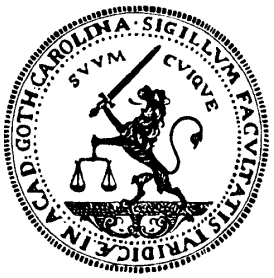

FACULTY OF LAW
University of Lund

David Sommestad

Personalization and/or Privacy?

A study regarding the protection of privacy
in personalized mobile services from an U.S. / E.U. angle

Master thesis
20 credits/points

Supervisors
Ulf Maunsbach and Michael Rustad

Field of study
Information Technology Law

Semester
Spring 2001

Abstract

M-commerce is the newest edition to the IT-society. The third generation mobile networks are being deployed in Japan, the U.S., and Europe. For mobile services to work, a certain degree of personalization is necessary. Personalization is already used in wired services, with the mobile Internet a new dimension of personalization is added; user location.
Personalization only works if personal data of the user is collected. This leads to questions regarding the protection of privacy.
The E.U. directive on data protection imposes strict rules on companies collecting personal data. U.S. companies who do business in Europe need to comply with the directive.
Central to both U.S. and E.U. legislation and policy is informing the user about personal data collecting activities. Users need to be able to understand collecting companies methods, and be able to disclose their privacy preferences. This is a problem in the wired world, and will be an even bigger problem in the wireless environment. The small screens on wireless devices are not suited for reading lengthy privacy notices. Users must be able to consent to their personal data being collected through a different channel. Whether or not this is made by technical means (on the wireless device), or before the services are being used, legislation (although necessary) should not hamper the evolution of m-commerce.

Table of Contents

Foreword / Acknowledgements

The work on this essay started a cold February day in Boston, MA. Six months later, I'm finishing off this project in Sweden. It has been an interesting journey; looking back I realize that better knowledge in high technology would have made this essay a lot easier to write. Other than that, I think it went along pretty smooth.

I would like to thank my supervisors, Professor Michael Rustad at Suffolk University Law School and Ulf Maunsbach at the University of Lund.

Special thanks to my father, Mats, whose financial support was crucial for my trip to Boston. I would also like to thank Mattias Malmnäs at Adaptlogic for explaining the techniques behind personalization.

Purpose of essay

My purpose with this essay is to elucidate the legal issues regarding privacy in a personalized mobile environment. Legislative measures in the U.S. and the E.U. will be described, emphasis will lie on how wireless users are informed about personal data collection, and how they can give consent to this collecting activity.

In order to personalize something, a vast amount of personal data on the user is needed. This raises questions about personal privacy and integrity.
Personalization will make life easier for the user, but is it worth sacrificing personal privacy for it? Does the positive effects of personalization outweigh the negative effects?

In order to enjoy the advantages of personalization, one has to give up some privacy. "More is better" when it comes to personalization. The accuracy will increase for each piece of data collected, and from each "touch point" this data is taken from. Clearly, users don't care about every kind of data collected, but when it comes to more sensitive information, or the amount of personal data stored reach a certain extent, some of us will say "no".
We all have different preferences as to how much privacy we are willing to give up. Some people are willing to give up more personal information than others. Today, users don't have much choice. Supply information or don't, it's either or.
As websites, digital ads, and wireless devices become personalized this will change. Companies will be forced to supply "personalized privacy policies". This raises a practical problem. How shall privacy preferences from users be disclosed in the wireless world?

Material / Method

M-commerce is a fairly new phenomenon in the IT-society. Literature on the subject is difficult to find. Instead I have relied on information found on the Web. Central to this study has been transcripts from workshops on the subject held by the Federal Trade Commission and the World Wide Web consortium; and Guidelines issued by The European Working party on Data protection and the The Cellular Telecommunications Industry Association (CTIA). Articles published in *Wired Magazine,* and reports from Forrester Reasearch have helped giving a marketers' view of the m-commerce world. One interview has been made, with the Marketing Manager of a personalization software developing company, giving me insights in the technological bit surrounding m-commerce personalization.

Definitions and Abbreviations [1]

15 U.S.C. – United States Code, title 15 (commerce and trade)

Bit - Binary Digit, the smallest unit of information on a machine. A single bit can hold only one of two values; 0 or 1.

Bluetooth - short-range radio technology aimed at simplifying communications among Net devices and between devices and the Internet.

Byte - One byte is composed of 8 consecutive bits.

CDMA - Code-Division Multiple Access, a digital cellular technology that uses spread-spectrum techniques.

Cell – Mobile cellular communications systems divide a geographic region into sections, called *cells.*

Clickstream Data – Data regarding web browsing. Includes page served, time, source or the request, type of browsers making requests, etc.

Cookie - A message given to a Web browser by a Web server. The browser stores the message in a text file. This message is then sent back to the server each time the browser requests a page from the server.

EDGE – Enhanced Data Rates for Global Evolution. Technique which can upgrade existing GSM/GPRS networks, giving three times improved frequency spectrum efficiency for data.

Enhanced 911 – FCC initiative aimed at making it easier for emergency workers to locate wireless 911 calls. The FCC requires that by October 2001, mobile service systems should be able to trace emergency calls to within 125 meters of their location.

