Privacy in (mobile) telecommunications services

PENDERS, Jacques <http://orcid.org/0000-0002-6049-508X>

Citation:

PENDERS, Jacques (2004). Privacy in (mobile) telecommunications services. Ethics and Information Technology, 6 (4), 247-260. [Article]

Privacy in (mobile) telecommunications services[1]

Jacques Penders,
Sheffield Hallam University

Address: J. Penders
Howard Street
Sheffield
S1 1WB
UK

e-mail: J.Penders@shu.ac.uk
0114 225 3738 (work)
0114 278 1180 (home)

[1] Parts of this paper have been presented at Ubicomp 2002 in Goteborg and E-CAP 2003 in Glasgow.

Privacy in (mobile) telecommunications services

Abstract

Telecommunications services are for long subject to privacy regulations. At stake are traditionally: privacy of the communication and the protection of traffic data. Privacy of the communication is legally founded. Traffic data subsume under the notion of data protection and are central in the discussion.

The telecommunications environment is profoundly changing. The traditionally closed markets with closed networks change into an open market with open networks. Within these open networks more privacy sensitive data are generated and have to be exchanged between growing numbers of parties. Also telecommunications and computer networks are rapidly being integrated and thus the distinction between telephony and computing disappears. Traditional telecommunications privacy regulations are revised to cover internet applications. In this paper telecommunications issues are recalled to aid the on-going debate.

Cellular mobile phones have recently be introduced. Cellular networks process a particular category of traffic data namely location data, thereby introducing the issue of territorial privacy into the telecommunications domain. Location data are bound to be used for pervasive future services. Designs for future services are discussed and evaluated for their impact on privacy protection.

Key Words: Ethics, Privacy, telecommunications, data protection, traffic data, location data

Introduction

The aim of this paper is to examine current privacy regulations in telecommunications and to explore privacy requirements for future services. We will not extensively define the concept of privacy, but just strive towards an operational notion of privacy to serve the investigations. As a starting point we take the well-known notion of privacy as 'the right of the individual to be let alone' introduced by Warren and Brandeis[2] in 1890. That this notion applies is obvious, a ringing phone intrudes our lives in the sense that it is compelling us to interact with others at moments not decided by ourselves but by the caller. However, telecommunications technique is rapidly developing and together with these developments the moral issues change. A modern mobile phone has an on/off button which enables us to determine ourselves whether we would like to be disturbed or not.

Telecommunications are since long subject to privacy discussions[3], not so much for questions about the ringing phone but for the sensibility of the information that can be extracted from telephone services. As a result, telecommunications used to be surrounded with high protection and security barriers to ensure the privacy of the communication, but also to hide the so-called traffic data – that is data generated in the technical process of setting up a connection.

[2] S. Warren and L.Brandeis, The right to privacy, *Harvard Law Review* 4: 193-220, 1890.

[3] However, the debate was mainly held amongst specialists, refer to Willem F. Korthals Altes, Telecommunications, Itemization and Privacy: Some Developments in the EC and the Netherlands, *Media Law & Policy Bulletin* Vol. II, No. 1, 3 (1993).

Since the fast spread of Internet and its companion the World Wide Web, a public debate on privacy in information and communication technology (ICT) has emerged. Traditional telecommunications privacy issues have revived to cover Internet applications. This point is in particular pursued by the European Union; specific telecommunications regulations are reinterpreted to widen their scope of application towards all electronic communication services, including the Internet[4]. The discussions by no means have reached a final state, and recalling the telecommunications issues seems useful for the on-going debate. Interesting for the privacy discussion is also that the emerging telecommunications technology not just creates new problems but also relieves of older problems. Moreover, since 11 September 2001 the traditional privacy protection in telecommunications is under pressure[5].

There are more reasons to recall telecommunications issues. The telecommunication service area is changing rapidly. The introduction of the mobile phone in the last decade is an obvious example. In mobile telephony, while the mobile user is on-line, the actual geographical position of the user is known. These data are being made available to generate so-called location-based services, for instance, a service to guide you to the nearest parking spot. However, inadvertent disclosure and subsequent abuse of location data might violate basic privacy rights. Reception of the location data might, for instance, guide a malicious receiver to a physical confrontation with the victim, a clear case of infringement of the ‘right to be let alone’.

Less obvious, but basic to the discussion in this paper, is that telecommunication technique is evolving towards open systems, systems where multiple parties are enabled to cooperate in order to provide (complex) telecommunications-based services. By doing so the traditional security barriers are holed.

The distinction between a telephone and a computer is disappearing; computers can be used as a telephone. Wireless computer networks have been introduced and mobile phones are extended to comprise computing power and television like displays. Integrating mobile telephony and computing opens a whole new range of services, modelled after Internet services. Currently, a new generation (so-called 3G) of telecommunications service networks is in development in which the (terminal) devices are assumed to be a mixture of computers and phones. With regard to the 3G services, this paper precedes their implementation, as the systems are not yet in operation. The aim is to open the discussion at an early stage. Thus, we explore possible future problems, and discuss leads for solutions. Solutions are preferably found in applying so-called Privacy Enhancing Techniques (PET)[6]. We show with examples that easily obtained changes in the technical design lead to important gains in terms of privacy protection.

The paper is organised in two parts: Privacy in Current Telecommunications and Privacy and Advancing Technology. Part one recalls and explains the privacy issues within current telecommunications; central is the notion of traffic data. We explain what traffic data are and

[4] Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. *Official Journal of the European Communities*, C113 E, 14-5-2002 pp. 39-53. We refer to this directive as [EU 2002/58/EC]. Refer in particular to the 'Whereas clause (4)'.

[5] At stake is what is called 'Data Retention', we return to this issue later on.

[6] S. Kenny and Borking J.J., The Value of Privacy Engineering, *The Journal of Information, Law and Technology* (JILT), 2002 (1).

what makes them relevant for the privacy discussion. The second part of the paper reviews the issues, as they will appear in the advancing telecommunications technology. Location data are playing a central role in the technical developments, but also raise important privacy issues.

Part 1, Privacy in Telecommunication Services

The notion of privacy

In Europe, privacy is a human right, defined in Article 8 of the 1950 European Convention of Human rights: *"everyone has the right to respect for his private and family life, his home and his correspondence".* The right being given (to European Union subjects, but also in nearly every country in the world[7]) there is no urgency to extensively defend its basis in this paper. Generally, it is believed that privacy is vital to the individual, because it promotes "human growth, development and personality". "When we can shield ourselves from others we are able to learn better, to develop intimate relationships with others, to relax and promote our mental health". Moreover, "the more privacy we have, the less we feel under social pressure to conform, which adds to our mental health."[8]

The right to privacy is given, but what exactly is privacy? More in particular, what aspects are at stake in the context of telecommunications and ultimately what has to be done in order to respect and protect privacy? The starting point for the discussion is the notion of privacy formulated by Warren and Brandeis in their article of 1890, as the 'right of the individual to be let alone'. Warren and Brandeis considered privacy protection as consisting of not publishing certain information. It is interesting to note what matters they considered: "*The matters of which the publication should be repressed may be described as those which concern the private life, habits, acts and relations of an individual*". This circumscription is reflected in the following recent definition of privacy. Privacy is: "*The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information*."[9] This definition states a right to be protected, implying that others then the subject have the duty to protect. And indeed protection is central in telecommunications privacy.

