic] of the processing as also related to specific categories of data controller or processing, following the request, if any, submitted by the data controller.

Id.

119. Air Pullman S.p.A., June 5, 2008 (It.), *available at* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1672796 (last visited Aug. 28, 2013).

120. *Id*.

121. *Id*.

122. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, MOUNTAIN RESCUE (2008) (It.), *available at* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1580543 (last visited Aug. 28, 2013).

123. *Id*.

124. COLL. BESCHERMING PERSOONSGEGEVENS, *supra* note 14.

act, due to the fact that the consent to the processing of data is not sufficiently specific. The Dutch DPA also concluded that the communication to third parties did not violate the law, since the data were given in aggregate form and since all references to individual persons had been deleted. Nevertheless, Tom-Tom has had to change its privacy notice.[125]

The cases indicated above and their very limited number show that the issues related to mobile technology are still far from being fully understood. For the operators, this is tantamount to "so far so good." But what about the future? Will this attitude remain as it is or is it bound to change?

Well, first of all, all data protection authorities in Europe know what is going on and are just waiting for the right case to come along. A trigger is all it takes to attract the attention of the data protection authorities around Europe. If one looks at what has happened and is happening to Google, one can understand many things. Many local data protection authorities have opened an investigation of the Google Maps "Street View" feature;[126] the application has also caused Google problems in Europe[127] and elsewhere.[128] Until recently, data protection authorities hardly dared to act against Google, even though it was very clear that many of Google's practices were not in line with the law. The present privacy problems of Google are an example of what happens when the authorities understand the issues and decide to act.[129] And, as most lawyers in this field know, the problems are far from being over—the WP29 has been delegated by the other authorities to investigate Google's new privacy policy, and things seem to be at a stalemate.[130]

---

125. *Id*.

126. *Google Streetview Cars Will Have To Be Clearly Marked*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (Oct. 25, 2010), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1761443.

127. *Germany: Google Fined Over Street View Privacy*, SKY NEWS, Apr. 22, 2013, http://news.sky.com/story/1081382/germany-google-fined-over-street-view-privacy.

128. Adi, Robertson, *Google Settles Street View Privacy Case with 38 States for $7 Million*, THE VERGE, Mar. 12, 2013, http://www.theverge.com/2013/3/12/4094522/google-settles-street-view-privacy-case-with-states-for-7-million.

129. *"Captured" Communications on Wi-Fi Networks: The Italian DPS Requires Google to Block Data Processing and Reports the Case to Judicial Authorities*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Sept. 21, 2010, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1751001.

130. *GOOGLE's New Privacy Policy: CNIL Sends a Detailed Questionnaire to Google*, COMMISSION ON INFORMATION TECHNOLOGY AND LIBERTIES, Mar. 19, 2012, http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-cnil-sends-a-detailed-questionnaire-to-google.

If and when the data protection authorities will fully open their eyes on the privacy issues created by mobile technology is hard to tell, and it clearly may depend on many circumstances; nevertheless, one cannot help but point out that when the new proposed Regulation on data protection replaces the old Data Protection Directive, the scenario shall be quite different. Just one thing as an example may suffice: violations today are subject to relatively limited fines. While there are also criminal implications in some member states of the EU (Member States), no real case has been brought forward against Google (apart from the Vividown case,[131] which ended up with Google's officials' acquittal).[132]

The proposed Regulation calls for fines up to €1,000,000 or 2% of the total turnaround of the violating company.[133] This starts to be a significant sum under any standard. In other words, privacy laws have been around for the better part of the past 18 years and no one can claim ignorance of the law anymore (assuming that this was a good defense, in the first place).

VI. CLOUD COMPUTING

The WP29 has analyzed the privacy issues related to cloud computing[134] and, although once again the issues of mobility data are not expressly mentioned, they are nevertheless examined.[135] The document indicates that personal data are being processed in many different countries, and some of them may be processed in third countries outside the EU.[136] The WP29 has no doubts as to the possibility of applying European data privacy law when the controller is located in one or more Member States.[137] As mentioned above,[138] I

131. La Corte d'Appello di Milano, 21 dicembre 2012, 8611/2012.

132. Oreste Pollicino, *Google Versus Vividown Atto II: Eco le Motivazioni*, DIRITTO 24, Feb. 28, 2013, http://www.diritto24.ilsole24ore.com/avvocatoAffari/mercatiImpresa/2013/02/google-versus-vividown-atto-ii-ecco-le-motivazioni.html.

133. *Draft Proposal*, *supra* note 4 at 93.

134. Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing*, 2012 01037/12 (WP 196) (EN), *available at* ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (last visited Aug. 28, 2013).

135. *Id*. at 2 ("[C]loud computing services can trigger a number of data protection risks, mainly . . . insufficient information with regard to how, where and by whom the data is being processed/sub-processed.").

136. *Id*. at 6.

137. *Id*. at 7.