GSM - Global System for Mobile communications. One of the leading digital cellular systems in the world. Uses narrowband TDMA, which allows eight simultaneous calls on the same radio frequency.

GPRS - a standard for wireless communications which runs at speeds up to 150Kbps.

HDML - Handheld Device Markup Language. Used to format content for Web-enabled mobile phones.

HTML - Hyper Text Markup Language, the authoring language used to create documents on the World Wide Web.

[1] Technical definitions found at www.webopedia.com ; an online computer technology encyclopedia supplied by www.internet.com

HTTP - Hyper Text Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

IP - Internet Protocol. IP specifies the format of packets, and the addressing scheme. IP by itself is something like the postal system, but there is no direct link between the user and the recipient. The current version of IP is IPv4, a new version called IPv6 is under development.

Kbps - Kilobits per second, a measure of data transfer speed. One Kbps is 1000 bits per second

Mbps - Megabits per second, a measure of data transfer speed. One Mbps is 1000 000 bits per second.

PIM - Personal Information Manager, a type of software application designed to help users organize random bits of information.

SMS - Short Message Service, the transmission of short text messages to and from a mobile phone, fax machine, and/or IP address. Messages must not be longer than 160 characters and contain no images of graphics.

SPAM – Unsolicited Electronic junk mail or junk newsgroup postings. There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python "SPAM" song.

TDMA - Time Division Multiple Access, a technology for delivering digital wireless service. TDMA works by dividing a radio frequency into time slots and then allocating slots to multiple calls.

Touchpoint – Channels through which users are being profiled. Websurfing, use of cell phones, contact with telemarketing firms etc., are all different touchpoints.

URL - Uniform Resource Locator, the global address of documents and other resources on the World Wide Web.

WAP - Wireless Application Protocol, a secure specification that allows users to access information instantly via handheld devices.

Web Bug – A graphic on a Web page or in an email message that is designed to monitor who is reading the web page or email message. A web bug is often invisible because they are typically only 1-by-1 pixel in size, with no color. Among the information collected is the IP address of the computer that the Web bug is sent to, the URL of the page the Web bug comes from, and the time it was viewed.

WML - Wireless Markup Language, and XML language used to specify content and user interface for WAP devices.

Introduction

"We noticed your interest in our special Oz vacation-deal, offered at our website last week. Today's temperature in Sydney is 25 degrees; in Stockholm it's 3. Wouldn't you rather be in Australia right now?" The message on my Palm Pilot™ startled me, how could the travel agency know that I was interested in going to Australia? It could of course be another SPAM-message sent out to a bunch of people who happened to be on the travel agency's mail-list. Then came the scary message; "You are now two blocks from our local office. If you book your trip today, we will give you 10 percent off the already low ticket-price."

The travel agency knew both my interest in a trip to Australia (I spent eleven minutes at their website last week, according to their notes), and they knew I was just about to walk by their office.

Of course, this didn't really happen (I don't own a Palm Pilot). But it could, and not in a distant future. The technology for *Personalized and Location-based Marketing* is already here. Soon we will see it in full use. Should we be scared about this? Have we reached the state of "Big Brother" that Orwell wrote about, fifty years ago?

As I'm writing this, I am looking down at Park Street Cemetery in downtown Boston, where among other great men of the American Revolution, James Otis is buried. He stressed the importance of privacy, and much thanks to him, the United States got its fourth amendment to the Constitution. 200 years later, in the advent of another revolution, this time involving wireless devices in networks instead of limeys in red coats, the thoughts of James Otis are maybe more important than ever before.

Privacy groups are formed all over the western world, trying to pursue lawmakers, content-providers, service providers, and other actors on the digital scene to actively protect the privacy of the modern citizens. On the other side there are people who say things like "You have zero privacy anyway, get over it!"[2]

Is there a way to enjoy the new technology without sacrificing ones personal integrity? Is it possible to combine personalization with personal privacy?

[2] Scott McNealy, CEO Sun Microsystems (as quoted in a *Wired News* article, January 26 1999)

So what exactly is *Personalization?*
According to the Personalization Consortium[3], personalization is the use of technology and customer information to tailor e-commerce (and m-commerce) interactions between a business and individual customers. Using information obtained about the customer, the exchange between the parties is altered to fit that customer's stated needs as well as needs perceived by the business.

The purpose of it is to:

- Better serve the customer by anticipating needs
- Make the interaction efficient and satisfying for both parties
- Build a relationship that encourages loyalty

While personalization is an often-confused marketing term and initiatives and definitions widely vary, the true benefits are often very simple and commonly defined. They include permission-based marketing, targeted messages, convenience for consumer shopping or information searches, and customizing offers to consumer-driven preferences.
In a wireless environment, effective personalization is crucial. Small screens, and small keyboards make it difficult to find information in an easy way. The fewer "clicks" before reaching the desired information, the better. With wireless also comes the fact that the user is mobile, personalization can thus also be made location specific.

So far, so good; but fact is that the collection and processing of personal data can be misused. Privacy is a concern, especially in the wireless environment. Users need to be able to disclose their privacy preferences in an easy manner; they must also be able to trust the companies that collect personal data.