In their worldwide surveys of privacy the Electronic Privacy Information Centre and Privacy International distinguish four concepts of privacy. They are: "*Privacy of communications***,** which covers the security and privacy of mail, telephone calls, e-mail and other forms of communication; *Bodily privacy*, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches. *Information privacy*, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. This concept of privacy is also known as 'data protection'. And the last one, *Territorial privacy*, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space".[10]

Making a step ahead of the telecommunications discussion we point out which of the four privacy concepts apply. *Privacy of communications* designates confidentiality of communications. The communication traditionally covered letters and in telecommunications

[7] For instance refer to Global Internet Liberty Campaign [http://www.gilc.nl/privacy/survey/], or the annual privacy survey by Banisar et al. '*Privacy & Human Rights*' published by EPIC and PI.

[8] D.P. Michelfelder, The moral value of informational privacy in cyberspace. *Ethics and Information Technology* (3), pp. 129-135, 2001.

[9] David Calcutt, Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, page 7.

[10] Banisar et al., *Privacy & Human Rights 2002,*p 3.

conversations between users. Nowadays it is extended to include all types of digitised information exchanged[11] and is often referred to as the 'content'. Privacy of communications is in many countries a specifically described constitutional right[12]; which we will not further discuss. *Bodily privacy* hardly applies in telecommunications. Though one might find exceptions for instance where equipment and radio techniques are concerned, it is excluded from the current discussion. *Informational privacy* or data protection covers confidentiality of traffic data and is the main issue of the present discussion; we will go into it shortly. The fourth concept is *territorial privacy,* which seems not to apply directly. However, mobile telecommunications services use location data. While the mobile terminal is active, the actual position of the user is known[13]. Inadvertent disclosure and subsequent reception of this information might guide a malicious receiver to a physical confrontation with the victim; we take this up in the second part of this paper.

Traffic data

The telecommunications companies (of Western Europe) developed in connection with the mail services. The privacy regime of telecommunications has its origin in the confidentiality surrounding mail serves.[14] Confidentiality regulations surrounding mail services are known to exist at least since the 16-th century, but probably much earlier. At the core is and was the confidentiality of the mail. However it comprises more; already in the 16-th and 17-th century not only the letter itself, but also traffic data such as the addressees' names and their addresses were considered highly sensitive (business) information[15] requiring protection and confidentiality. These confidentiality aspects have survived in modern laws and regulations concerning postal services[16] but also migrated to the telecommunication services area. Along its development, national laws and regulations extensively regulated the telecommunications services. Nowadays within the European Union, the European Commission initiates and supervises the regulation, issuing directives concerning telecommunications and privacy.[17]

As is clear from the letter mail services, traffic data are generated to direct the communications. We will briefly explain why traffic data is generated in telecommunications. For convenience the explanation is restricted to traditional fixed line telecommunications, which is still a paradigm for new technologies. Privacy relevant particularities of new technologies are added where appropriate. We first explain the technical process of setting up a telephone connection; this process generates so-called signalling data. Signalling data are at the basis of the more casual notion of traffic data.

[11] '*Communication*' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service [EU 2002/58/EC].

[12] For instance in the Netherlands' constitution "Grondwet, artikel 13", moreover it is described in Article 8 of the 1950 European Convention of Human rights.

[13] Below, in the last section we will explain how and why mobile systems use location data.

[14] Postal and Telecommunications trafic data are still treated similar in, for instance, the UK's Regulation of Investigatory Powers Act 2000.

[15] As a result couriers were forbidden to show addresses to others: thus blocking mail exchange between (professional) couriers [Penders, 1999].

[16] For the Netherlands refer to the 'postwet' (Postal service Act).

[17] For convenience, this paper is based mostly on the situation in the European Union. The reason being that the developments in the EU are rather well documented and moreover it is not in the scope of this paper to investigate regional differences. For an overview of the European regulations, refer to [http://europa.eu.int/ISPO/infosoc/telecompolicy].

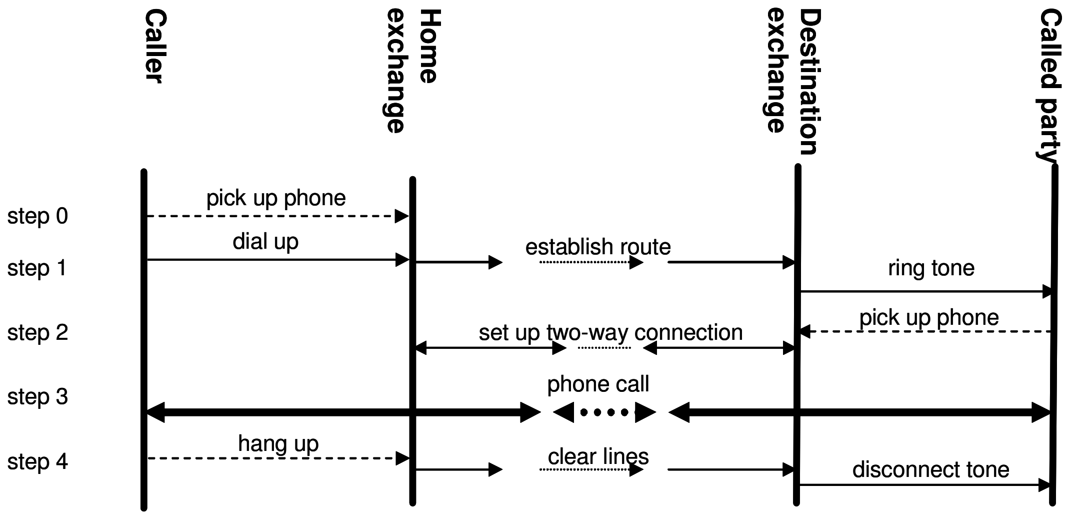

Figure 1, the process of making a telephone call

A telephone call starts with picking up the phone [step (0) in figure 1] and ends when either side puts the horn down [step (4)]. By picking up the phone a connection is made to the telephone exchange (called the home exchange). In step (1) the caller dials a phone number that is used by the home exchange to determine a route towards the destination; the exchange then attempts to contact the destination exchange (possibly via several intermediate steps). The destination exchange triggers the ring tone of the destination terminal (phone). Step (2) starts when the called party answers the phone. Stepwise the connection is set up starting at the destination along the route determined in step (1) (but in reversed order) to the caller. In step (3) the connection is used: the two parties have their conversation or whatever. In step (4) after the horn is put down at either side, the lines used for the connection are one by one released.