138. *See* discussion *supra* Part I.C..

believe that personal data processed by means of cloud computing techniques fall under the category of mobility data; in this respect WP 204 analyzes the transfer of data to third countries.[139] Various alternatives are examined. First, the possibility that the provider of cloud services is established in the US and has adhered to the Safe Harbour Rules.[140] Having signed up for the Safe Harbour is not sufficient; a contract has to be signed detailing duties of both controller and processor.[141] But the processor may be in a third country which does not provide adequate protection. In this case standard contractual clauses have to be signed.[142] Another alternative examined is the Binding Corporate Rules (BCR).[143] A significant improvement has occurred recently with the opening of the BCR procedures for data, which apply to employees as well as customers.[144] BCR are procedures adopted by Member States to allow mobility of personal data within a company that adopts a code of conduct, binding on its employees in any country in the world.[145] Once the BCR have been adopted, they have to be submitted to a competent data protection authority in Europe, as defined by WP 195.[146] This authority can negotiate on behalf of all the other authorities and, if necessary, can negotiate (along with two other authorities) the text of the BCR.[147] Once the BCRs are approved, each individual authority in any given country then authorizes the transfer of the data within the company, regardless of the country in

139. Article 29 Data Protection Working Party, *supra* note 134, at 17.

140. *Id*.

141. Council Directive, *supra* note 2, at 43.

142. Article 29 Data Protection Working Party, *supra* note 134, at 18.

143. *Id*. at 19.

144. For more information on Binding Corporate Rules, see *Overview on Binding Corporate Rules*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm (last visited Aug. 28, 2013).

145. There are over 30 multinational companies (including an international law firm) whose BCRs have been submitted to local authorities and have been approved. For the full list see *List of Companies for Which the EU BCR Cooperation Procedure is Closed*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last visited Aug. 28, 2013).

146. The WP29 published WP 195 in 2012 with its recommendation on a standard form for approval of the BCRs. Article 29 Data Protection Working Party, *Working Document 02/2012 Setting Up a Table with the Elements and Principles to be Found in Processor Binding Corporate Rules*, 2012 01037/12 (WP 196) (EN), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf (last visited Oct. 5, 2013).

147. *Id*.

the world where the data shall be transferred to.[148] This is the perfect procedure to follow in case of cloud computing processing of personal data. In this respect the issue of "where are my data" becomes meaningless, since the data can circulate freely within the organization. There are drawbacks, of course (e.g. the use of subcontractors can be an issue), but the main advantage is the forum shopping; a company can choose the lead authority of the country it prefers and negotiate with it. Adopting a BCR is a much more powerful and reliable way of transferring data (regardless of the use of cloud computing), since it is a simplified procedure and the advantages gained are significant. In addition, I strongly believe that establishing contact and communication with the local authority, regardless of the country one operates in, is always positive and gives added value to any other process related to the evaluation of how personal data are being processed.[149]

CONCLUSIONS

Presently, EU data protection legislation does not address mobile technology as such. There is no definition of what mobility data are, and none is called for in the draft Regulation presently being debated. Only the WP29 has examined some aspects of mobility data, but in a very general fashion[150] at the outset and only to analyze the issue in more detail very recently.[151]

This unsatisfactory status is reflected in the little attention given so far to the processing of mobility data by national authorities. This may not be an issue by itself, but leaves significant questions yet to be answered.

The main issue is the following: mobility data are regulated by the Data Protection Directive (Directive 95/46/EC) which is based mostly on the Strasbourg Convention. The Strasbourg Convention

148. The WP29 has published several documents on BCRs, namely WPs: 74, 107 and 108 between 2003 and 2005; more recently, in 2008, three new documents have been published: WPs 153, 154 and 155. *Opinions and Recommendations*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2 (last visited Aug. 28, 2013). For a comprehensive listing of the WP29's documents see *id*.

149. Article 29 Data Protection Working Party, *Explanatory Document on the Processor Binding Corporate Rules*, 2013 00658/13 (WP 204) (EN), *available at* ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf (last visited Aug. 29, 2013).

150. *See* discussion *supra* Part III.

151. Article 29 Data Protection Working Party, *supra* note 32.

was signed in 1981, and everyone with some experience in this field knows that an international treaty of this kind is between 3 to 6 years in the making. This means that the Strasbourg Convention reflects the IT world of the mid-seventies when distributed processing, the first form of networking that developed in contrast to the dominance of the IBM mainframe architecture, was barely emerging. In few words, this means that a technology that has emerged and evolved in the third millennium is subject to a law which is not simply obsolete, but was conceived in an era when mobile phones, GPS, tablets and the like simply did not exist. This is what I mean when I say that the present status is unsatisfactory. Legislators, therefore, have to wake up quickly and act, if they are serious about protecting the privacy rights of the citizens.

Having said this, in the wake of the new Regulation, controllers better clean up their act in this field. Faulty information notices (if any at all), refusal to answer any questions whatsoever by the part of the data subject, a general attitude that gives the impression of lack of care on the themes of privacy is not acceptable and is something that, under the new Regulation, may be very costly.