Legislation, self-regulation, and technical measures are needed in order to protect the personal integrity of wireless users. When collecting personal data, the power must ultimately lie in the hands of the user. Disclosing privacy preferences in an effective way should be easy, but is it?

[3] www.personalization.org

1. The Mobile Internet

In this chapter I will describe the fundamentals of wireless data communications. Who are the actors on this scene? How is the Internet made available on wireless devices? What devices exist today? What services can wireless users expect to see in the future, and what will happen to their personal integrity?

The Mobile Internet is about offering the mobile consumer a whole new range of services that take advantage of four important cornerstones[4].

1. The mobility aspects of being able to access services and interact with others while on the move.
2. The ability to carry out small payment transactions via the mobile device.
3. Applications taking into account the geographical location of the user.
4. Services that are oriented towards the individual considering his or hers profile.

In short, Personalization and Location is the key to the "mobile Internet". It is not about making the Internet available on mobile devices. As will be described in this chapter, technology has not reached the point yet to where the Internet, as we experience it from a wired environment, can be made completely mobile. The low bandwidth and the small screens on today's devices are the two major roadblocks that lie in the way of a smooth mobile information highway. Personalization can solve many of the issues that the mobile world face; by showing the "right content" at the right time.

1.1 The Devices

Two different kinds of wireless devices are predominant on the market today; the cell phone[5] and the Personal Digital Assistant (PDA). One is primarily for voice communication and the other for text and images. Cell phones are clearly limited when it comes to text and image reception, and PDA's still don't work as phones.
So far, there are no good hybrids on the market[6]. To surf the web with a PDA you need to connect it to a cell phone; by cable, Infrared Data Communication or Bluetooth.

[4] These exact "cornerstones" are stated by Fadi Pharaon, Senior Vice President of Melody Interactive Solutions. www.melody.se/about/wireless.jsp?4 , similar statements can be found at www.nokia.com and www.ericsson.com

[5] Cell phones that can connect to the Internet are sometimes called "smart phones". Both terms will be used in the essay.

[6] The hybrids are getting better and better. As I see it, Nokia is leading the race at the moment with the new Nokia Communicator.

Cell phones are, due to their small screens and the low bandwidth of today's wireless networks, not a good device for receiving information (except short messages, and some WAP services.) The problem with the low bandwidth is about to be solved. The third generation of mobile communications technology, 3G, is about to be launched in Europe and the U.S. It is already in use in Japan[7].

1.2 WAP – GPRS - 3G

WAP is an application designed to enable mobile access to the Internet and advanced telephony services. Services include weather forecasts, stock quotes, and some other rather "basic" information services. WAP over GSM has a data rate of 9.6 Kbps.
WAP technology links wireless devices to the Internet utilizing a WAP gateway and a special language (WML/HDML) to translate a mobile web request into a traditional (HTML/HTTP) request that the Internet server can understand and vice versa when the mobile user receives the requested information[8]. The low bandwidth of today's wireless networks makes it impossible to enjoy more advanced information services.

GPRS (general packet radio service) is an upgrade to GSM mobile networks that adds a packet-switched layer and is expected to deliver data rates up to 384 Kbps[9]. More importantly, it will allow operators to charge by volume of data transferred instead of time connected. These means that users could be permanently connected to the Internet, but only be charged for accessing email or newly requested web pages.

3G is an ITU[10] specification for the third generation (analog cellular was the first generation, digital the second) of mobile communications technology. 3G promises increased bandwidth, up to 384 Kbps when a device is stationery or moving at pedestrian speed, 128 Kbps in a car, and 2 Mbps in fixed applications.
The hype surrounding this new technology is massive. One of the leading vendors on the wireless market, Nokia, believes that next year (2002), Europeans will get speeds up to

[7] The 3G net in Japan is carried out by NTT DoCoMo, www.nttdocomo.com/top.shtml
[8] Ericsson, www.ericsson.com/wapsolutions
[9] to reach 384Kbps, EDGE-technology needs to be implemented (see definitions). www.ericsson.com/3G
[10] Short for *International Telecommunication Union*, an intergovernmental organization through which public and private organizations develop telecommunications. The ITU was founded in 1865 and became a United Nations agency in 1947. It is responsible for adopting international treaties, regulations and standards governing telecommunications.

2Mbps on mobile devices and connect anywhere at anytime[11]. Maybe that time span is a bit too optimistic. Forrester Research[12] believes that it will take until 2007 before Europeans can enjoy the full advantages of 3G.[13] Both Nokia and Forrester agree that GPRS will play an important roll in mobile communications in the next few years.

1.3 Network carriers and gateways

Surfing the web from a mobile device requires that the content requested is transformed into a format that suits the device. Instead of using the usual HTML language, the content pages uses another language, one of the most common is WML.
The transformation takes place in a gateway between the cellular network and the Internet. It takes WML-formatted information from the content server and translates it into the compressed format that the mobile device understands.

There are a variety of gateways that stand in between the user and the service at the other end of the network. In many cases, those gateways are for purely technical purposes. In some cases, those gateways exist to manage or in some cases alter the business relationship or other kinds of relationships that the user has with the service provider on the other end[14].
As will be shown in the next chapter, the gateway plays an important part in the personalization process.