Important is the distinction between signalling (steps 1, 2, and 4) and the conversation itself (step 3). Step 3 takes place at a different level. For instance in the mobile telephony GSM, the steps (1, 2, and 4) transmit data over a separate channel[18] different from the channel used in step (3). Thus, signalling data is a technically distinct category of data, differing from the communication. In telephony, if any one happens to overhear an arbitrary conversation in step (3), he does not know who is calling whom: no signalling data, neither the calling nor the receiving number is included[19].

Signalling data are purely technical information and as such hardly interesting. However, this changes when the data are combined with other sorts of information. The calling number and the dialled number of step (1) and the start time of the connection in step (2) as well as the ending time of the call in step (4) are stored in a so-called Call Detail Record (CDR). For the calling line, these CDRs are collected over a period of time to calculate a bill. The term 'traffic data' refers to any combination of signalling data and number information, with a CDR in the core. Note the all-encompassing EU definition of traffic data: "*any data processed*

[18] In fact the same channels that is used for SMS.

[19] To have access to this information certain switches at the exchange have to be turned over, access to these switches as well as the conditions under which they may be used is regulated by law, see part 2 of this paper.

for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof."[20]

Traffic data is sensitive with regard to privacy and indeed, traffic data has been the source of extensive discussions concerning privacy, as we show by some examples. Before discussing the examples, we note that in telecommunications the subject of traffic data is a telephone number, which is not always the same as a person. A regular distinction is that between a user and a subscriber. The '*user*' means any natural person using a service, whereas the '*subscriber*' is the legal entity that is party to a contract.

In Europe[21], telephony exchanges that can produce CDRs automatically were introduced in the network at the end of the eighties and beginning nineties. An important advantage of the automatically generated CDRs is that an itemised telephone bill can be produced[22] in which every called number can be specified. The bill is send to the subscriber, and gives him insight into the calling behaviour of the users[23]. Compromising situations might occur within a household consisting of several users; this resulted in Germany into the requirement that all adult family members have to give consent, before an itemised bill can be asked for[24].

Other examples showing the relevance of traffic data are cases of so-called '*heavy breathers'*, generally called malicious calls[25]. In the eighties cases were reported where victims sought relief by their telecommunications operator, without the operator being very helpful. At the time, it was technically rather complicated to trace telephone calls. However, the modern telephony exchanges that automatically produce CDRs also enable so-called calling line identification. In a modified form, calling line identification is currently provided as a public functionality enabling display of the calling line number. In short, the equipment nowadays suits to easily trace down malicious callers upon request by the victim, so that specific measures can be taken[26] which generally speaking are quite effective.

Privacy protection

To summarise, the privacy issues in telecommunications concern the communications as well as the traffic data. Privacy of the communication is a well-established right. Communications are made purposefully but are transient in a normally operating telecommunications network. Traffic data serve technical purposes, are generated beyond the users control and are stored. Traffic data reveal with who and when we are in contact. In terms of Warren and Brandeis[27] traffic data reveal our 'habits and relations'. Thus, in telecommunications the right of privacy comes down to: *the right to be protected against intrusions into one's personal data.*

What should the protection consist of? Thompson[28] argues that protection (or security) requires secrecy of information, as secrecy ensures avoidance of risk for "malicious intent".

[20] [EU 2002/58/EC].

[21] In the USA this practise existed already for longer times, refer to Korthals Altes op. cit..

[22] Refer G. Huitema and P. Cramer, Itemised telephone bills*, Studieblad PTT Telecom* juli/augustus 1992 (in dutch). The paper describes the introduction of itemised bills in the Netherlands.

[23] This is partly true for mobile telephony, with so-called pre-paid or pay-and-go services the pre paid account is charged and no bill is issued; note that in this case the 'subscriber' might remain anonymous.

[24] An example is presented by Deutsche Telekom at http://www.telekom.de/dtag/downloads/Einzelverb.pdf.

[25] For an impression of the annoyance caussed refer to T.S Fernando, The Malicious Caller and The Telephone Agony Nov, 2000 http://infolanka.com/org/diary/99.html.

[26] Refer to British Telecom http://www.bt.com/customerservices/cust_services.jsp for examples of measures.

[27] refer to the citation of Warren and Brandeis given earlier.

[28] Paul B. Thompson, Privacy, Secrecy and Security, *Ethics and Information Technology* 3, 13-19, 2001.

Secrecy can be achieved in two ways; either no data are collected (and stored) so nothing can become known or if data are present lock them away. In the European Union the basic privacy regulation is the European Data Protection Directive[29]. Telecommunications is covered by the DPD and the directive is worked out in a directive entitled '*the processing of personal data and the protection of privacy in the electronic communications sector'*. [30] The DPD addresses data collection as well as data protection. Data collection is allowed only if for a particular (and legal) purpose (read: service); moreover any party collecting or storing personal data is responsible for these data. The responsibility includes protection of the data. Concerning traffic data in telecommunications some further obligations and limitations are described. Traffic data should be erased as soon as they are no more needed for transmission purposes. An exception is made for data necessary for billing (and interconnection payments), for these purposes traffic data may be stored and processed up to a fixed time limit[31]. These regulations concern the processing of data without the consent of the data- subject. Of course, once consent of the data-subject is obtained more processing is allowed.

Computer Networks

The above has given an overview of the current privacy issues in telecommunications. Before jumping to the impact of advanced telecommunications technology on privacy, a short note concerning the Internet. Within the European Union the telecommunications' privacy regime has been enlarged to include computer networks as well. However there are differences between a telephony network and the Internet. In the Internet (technically called TCP/IP applications) 'signalling' information is send out via the same channel as the communication; refer for instance to the header of an email. The reason is technical: the route for forwarding communications is determined en-route. Thus, the distinction between the communication and traffic data -so clear-cut in the case of telecommunications- is blurred[32]. If anyone in the general public happens to intercept the e-mail, the communications as well as the traffic data are received.[33]

A difficult issue in computer networks concerns unsolicited messages or Spam. Basically unsolicited messages do occur in telephony, however the origin of a message is quite well traceable (refer to the discussion on malicious calls) which turns it into a manageable problem.

Part 2, Privacy and Advancing Technology.