1.4 Device Customization

In the wired world, systems assume that users are at their desk in the office or at home. That is, the user's information stays constant, as does the access point. In the wireless world, however, users are mobile and the devices they use for accessing the information have limitations as to screen size and transaction speed. Showing the right information based on location, time of day, and bandwidth is critical.

Information needs to be customized to the device from which the user access the net. In the "traditional" world of the Internet, businesses have assumed that the user has a personal

[11] www.nokia.com/3G/whatis_faq.html
[12] Forrester Research is an independent research firm, with its headquarters in Cambridge, Massachusetts.
[13] Americans will have to wait even longer, see www.forrester.com/ER/Press/Release/0,1769,263,00.html
[14] Donald Bromley at the Wireless Web Workshop, p12 of second proceeding.

computer. Now, the mobile world has leveled that assumption. Users might have one of the many varieties of cell phones, a PDA, or some form of hybrid.
Thus, the page layout, the site navigation, and the page content will change, in some cases dramatically, based on the user's device. What the user will see can be determined by the connecting devices' bandwidth and display.
This leads to a problem when it comes to displaying privacy policies on the device. Should only the users with the fastest connections and large screens be able to view the providers privacy notice? I will discuss this in my conclusion.

1.5 Mobile Services

The introduction of the smart phone has brought about exciting possibilities for consumers and businesses. With the ability to check e-mail, get stock quotes, access the Web, pay bills, and purchase goods and services anywhere anytime, consumer demand for smart phones is likely to rise steadily. Forrester Research predicts 177 million U.S. consumers will subscribe to some form of mobile service in 2005, and 111 million will access the mobile Internet at least once per month[15].

1.5.1 An example of mobile services that may be available in the near future

You find a parking space on the street outside your favorite store, and then you realize that you don't have the right change. Not a problem, you take out your cell phone, dial a number, point it at the meter and enter the amount and the time that you want to keep this space, and the cost is automatically deducted from some account you have elsewhere. After a full day of shopping, you decide to grab a cup of coffee. As you walk by Espresso House, a beep from your cell phone indicates that you have received a coupon entitling you to a ten percent discount on the first Latte. With a buddy list on your cell phone, friends and family within a five-block radius can be alerted to your location in case they want to stop by and chat.

1.5.2 Services based on user location

Location information has been processed in mobile communications networks from the very beginning. As long as this information was only generated and used for establishing a connection to the mobile device, location information resided only with the operators of telecommunications networks, which are in most countries bound very strictly by

[15] Forrester, *Mobile Internet Realities.*

telecommunications secrecy[16]. The precision of the location depended on the size of the respective cells in the cellular networks[17].

Partly driven by legal obligations to make more precise information about the location of a mobile device available for emergency services[18], network operators have started to modify the technical infrastructure of their networks to conform to these obligations. This means that much more precise information about the location of any mobile device will be available in the near future. Equipment manufacturers claim that even today a precision of up to 5 meters is technically possible when using GPS-assisted systems[19]. The problem with location-based services is that these services will most likely not only be provided by telecom operators, but by third parties that are not legally bound by the restrictions of telecommunications secrecy[20].

Wireless tracking technology[21] would allow a gateway to know the exact location of a cell phone user. This information could then be used to deliver location-based, highly personalized information such as the previously cited coffee coupon, directions for traveling, or location of the nearest store. The Swedish Telecom giant Telia, already supplies their customers with "location based yellow pages"[22], by knowing the users location a more relevant excerpt of the yellow pages can be supplied. On the other side of the Atlantic, General Motors is using tracking technology to give customers directions while traveling through their OnStar system[23]. The system includes the potentially life-saving feature of the ability to dispatch emergency units to a driver's location in case of an accident. When cell phone users call for emergency services without knowing their location, tracking technologies could help send appropriate life saving services. Although this is different from sending targeted advertisements, it demonstrates the considerable opportunity to deliver convenience and personalization to consumers through wireless tracking.

[16] In the U.S. The Wireless Communications and Public Safety Act of 1999, in the E.U. The Telecommunications directive 97/66.
[17] Working Party, Location Practices, p.2.
[18] The FCC has issued an "enhanced 911 program" see the subchapter on U.S. Legislation.
[19] www.vindigo.com
[20] Working Party on Data protection, *Privacy and location information in mobile communications services.*
[21] see next chapter.
[22] the service is called "nära dig", www.teliamobile.com
[23] www.onstar.com

1.6 Personal Integrity

Whether tracking is used to save a life or ten percent on the next cup of coffee, the potential to deliver convenience to the end user is impressive. Despite its benefits, the down side of utilizing wireless tracking technology and highly personalized applications are their intrusive nature. Tracking technology has the potential for "Big Brother," to monitor an individual's every move. The use of tracking technology, however convenient, may be seen as an invasion of privacy and a hindrance to an individual's ability to move freely. Combined with a highly detailed user profile, it is easy to see similarities to Orwells "1984".

When used to send personalized location-based information like coupons or alerts about nearby establishments, this "Big Brother"-feeling will be clearly noticeable for the smart phone users. Much like the annoyance of SPAM emails filling inboxes, users of smart phones could become virtually drowned with unwanted alerts and advertisements as they walk down the street. Although SPAM emails are annoying, they are not personalized. The user usually throws them in the trashcan as they would do with traditional advertisements received with "snailmail". "Personalized SPAM" will be more annoying, suddenly the marketers not only know the users name, but also his or hers location and interests.