Changing environment

Until recently the market in the telecommunications services area was relatively simple. Most European countries had a single state-owned telecommunications company. As discussed above, technically speaking there used to be no reason to export the (traffic) data out of the network of the operator, except for international calls. Thus, the telecommunications network

[29] [EU 95/46/EC] Directive 95/46/EC 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. *Official Journal L 281 , 23/11/1995 p.0031 – 0050.* Often refered to as the Data Protection Directive (DPD)

[30] [EU 2002/58/EC]

[31] [EU 2002/58/EC] Time limits vary per country, for instance six months in Germany, three years in Finland and Ireland, five years in Spain; refer to http://wiki.ael.be/index.php/OverviewDataRetention.

[32] A consequence is that to comply with data retention regulations (discussed later on) Internet operators (ISPs) have to process emails in order to extract traffic information .

[33] The fact, that communications contain 'traffic data' is the drive behind sniffing on the Internet, sniffers first scan the communication for interesting clues and if something of interest is found then the header points out a way to use it; refer to Ryan Russell, *Hack Proofing your Network*, Syngress Publishing 2000.

could operate behind the doors of these (governmental) companies. Moreover, privacy protection also consisted of hiding the communication and the traffic data within the company's systems and behind the company's doors. Because of the simple market situation, these companies could easily be addressed for any problems, including those concerning privacy.

However, this situation is drastically changing as currently profound changes are in progress in the telecommunications sector. Of course, these processes are not restricted to Europe, but they happen to be rather well documented within the European Union. The reason being that they are strongly encouraged by the European Union[34] and thus well reflected in EU policies.

There are two - mutually influencing - mainstream developments. The first is that of the 'liberalisation' of the telecommunications services[35], and the second is that of the 'open network provision' (ONP)[36]. The aim of liberalisation was to break down the monopolies of the state owned telecommunications companies. And indeed, it has had this effect, the monopolies were broken and other service providers became active. The aim of open network provisioning was and is to provide access for third parties to the telecommunications infrastructure at various levels. It started at the far end by defining an open market for telecommunications terminal equipment[37] as a result a European user can nowadays connect nearly any device of whatever manufacturer to his telephone line. After the terminal equipment, soon followed the liberalisation concerning 'interconnection'[38]. Interconnection concerns roughly the connections behind the telephone exchanges by which telecommunications networks are connected. A major issue at this very moment is the opening up of the 'local loop[39]', simply said that is the connection between the private home and the home telephone exchange. Referring to figure 1, the processes on the far left and right hand sides of the diagram use the local loop, while interconnection concerns the middle part indicated by dotted arrows.

The effect of the liberalisation and ONP on current telecommunications services is that whereas before there was only one (state owned) company having full access to and control over the telecommunications infrastructure and its operations, nowadays there are several companies with interwoven infrastructures and operations. As a consequence, to operate their services and in order to be able to bill for services, these companies have to exchange traffic data[40]. The importance for the privacy discussion is clear: traffic data must be made available to many more parties and thus simply shielding the network to conceal the data isn't possible anymore.

Confidentiality of Spheres of Life

Exchange of traffic data has become a prerequisite to enable services; nevertheless confidentiality of the data has to be maintained. The confidentiality to be sought for should be

[34] For a brief overview, as to why the European Union became so much involved, refer to Korthals Altes op.cit..
[35] refer to [EU90/388/EEC] Commission Directive of 28 June 1990 on competition in the markets for telecommunications services. *Official Journal* L192/10, 24.07.90
For developments in the USA refer to the Telecommunications Act of 1996, http://www.fcc.gov/telecom.html.
[36] [EU 98/10/EC]
[37] [EU 88/301/EEC] Commission Directive of 16 May 1988 on competition in the markets in telecommunications terminal equipment, *Official Journal* L 131 , 27/05/1988 P. 0073 - 0077.
[38] refer to the Interconnection Directive 97/33/EC.
[39] refer to EU Regulation No 2887/2000 of the European Parliament and of the Council of 18 December 2000 on unbundled access to the local loop, *Official Journal L 336 , 30/12/2000 P. 0004 – 0008*
[40] The necessity to exchange data derives from the protocols used, refer to the section on traffic data above.

a relative concept. And indeed, we do not mind that our traffic data are used to calculate an accurate telephone bill: we even expect this, but on the other hand we certainly object when we are asked why we made a call to a certain phone number. The point of confidentiality is that the use of our traffic data should be restricted to having the phone line operating properly and calculate a valid bill, and the data should only be used for these purposes. The relative confidentiality of data can be captured by the rule that the data are to be used freely within the sphere of providing a service but should remain concealed to the outside of this sphere.

In fact the principle of relative confidentiality applies to many areas of life. Generally, we conceive of our life as separated in quite some spheres, our medical sphere, our private home, our friends, our colleagues, the grocery shop, insurance company, the telecommunications service provider. In each of these spheres, we reveal data about ourselves, let our doctors collect medical data, we discuss intimate facts with friends, we reveal our shopping list when buying products etc. However, accessibility of our data should be restricted to this sphere: the insurance company should not have access to our shopping list etc. On the other hand, we expect that within a sphere, data be exchanged; in the medical sphere, we expect that our medical attendants take notice of all available medical information about us before starting a treatment. As proposed by van den Hoven[41] we might consider it as an adaptation of Walzer's notion of "Separate spheres of justice" to the notion of privacy. The relative confidentiality of data complies to the **confidentiality of spheres of life**, or the rule that *separate spheres of life should remain separate, and that our personal data should not be exported from the sphere where they were generated*, unless we ourselves reveal the information. In particular in cases where we cannot control the information flow ourselves, we expect and even have the right that the rule is respected. The definition of privacy as 'the interest we have in denying to others the ability to secretly track our comings and goings'[42] is based on the expectation that the separate spheres of life are closed. The 'others who secretly track' refers to parties who are trying to cross borders between the spheres of life.

Returning to the sphere of telecommunications, we consider who might intrude into our data. It is useful to make a distinction between the general public and law enforcement agencies or between the *'public'* aspect of privacy and the more hidden '*national security'* aspects of privacy. The arguments for protection of personal data surely hold when the intrusions might come from just some member of the public, irrespective of their intentions; as long as no consent is given, personal data should not be publicly accessible! The situation is more delicate when law enforcement and national security are concerned. Privacy provides the individual on the one hand the privilege to withdraw from the public, but on the other hand it also allows the individual to conceal. In the interest of society, law enforcement agencies have to trace (suspect) individuals and are legally provided with means to do so. At this point the right of the individual to privacy has to be balanced against the community's interest for safety.

Where law enforcement is concerned the difference between communications and traffic data is crucial. *Lawful interception* is (in telecommunications) the tapping (and storing) of communications. Telecommunications providers have to ensure that access to the connections is possible[43]. Since Lawful Interception is overruling the right to privacy of the

[41] Jeroen van den Hoven, Privacy and the varieties of informational wrongdoing, *Australian Journal of Professional and Applied Ethics*, vol. 1, no. 1 (1998), pp. 30-43).

[42] D.P. Michelfelder, op.cit..

[43] In the Netherlands: article 13 of the Telecommunicatie Wet; in the UK: Regulation of Investigatory Powers Act 2000.

communication, national law -often with a basis in the constitution- also stipulates how authorities have to proceed.[44] Roughly, the procedure is that legal authorities define the target, thereafter the law enforcement agency may intercept all this subjects' communications and the telecommunications operator is bound to provide proper access. When appropriately recorded the communication might also be used as evidence in a court trial. *Data Retention* concerns traffic data. As discussed above, telecommunication service providers have traffic data; law enforcement agencies request these data for tracking purposes. Important to note that in data retention no target is identified, it concerns all traffic data of all users. Data retention overrules the data protection legislation, but is not directly described in legislation: it is only indirectly allowed. The directive on privacy in electronic communications (Directive 2002/58/EC) for instance requires in article 6 that traffic data are erased; article 15.1 however makes exceptions by saying that legislative measures might restrict the scope of article 6. Briefly summarising data retention: no one is obliged to generate traffic data, but if there are data one is forced to store them to serve law enforcement. The tragedy of September 11, 2001 revived the public privacy debate concerning data retention, and in particular the period for which operators have to store traffic data.[45]

The main subject of this paper is the protection of the privacy of the individual against the public; we will not further dig into the law enforcement aspect. The public aspect of privacy can be dealt with without necessarily choosing a position with respect to the national security aspect, that is to say, presupposing that the sphere of law enforcement is closed and sealed.

Envisioning Technology

As discussed above, telecommunications technology has changed enormously. The combination of telecommunications and computing technology has resulted in the Internet and the World Wide Web. In parallel, mobile telephony was for the first time introduced and is already developed into a consumer service. Developments proceed, recent technical developments aim towards integrating mobile telephony with wireless computing. Thus as is already the case in fixed telephony, the distinction between a (mobile) telephone and a (handheld) computer as terminals of a (mobile) communication network disappear. In the case of mobile telephony this opens up a whole new range of services, modelled after Internet services, but with far more opportunities.

In a vision document-called Freeband- presented by the Dutch Ministry of Economic Affairs the developments are described[46]. Central in this vision document is the idea of a user being always and everywhere surrounded by a so-called 'information cocoon'. The realisation has to be worked out yet, but the major functionality is described in the vision document: *"Regardless of position and movements, the user has all desirable communication at his disposal…. The user carries –literally and figuratively- an unambiguous and unique communication profile with him, which permits differing adjustments depending on the preferences associated with a given time and place and suiting the occupation at that moment. … he can navigate through the complete communication and information landscape …. He is not phoning, e-mailing, internet surfing or watching TV, but* ***he is just always in contact****..."*

This citation typically contains all the aspects of current developments where it says that the complete communication and information landscape is available. It assumes that open network provisioning (ONP) is fully realised and even enables to switch between networks

[44] For details refer to standardisations on Lawful Interception by the European Telecommunications Standards Institute; http://www.etsi.org/ or http://portal.etsi.org/
[45] For details refer to http://www.epic.org/privacy/intl/data_retention.html.
[46] refer to www.cic-online.nl/files/VrijBand_eindrapportage.pdf (in Dutch).

such as fixed telephony, mobile telephony and TV channels. Moreover, it presupposes that operators of different networks and information services providers all ‘cooperate’ in realising the envisaged value added services. In fact technical standardisation forums are currently defining functionalities to exchange traffic data on-line between different networks[47].

Location-based services

We will not challenge the Freeband vision for whether it is fully realisable. The vision however is quite explicit in that the user can use all services irrespective of whether he is on the move or just at home. It is at this point that an important privacy issue is at stake. In order to set up and maintain a connection, the network needs location data, and when switching between networks (as is an important aspect of the vision) the need for location data increases, as we explain below. Location data is basic to the Freeband vision, and it is exactly location data that introduces territory privacy as an issue in telecommunications. A mobile device is intended to be taken by the user wherever he goes, but the device leaves electronic traces behind that mark the user’s geographical behaviour. In the remainder of this paper we look ahead at how location data might be used in new generations of telecommunications-based services and evaluate the consequences with respect to privacy.

Location Data

The European Union’s regulations state: *‘location data’ means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*[48]. We briefly explain why location data is necessary in a telecommunications service and then discuss the related privacy issues.

A telecommunications service is usually a two-way point-to-point connection of which the end-points need to be known, otherwise no connection can be set up. For a fixed telephony network this is obvious: before a connection can be established, a route has to be determined from the caller to the receiver so as to make a reservation on the intermediate fixed lines, refer to Figure 1. Since the lines are fixed, the route carries (implicitly) geographical data with it. A cellular network for mobile telecommunications –for instance GSM- works basically in the same manner, though the underlying techniques differ considerably. In a cellular network, the mobile terminal is wirelessly connected to a base station, one at a time. Within the service area of the base station the user can freely wander around while the radio-link to the base station is maintained. Cellular networks also have so-called ‘handover’ mechanisms, which allow a user - while wandering around - to move from the service area of one base station to that of another one.[49] Since it is known to which base station a user is connected also his geographical location is known.

In the Freeband vision cited above, a user is “just always in contact”. To appreciate the implications of this statement consider the following (imaginary) example of a user and his/her terminal. The user wakes up in the morning, and switches on the terminal, which at home is connected to the in-house wireless telephone unit. After breakfast, the user travels to work, while the connection is maintained via GSM. At work the terminal switches to the company’s wireless computer network. After work the user drops in at a friend’s, a pub and at the end of the day the user arrives back home and just before going to sleep disconnects the terminal. During the day, the terminal has several times switched networks, at each occurrence the network operator has collected location data. Moreover, the user wants all day

[47] Examples are the Open Service Archtecture (OSA) standard and Parlay, refer to www.parlay.org.
[48] [EU 2002/58/EC], section on definitions.
[49] This description is limited to a minimum, for a little more detail refer to Scourias.

to be reachable for others, so at least one of the service providers (or network operators)[50] must have an overview and keep track of where and on which network the terminal is reachable[51]. In fact this service provider has to keep track of the user's actual whereabouts. At the moment of writing this paper, it is not clear yet, how and by whom all these points will be resolved, nevertheless it is obvious that quite some privacy sensitive information has to pass around amongst network operators and service providers.

Network operators by technical necessity have to exchange location data in order to be able to provide the telecommunications service. This fact is of juridical importance; these location data are considered to be traffic data. In the European Union the generation of traffic data, and these location data, is considered as justified, refer to the definitions above. This type of location data, may further be used for "*the provision of value added services, to the extent and for the duration necessary for such services, if the subscriber or user has given his consent*"[52].