A report from Jupiter Communications predicts the average web user can anticipate encountering more than 950 messages per day in 2005, including e-mail and banner advertisements, nearly double the amount today[24]. When encountering such a large volume of messages, cell phone users, who currently pay for airtime minutes while accessing the wireless web, may be reluctant to receive and view wireless advertisements despite their convenience as they will pay to receive advertisements that has the potential of clogging email inboxes.

Disclosing user privacy preferences will be of uttermost importance in such a business climate. Should the user "opt-in" as soon he or she is interested in receiving ads on the cell phone? If so, personalization will be necessary. Personally I would, for example, like to receive coupons from Espresso House, but not from the textile store next door.

[24] Jupiter, Marketing Report.

2. User Profiling

The general idea when collecting personal data is; the more data collected, the better and more personalized service can be provided. Collecting data from different touchpoints gives a broader view of the users habits and preferences. The data is analyzed and can be combined with demographic data from third-party sources, data on the users offline purchases[25], or collected directly from users through surveys and registration forms. User information includes the user's stated profile. This profile might not only contain information such as name, address, and phone number, but also transactional information on purchases from last week or last year, which, like the profile information, can come from multiple back-end systems[26].

From a personal integrity point of view, this is the main problem area; bringing information together can eventually construe a map of the users life. That is why "harmless" user surveys on websites, in stores, in direct mail campaigns etc., play a much more important roll than users usually think when it comes to "mapping" a users habits.

Constructing a "map" of a users habits and preferences is usually called profiling. Marketers are making a profile of the user. Although this essay focuses on the disclosure of privacy preferences in the wireless world, it is important to briefly describe profiling practices in the wired world as well. The companies that collect personal information are usually active in both the wired and unwired world. Personal profiles can thus be derived from user activities on both the wired and wireless web.

2.1 Online Profiling

Online profiling is a complex concept that is subject to different definitions. It may mean the collection of anonymous transactional data that is used to create targeted advertisements; it may also mean the merger of *clickstream data*[27] with personally identifiable information[28]. Internet technology enables marketers to collect personal information without first informing the user. *Cookies* and *Web bugs* invisibly record online behavior, enabling Internet marketers to create a profile of a given consumer. This process has created much objection among privacy advocates[29], who fear that such activities are too intrusive, particularly because the consumer is largely unaware of the information-gathering activity

[25] Use of credit cards, retail store member cards, responding to direct-mail surveys etc. all leave traces.
[26] Forrester, *Customer Context Servers,* p.8
[27] See Definitions and Abbreviations.
[28] FTC, workshop on Online Profiling, testimony by *Center for Democracy & Technology.*
[29] see for example www.epic.org and www.cdt.org

Network Advertising Companies - Banner Advertisements

Banner Ads are usually not selected and delivered by the Web site visited by a user, but by a network advertising company that manages and provides advertising for numerous unrelated websites. In general, these Network advertising companies do not merely supply banner ads; they also gather data about the user who view their ads[30]. This is accomplished by the use of *cookies* and *web bugs* which track the individual's action on the Web.

Among the types of information that can be collected by network advertisers are; information on the Web sites and pages within those sites visited by users, the time and duration of the visits, query terms entered into search engines, purchases, "click through" responses[31] to advertisements, and the referring page[32].

The information gathered by network advertisers is often, but not always, anonymous. The profiles are linked to the identification number of the advertising network's cookie on the users computer rather than the name of a specific person. This data is generally referred to as non-personally identifiable information. In some circumstances, the profiles are linked or merged with personally identifiable information. This information can include name, address, phone number, e-mail address and social security number, and is made possible in one of two ways[33]:

- The user has identified him or herself at the website where the banner ad is located. This can be done by entering any personal identifiable information on the website, such as name or e-mail address. The website then provide that information to the network advertiser.
- Depending on how the personal information is retrieved and processed by the website, the personally identifying information may be incorporated into a URL string[34] that is automatically transmitted to the network advertiser through its cookie.

The profiles created by the advertising networks can be extremely detailed. A cookie placed by a network advertising company can track a consumer on any website served by that company, thereby allowing data collection across unrelated sites on the web. And since cookies are generally persistent, the tracking occurs over an extended period of time, resuming each time the individual logs on to the Internet.

[30] www.tinhat.com/internet_privacy/company_data_collection.html
[31] When a user requests additional information about a product or service by clicking on a banner ad, he or she has "clicked through" the advertisement.
[32] www.privacyalliance.org/resources
[33] FTC, online profiling workshop, transcript p.3.
[34] See Definitions and Abbreviations.

2.2 Wireless Profiling

Although the mobile Internet and the wired Internet basically is the same net, there are as previously described, some differences. "Normal" websites need to be transcoded[35] into another language in order to work on wireless devices. As for the wireless profiling, this makes a difference. Most wireless languages don't support cookies or webbugs. The user can thus not be identified as a repeat customer to websites he or she has been visiting before. The users identity is revealed only to the network carrier, and that information should be safe there. However, there are some exceptions. There is no difference from wired web surfing if the user logs on to a portal or gateway, with his or hers individually assigned ID-number. Nor can the users identity remain totally anonymous if the gateway (in agreement with the network carrier) "forces" the use of the same IP number every time the user goes online[36].