At this point it is useful to emphasise that there are location data that are not traffic data. For example a mobile terminal might be provided with a GPS-device to obtain accurate location data. Such data are not necessary to establish a telecommunications connection, and therefore reside under a different regime. The main point of difference is that in advance of acquiring the data the consent of the user or subscriber is required. "*The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service*". [53] Note that the generation of either category of location data is subject to serving a purpose.

We restrict the discussion to location data that are considered to be traffic data. This category is of most interest since network operators legally have these data available, while the user has not yet given consent on further processing, and further processing is needed to enable the 'just always in contact' concept explained above. The considerations however apply for non-traffic location data as well.

Service designs

The always-in-contact services involve many parties exchanging data. Moreover, the services might involve any aspect of daily life and thus data exchanges pervade all aspects of everyday life. Concerning privacy, a no-data exchange situation is not the case; but openness of systems not necessarily has to mean that all data are exported to or available to everyone. We obtain better confidentiality by minimising data collection and by minimising data exchange and exportation[54]. A better reading of openness is that functionalities are available to all parties who on behalf of the user have a need for them. From this point of view we study several designs for location-based services and show that privacy preferences can be taken into account and indeed make a difference.

[50] Note that, in accordance with ONP (refer to previous section), this function is not necessarily designated to a network operator

[51] In a GSM network, this function is assigned to the Home and Visitor Location Register, refer to J. Scourias op. cit..

[52] [EU 2002/58/EC], article 6.

[53] [EU 2002/58/EC], article 9.

[54] This idea is basic to privacy enhancing technologies (PET) Kenny and Borking 2001 op. cit..

The end-user services to be realised are of the type: “find me a near-by xx”. Where xx stands for a geographical spot: a shop, a restaurant, or an access point to another network[55]. Xx might also stand for another user[56], but the latter requires additional precautions, which we do not discuss in this paper. In each of the designs the same end-user services are obtained, while the designs differ considerably in how much privacy sensible data is exchanged between the participants in the service.

In the designs, it is supposed that a third party provides the (end-user) service; the third party is distinct from the telecommunications network operator. The network operator provides the basic communication links. Thus in the services at least three parties are to be identified, the user, the third party service provider (below denoted as *3-rd party*) and the network operator. Basic to the services are the location data of the user. The designs start from the point where the mobile phone is on the network. Referring to Figure 1, step 0 has been made and the network operator is therefore the (legitimate) source of the location data.

Two scenarios are possible, a so-called pull scenario and a push scenario. In a pull scenario the user initiates a request for service upon which the 3-rd party reacts: ‘the user calls the 3-rd party’. In a push scenario, the 3-rd party initiates sending a message that is ’the 3-rd party calls the user’. However in the latter, before doing so and in accordance with regulations (see above) the user first has to give his consent to the 3-rd party meaning that the user has to subscribe to the service in advance. Push scenarios are generally considered as means of commercial advertising and thus have the advantage that they are more likely to be free of charge for the end-user.

Push

We first consider push scenarios. We suppose the user has subscribed to the service and thereby given the required consent with regard to the data processing. The push designs 1 to 3 are drawn in Figure 2 to Figure 4. The bullets and the broken arrows connected to them depict the preceding (subscription related) actions. Our main interest is in the consecutive steps by which the 3-rd party gets his message delivered at the user’s terminal. For simplicity, we suppose the message to be send is ready. It might sound as “we have a great place for you…”. The point to discuss is how those users are found that are geographically close enough to be a target for this message.

In design 1 (Figure 2) the network operator sends the id’s of all terminals that satisfy the geographical conditions to the 3-rd party. The 3-rd party selects those that have subscribed to his service and sends them a message. In design 2, the 3-rd party has notified the network operator in advance which users have subscribed to the location service. So, at the moment(s) that the 3-rd party is ready to send his message, the network operator checks out which subscribed users are on-line in the geographical area, and returns the particular id’s. Upon receipt, the 3-rd party sends these users the message. In design 3, as in design 2, the 3-rd party has notified the network operator of his subscribers, and has send the prepared message. So at the relevant moment the network operator sends the message to the subscribed users.

[55] The scenarios, which we discuss here, also apply when switching between networks and setting up the first contact between terminal and access point. However, to simplify the discussion, we use the concrete example of a shop or restaurant advertisement, and return to the switching networks point later.

[56] An example is the Find Friends service announced by AT&T in Wired News, 27 june 2002.

Evaluating the designs from the perspective of obtaining the best respect for privacy by limiting export of data, obviously design 3 is preferred. In design 3, the 3-rd party does not receive any location data; all data remain with the network operator who is the source of the data. Design 1 is the worst in this respect, since location data of non-subscribers are forwarded to the 3-rd party. Taking the EU regulations[57] literally design 1 might not be legally justified. Design 2 is from a privacy perspective better, since only location data of subscribers passes from the network operator to the 3-rd party.

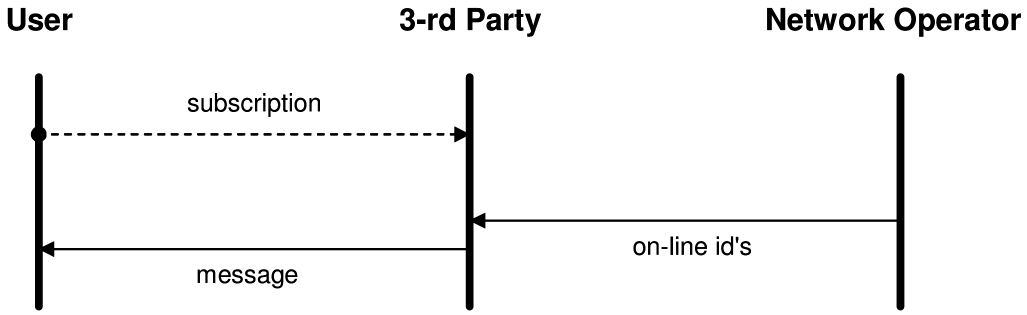

Figure 2, design 1: push scenario 1

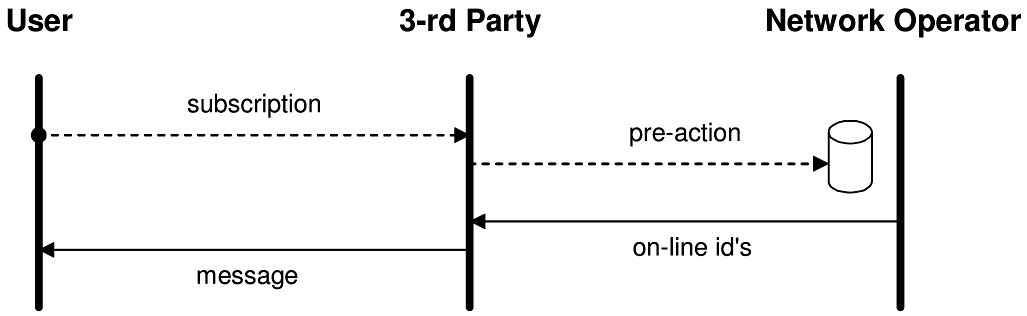

Figure 3, design 2: push scenario 2

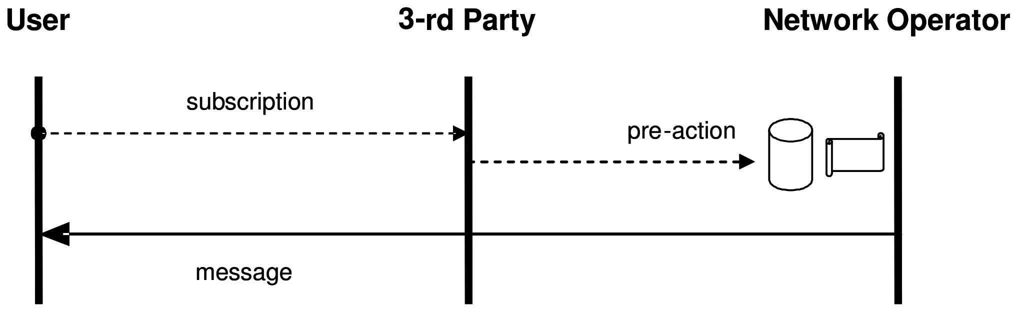

Figure 4, design 3: push scenario 3

Pull

We continue with the pull scenario. In a pull scenario the user has the initiative, and in doing so he gives his consent. Therefore, in the designs 4 and 5 in Figure 5 and Figure 6, all arrows are of equal nature. In design 4, the user contacts the 3-rd party with a request for service. The

[57] [EU 2002/58/EC]

3-rd party forwards a request for location data to the network operator, who returns the data and the 3-rd party completes the user's request. From the privacy point of view, this design is comparable to design 2 above: only selected data are passed to the 3-rd party.

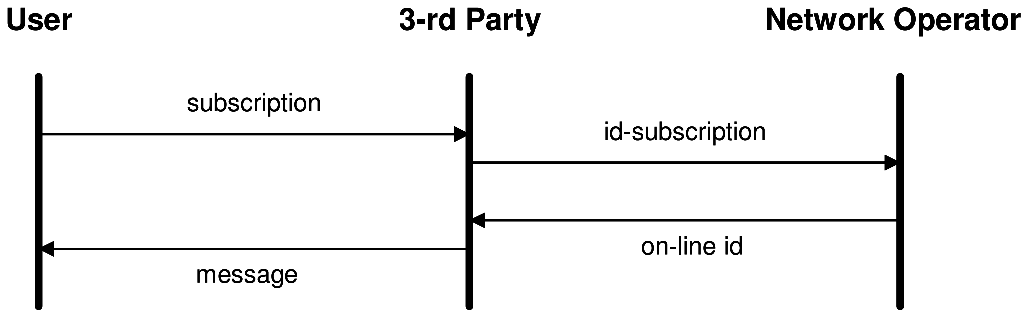

Figure 5, design 4: pull scenario 1

In design 5, the user contacts his (current) network operator and asks for his location data, which the operator returns. The user also contacts the 3-rd party with a request for service, and transfers his location data[58]. From a privacy perspective, design 5 is very nice: it provides the user control over his personal data.

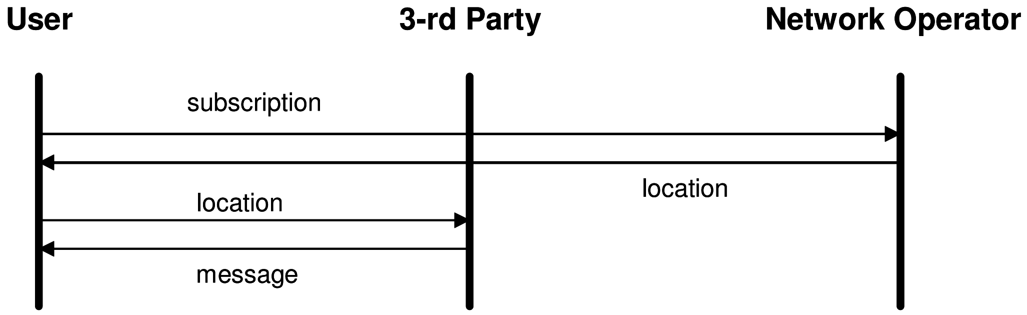

Figure 6, design 5: pull scenario 2

Evaluation

In the designs shown, it is assumed that the user is as much as possible in direct contact with the 3-rd party; therefore the third party is in the middle of the diagrams. The alternative would be to have the network operator play the role of the middleman. Many current GSM services are constructed in this manner. Network operators provide -via portals- additional services that originate from 3-rd parties operating in the background. The consequence of such designs is that the network operator is the client-contact point for the 3-rd party. The third party may not even know his clients, clients may remain anonymous. However, being the client-contact point the network operator plays a key role providing additional (business) power, which is not the intention of Open Network Provision. For this reason these alternative are not worked out in this paper.

Comparing the five designs from the privacy point of view, the last design (design 5) is clearly the one preferred, since the user himself is in control of his data. From a privacy perspective Design 3 is clear and transparent: no personal data are exchanged as no direct contacts are established between the user and the 3-rd party. The user remains anonymous to the 3-rd party; the drawback is that the network operator is granted the role of middleman. Designs 2 and 4 imply exchange of personal data, beyond the control of the user; alertness on

[58] We remark that this could be implemented on the terminal as a 'double click' function. By this supposition we aim to avoid discussions about the user's perception of the service.

privacy issues is recommended. Design 1 is straightforwardly a bad design: data of non-users are exported to a 3-rd party. Since design 1 is disputable from a juridical point of view, we leave it out of the discussion.

From the privacy point of view designs 3 and 5 are preferred. However, the perspective changes considerably if the 3-rd party is a network provider, one of the many that are needed to establish the 'always in contact' vision. Recall the example of a mobile user who is 'always in contact'; the user's terminal is assumed to switch between networks. To do so, the terminal has to find network access points in its vicinity and a protocol is needed to hand over services from one network to another.

To describe what might happen we can again distinguish between push and pull scenarios. In the push scenarios, the current network provider advises which alternative networks are available. Design 1 -which we discarded- would come down to listing all potential on-line clients to the 3-rd party. In design 2, the network operator indicates that some of the 3-rd party's clients are on-line and within reach and the 3-rd party may take over. In design 3 the network operator notifies the user that the 3-rd party network is available; the user may decide to connect to the 3-rd party. In the pull scenarios the user has come into contact with the 3-rd party network. In design 4, the 3-rd party contacts the network operator for information to maintain the communication session with the user. Design 5 differs in that the user requests the details and passes them on to the 3-rd party.