As the 3G nets are deployed, each wireless device will require their own IP address. The new IP-standard, IPv6, will eventually become the standard protocol on the wired web. The current IP version (IPv4), has its limitations as to the number of available IP-addresses. With the launch of the mobile internet, and as more and more users worldwide get online, the number of IP addresses will run out. There is a need for more addresses; with its 128-bit address space, IPv6 will meet this need. By enabling an end-to-end connection, IPv6 will make it possible to keep a channel open with subscribers, and tailor services to their location, interest and lifestyle.[37] The user will thus not be anonymous to the provider.

2.2.1 Gateways

Gateways receive, translate and forward all requests telling who requests what, using what device and thus can easily create extensive personal user profiles.

Web or WAP server sites often ask for user- and user-side specific data to offer customized services or for market analysis purposes. Input parameters to a mobile context aware service can be the user identity, user location, device type and capabilities, user settings in the device, the user's previous behavior[38]. A new framework for this user identity identification is currently under construction (see below).

---

[35] The term "transcode" is used by IBM to describe the transformation of Internet information into a readable language for a wireless device.
[36] www.yale.edu/pclt/comm/tcpip.htm
[37] www.hi3g.com
[38] WAP-W3C workshop, Statement of the *Computer Security Research Group* at Karlstad University, Sweden.

2.2.2 Composite Capability / Preference Profiles (CC/PP)

A number of wireless companies[39] are currently involved in a working group that is developing a new framework for describing and managing software and hardware profiles. A CC/PP is a description of device capabilities and user preferences that can be used to guide the adaption of content presented to that device. Particularly in wireless networks CC/PP is intended to provide information necessary to adapt the content and the content delivery mechanisms to best fit the capabilities and preferences of the users and their agents. However, the capabilities and preference information (CPI) contains detailed characteristics about the user's device, software, network and personal settings, which can be unique for a specific user with a specific device. Thus, the CPI can serve as a unique identifier and can, like a user-id, be used to trace a user's request activities at the origin server's site. CPI in combination with the user-id can tell what device, software or network a user is using[40]. Such information can be misused for launching attacks against the user, if it gets into the wrong hands.

2.2.3 User Location / Wireless Tracking

For location-based services to work, the users location must pinpointed by the company supplying the service. I've mentioned some of the services available in the previous chapter, and will now briefly describe the technique behind wireless tracking. A user's location can be retrieved in two ways; through the network and/or using Global Positioning System (GPS)[41].

2.2.3.1 Network

Networks can use the cell ID assigned to each active cell phone to obtain very rough estimates of users' locations. All cell phones must know their cell identity if they are switched on and have radio coverage. It is also possible to find out roughly how far a mobile is from the current base station. Companies like Canada-based Cell-Loc are taking methods of triangulation[42] used to locate skiers lost in snow slides and adapting them to analog and digital wireless networks in the U.S. and Europe.

---

[39] For example Nokia, Ericsson, and IBM. Full list of participating companies at www.ccpp.org

[40] World Wide Web consortium, www.w3.org

[41] world wide web consortium, workshop on position dependent information services, phone.com position paper, www.w3.org/mobile/posdep/pdcpositionloc.html

[42] A call to a wireless device is picked up by a number of cellular towers. Based on the signal's strength, the system approximates the handset's location. The technology's accuracy varies because it is approximating the location from antennas that cover the entire cell site.

The major advantage of using network-based location technology is that the system works with all cell phones, the problem is that network operators may not be able to process all location information once location-based advertising really takes off.

2.2.3.2Global Positioning System (GPS)

The second location technology puts the power in individual handsets using GPS.
The GPS uses satellites and requires direct line of sight to at least three satellites in order to determine a position[43]. This answers many privacy concerns by allowing users to manually disable the ability to locate them. However, the chip needed for this would have to fight for scarce space on handsets that are already crowded with voice-recognition and Internet access functions.

2.3 Personalization techniques

Companies that collect personal data sometimes collect more data than they need. This leads to a "Stasi[44] problem", as put by the Marketing Manager at Adaptlogic[45]. The real trick when it comes to effective personalization is to do something constructive with the personal data collection. there are a few techniques that are widely used among companies in the personalization business. The most common, according to the Personalization Consortium[46] are;

- **Collaborative Filtering.**
  Bases recommendations on the similar behavior patterns of other visitors. For example, visitors provide information about their preferences and then based on similar profiles in the system, collaborative filtering helps determine items that closely match their taste. This technique is for example used at Amazon.com, "we noticed that you bought the XY book, other readers of the XY book also bought the XYZ book"

- **Rule Based Filtering**

  Generates a profile of each customer, which is stored in a database and used to identify patterns of behavior. The patterns are transformed into assumptions, or logic rules in the form of "if-then" or "when-do" statements.

[43] www.gpsworld.com(glossary)
[44] The East German Intelligence and Security Service; notorious for collecting massive amounts of information on the citizens of East Germany.
[45] www.adaptlogic.com. Interview with Mattias Malmnäs, August 2001.
[46] www.personalization.org

For example, you may have a rule that reads if customer age > 25 & customer age < 35 & customer income > $40,000 then show Jeep Wrangler, else show Toyota Corolla.

- **Self-learning artificial intelligence applications**.

The user is profiled as the application is used. After frequent usage, the application ”learns” the user habits, and automatically delivers a personalized content. (see below)

Anonymous Personalization

Anonymous personalization would be the simple answer to this essays title. Is it possible to keep ones privacy and still enjoy the advantages of personalization? In some cases, the answer is yes. Profiling a user, and delivering personalized content to him or her, doesn't always need to involve using personally identifiable information. An example of anonymous personalization is a product developed by Adaptlogic. Their software uses the above mentioned self-learning artificial intelligence technique. Without going into too much technical mumbo jumbo, the program works like this[47];

1. The user requests a web page from a content provider.
2. The request goes through the self-learning server (stationed at a different location than the content provider server) on the way back to the user.
3. The server identifies the user with a user number, provided by the content provider.
4. The users “file” contains his/hers “web page behavior” data, the data is changed based on the new request (the server logically adapts to the request)
5. The users request is altered based on his/hers profile, and then delivered to the user.

This approach guarantees the users privacy. The content provider knows the user identity, but has no control over the self-learning server. The self-learning server has no idea who is behind the user ID-number. Thus, even though identification is made, no personal data can be derived from the users behavior on the website.

[47] interview with Mattias Malmnäs.

3. Legislation

In this chapter I will briefly describe and compare the existing privacy legislation and policies in Europe and the U.S. The focus will lie on the European Directive on Data Protection and the Fair Information Practices issued by the Federal Trade Commission. The Safe Harbor Agreement will be presented and commented in the end of this chapter.

The E.U and U.S. at this point in time have different approaches to privacy and data protection. Under the E.U Directive (see below), privacy is a matter of legal right; there are legal limits as to the extent to which personal data can be collected and used, and there is a system of enforcement by public authorities, over and above any redress consumers might be able to pursue under their own initiative.
In the U.S., privacy and data protection are seen as matters of industry self-regulation. Ultimately, companies can do what they like with personal data provided they can be said to have the consumers' consent. The real danger here is that consent clauses can be cleverly drafted to give companies almost a free hand to process data as they wish. This is, however, not happening on a regular basis; as companies that conducts "unethical" data processing can seriously damage their reputation.

3.1 European Legislation, the comprehensive approach

This European principle of self-determination puts the citizen in control of the collection and use of personal information. The approach imposes responsibilities on data processors in connection with the acquisition, storage, use and disclosure of personal information and, at the same time, accords citizens the right to consent to the processing of their personal information and the right to access stored personal data and have errors corrected.

For global information networks and electronic commerce, the comprehensive approach invokes some tension[48]. Without the statutory authority to restrict transborder data flows, the balance of citizens' rights in Europe could easily be compromised by the circumvention of Europe for processing activities[49]. Therefore the Directive includes two provisions to assure that personal information of European origin will be treated with European standards.

[48] Reidenberg, p.3.
[49] Servers where the processing takes place could for example be placed outside the E.U.

A choice of law clause in the Directive[50] assures that the standards of the local state applies to activities within its jurisdiction and a transborder data flow provision prohibits the transfer of personal information to countries that do not have "adequate" privacy protection[51].
Data protection in the U.S. still doesn't comply with the provisions of the Directive, and is thus not regarded as having an adequate privacy protection. For this reason, the Safe Harbor Agreement was drafted. The provisions of this agreement will be discussed after the subchapter on U.S. legislation.

3.1.1 The Directive on Data Protection

Europe has, for some years, had a patchwork of privacy legislation that has differed from country to country. The European Directive on Data Protection[52], hereinafter *the Directive,* has now been adopted within the European Union as a minimum standard for privacy legislation in each member state. As the Directive is passed into law in the member states[53], there will be some convergence of regulation although each country is still at liberty to maintain standards that are more restrictive than those of the Directive. The Directive employs general standards, such as "fundamental fairness", rather than bright line rules in determining compliance. The aim of the Directive is to afford any person whose personal information is transmitted an equivalent level of protection irrespective of the member state transmitting or processing the data.[54]
The Directive has been adopted to protect people against their personal integrity being violated by the processing of personal data. Processing of data includes collection, recording, storage, adaption or alteration, compilation and retrieval. The act also applies to personal data that is transmitted, disseminated or made available by other means. There is no requirement that data, which is processed by a computer, should be structured in a register or the like[55].

Personally Identifiable Information

According to the Directive Article 2, personal data mean any information relating to an identified or identifiable natural person (the data subject). The person is identifiable if he or she can be identified, directly or indirectly, in particular by reference to an identification

[50] Directive, art 4.
[51] Directive, art 25.
[52] *Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*
[53] As of July 1st 2001, all member states except Germany, France and the Netherlands have implemented the directive into their national legislation.
[54] Rustad & Daftary, p.390.
[55] Directive, art 2 (b).

number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the data subject[56]. Thus, encrypted information, and information stored in "back-end" systems is regarded as personally identifiable information if this information can be read and understood by a human being, if he or she is, or likely will be, in possession of the means to un-encrypt the information[57]. Compare *Anonymous personalization* in the previous chapter.