In designs 3 and 5 the user establishes his contact with the 3-rd party independent from the network operator, in designs 2 and 4 the network operator mediates. From a privacy perspective, designs 3 and 5 again would be preferred. However the strong points are also technical drawbacks. The designs require an extra step to establish direct contact between the user and the 3-rd party. From this point of view, the designs 2 and 4 are preferred because the user is from the first step directly in contact with the 3-rd party. Another point in the designs 3 and 5 is that the user completely disappears out of sight from the network operator; it is not difficult to imagine what problems this will create for a law enforcement agency. Designs 3 and 5 might therefore require addition measures to comply with legislation[59].

Over viewing the designs, it has become clear that in judging the design different view points have to be taken into account. From the privacy point of view user control over his personal data is preferred, however this might contradict the legislative requirements of traceability and interceptability. Minimal data exchange is the next option, however restricting data exchange might define and further establish the central role of the data owner (the network operator in the designs) in the business. Each design has advantages in some view point, but which advantage should count as decisive depends on the context in which the service is applied. What the discussion of the designs has shown is that privacy aspects have to be considered at the early stages, technology allows different options with varying privacy implications. In the 16-th century traffic data was considered sensitive business information, in the future mobile services traffic data still define business positions.

Conclusions:

Telecommunications services are for long subject to privacy regulations. Nevertheless the paper shows that privacy in telecommunications remains an issue for the future.

[59] Recall that communication services by law have to be interceptable.

Telecommunications services and computer applications are rapidly being integrated and thus the distinction between a telephone and a computer disappears. In particular in the domain of mobile telephony and mobile computing this enable a whole range of new services. However, this triggers new privacy issues.

In telecommunications the following concepts of privacy are traditionally at stake: privacy of the communication and the protection of traffic data. Privacy of the communication is a constitutional right. Traffic data are privacy sensitive as they reveal the behaviour of a user; traffic subsumes under the concept of 'data protection'. A particular category of traffic data is location data; the use of location data introduces the concept of territorial privacy into the telecommunications domain.

We have discussed the ongoing changes in the telecommunications environment, from a closed market of governmental companies operating technically closed networks, it evolves into an open market with several operators, operating technically open networks. Although confidentiality of traffic data applies, it is no longer straightforwardly obtained. To deal with the right to privacy in advancing telecommunications we introduced the notion of *confidentiality of spheres of life* to the discussion. To comply with this confidentiality, data should be used freely within the sphere of setting up and maintaining a service, but should remain concealed and not be exported to the outside of this sphere.

For the future, boundaries between networks are bridged, and the future user is envisioned as just being always in contact. From the privacy perspective this has the drawback that more privacy sensitive data are generated and also that more data have to be exchanged. Location data highly sensitive from a privacy perspective are basic for enabling the future telecommunications service perspective. Technology allows alternatives in the designs of the services. We have evaluated different design schemas from the point of relative confidentiality of data and shown their varying implications on privacy protection. However, to judge the designs different viewpoints have to be considered, advantages or disadvantages vary with the context of application. But, whatever considerations are decisive, we have shown that technology enables choices with varying privacy implications.

References

David Banisar et al., *Privacy & Human Rights 2002, an International Survey of Privacy Laws and Developments,* an annual survey first edition by David Banisar, the 2002-version edited by Sarah Andrews and Gus Hosein, published by the Electronic privacy Center and Privacy International, 2002.

Philip A. Brey, Methods in Computer Ethics: towards a multi-level interdisciplinary approach, *Ethics and Information Technology* 2, pp125-129, 2000.

David Calcutt, Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, page 7.

[EU 2002/58/EC] Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. *Official Journal of the European Communities*, C113 E, 14-5-2002 pp. 39-53.

[EU 98/10/EC] Directive 98/10/EC of the European Parliament and of the council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment (31998L0010) *Official Journal L 101 , 01/04/1998 p. 0024 – 0047* (A revision of [EU 90/387/ECC].

[EU 97/66/EC] Directive 97/66/EC of the European Parliament and of the council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. *Official Journal L 024 , 30/01/1998 P. 0001 – 0008*

[EU 95/46/EC] Directive 95/46/EC 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. *Official Journal L 281 , 23/11/1995 p.0031 – 0050.* Often refered to as the Data Protection Directive (DPD)

[EU90/388/EEC] Commission Directive of 28 June 1990 on competition in the markets for telecommunications services. *Official Journal* L192/10, 24.07.90.

[EU 90/387/EEC] Council Directive of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network provision *Official Journal L 192 , 24/07/1990 P. 0001 - 0009.*

[EU 88/301/EEC] Commission Directive of 16 May 1988 on competition in the markets in telecommunications terminal equipment
Official Journal L 131 , 27/05/1988 P. 0073 - 0077.

EU Regulation (EC) No 2887/2000 of the European Parliament and of the Council of 18 December 2000 on unbundled access to the local loop. *Official Journal L 336 , 30/12/2000 P. 0004 – 0008*

Jeroen van den Hoven, Walking the (Dutch) Shallows in a rising tide; thinking about Ethics and Information Society, Erasmus University Rotterdam 2000 (in Dutch; 'Wadlopen bij opkomend tij',).

G. Huitema and P. Cramer, Itemised telephone bills*, Studieblad PTT Telecom* juli/augustus 1992 (in Dutch).

S. Kenny and Borking J.J., The Value of Privacy Engineering, *The Journal of Information, Law and Technology* (JILT). 2002 (1).

Willem F. Korthals Altes, Telecommunications, Itemization and Privacy: Some Developments in the EC and the Netherlands, *Media Law & Policy Bulletin*
Vol. II, No. 1, 3 (1993).

Larry Lessig, David Post and Eugene Volokh, *Cyberspace Law for Non-Lawyers*, Topic: privacy 1: Privacy Law in Cyberspace, Electronic Frontier Foundation 2002. http://www.eff.org/Government/Legislation/Legal/CyberLaw_Course/cyberlaw.013

D.P. Michelfelder, The moral value of informational privacy in cyberspace. *Ethics and Information Technology* (3), 129-135, 2001.

Ryan Russell, *Hack Proofing your Network*, Syngress Publishing 2000.

John Scourias, A Brief Overview of GSM, *University of Waterloo*, http://styx.uwaterloo.ca/~jscouria/GSM/index.html or http://kbs.cs.tu-berlin.de/~jutta/gsm/js-intro.html.

Paul B. Thompson, Privacy, Secrecy and Security, *Ethics and Information Technology* 3, 13-19, 2001.

Anton Vedder, Accountability of Internet access and service providers – strict liability entering ethics, *Ethics and Information Technology* 3, pp 67-74, 2001.

S. Warren and L. Brandeis 1890, The right to privacy, *Harvard Law Review* 4 (December 15): 193-220, 1890.