Consent from the Data subject

Personal data may only be processed if the person who is registered has given his or hers consent to this. The Directive sets up some exceptions to the consent provision. Personal data may be processed without consent when prescribed by statute. In some cases it may also be allowed if the processing is necessary in order that one may, for example, be able to make a contract with the data subject or if it is necessary in order to comply with a legal obligation or to protect a substantial interest of the data subject. Personal data may also be processed if necessary in order to perform a task connected to the exercise of official authority.
Furthermore, in some special connections, the reasons for personal data being processed may outweigh the needs of the data subject to be protected against the violation of personal integrity[58].
A data subject may revoke his or hers consent. In that event, further personal data may not be processed. Very stringent rules apply to the processing of particularly sensitive personal data. Such sensitive personal data includes, for example, information about health, political opinion and religion[59].

A company that collect personal data need consent from their users. It is thus not enough to state a privacy policy at the web page, or wireless device from where the information is gathered. The user must actively consent to the information gathering. A consent-clause need to state the purpose of the information gathering, what information will be collected and what this information will be used for. The legality of a "click through" consent will be discussed in the next chapter.

[56] Directive, the ingress.
[57] Lindberg/Westman s.113.
[58] Directive, art 7.
[59] Directive, art 8.

Transfer of Personal Data outside the E.U.

The processing of personal data through the Internet (likewise the Mobile Internet) means that the data may be accessible to anybody in the world, even in countries that do not have adequate protection for the integrity for individuals or which perhaps do not have any rules in the area whatsoever.

The rules of the Directive concerning protective rules on the transfer of personal data have an important role to play. The rules mean, in principle, that consent is required from the registered person in order that personal data may be processed over the Internet. This applies irrespective of how the processing takes place. For example, it may relate to web sites, electronic mail, electronic distribution lists or items in news groups.[60]

In principle, it is forbidden to transfer personal data that is being processed to a third country (a country outside the E.U and EEA). However it is allowed, despite the prohibition, to transfer personal data to a third country if the registered person has given his or hers consent to the transfer or when the transfer is necessary in order that;

- a contract between the registered person and the controller may be performed or measures that the registered person requested may be taken before a contract is made
- a contract between the controller and a third party that is in the interests of the registered person may be made or performed
- legal claims should be established, exercised or defended
- vital interests of the registered person may be protected.

3.1.2 Implementation divergences among the member states

The harmonization achieved by the Directive is significant, but does not remove all divergences in the European national laws. The Directive creates a strong baseline of protection across Europe, but small divergences exist where the principles are interpreted by different supervisory agencies in each of the Member States. These remaining divergences in standards can pose significant obstacles for the complex information processing arrangements that will be typical in m-commerce[61]. For exampel, the definition of “identifiable person” is not the same in all member states national legislation, what some consider “identifiable”,

[60] Datainspektionen, Information on the Personal Data Act.

[61] Reidenberg, p.3.

others do not[62]. In order to reach consensus on critical interpretive questions, the Directive creates a "working party" of the Member States national supervisory authorities.[63]

3.1.3 Location information in mobile services

A common position reached by the working party, relevant to this essay, is the guidelines regarding *privacy and location information in mobile communications services*, adopted in February this year. The working party set up nine principles that actors on the m-commerce arena should follow[64].

1. The design and selection of technical devices to be used for such services must be oriented to the goal of collecting, processing and using either no personal data at all or as few data as possible.
2. Precise location information should not be generated in the first place as a standard feature of the service, but only "on demand" when it is needed to provide a certain service linked to the location of the users device.
3. The user must remain in full control on whether precise location information is generated in the network. In this respect, handset-based solutions where the creation of precise location information is initiated by the mobile device seem to offer a better degree of privacy than network-based solutions where location information is generated as a standard feature and choice of the user over this information is limited to the question whether it will be communicated to third parties.
4. Users should be able to disable the precise location determination at any time without disconnecting their device from the network. Users should also be able to disclose their location information at a chosen level of precision (e.g. building, street, city or state level).
5. Location information should only be made available to providers of value added services where the user has given his informed consent. Consent may be restricted to a single transaction or certain providers of value added services. The user must be able to access, correct and delete his or her preference data also in cases where the preferences of the user are not stored on the mobile device, but within the network.

[62] The Swedish Data Protection Act (Personuppgiftslagen 1998:204) has for example a broader definition of "personal identifiable data" than the U.K.(Data Protection Act of 1998).
[63] Directive, art 29.
[64] The working party has, according to art 29 of the Directive, advisory status. Thus, these guidelines are not enforceable rules.

6. The creation of movement profiles by telecommunications service providers and providers of value added services should be strictly forbidden by law unless where necessary for the provision of a certain service and based on the user's informed, unambiguous consent.
7. Location data is a highly sensitive category of information. Access, use and disclosure of such information should be subject to the same or similar controls as for content data protected by telecommunications secrecy.
8. Wherever possible, mobile network operators should not communicate location data together with personally identifiable information about the user to providers of value added services. Instead, pseudonymous information should be used. Personally identifiable information (e.g. the ID of the mobile device) should only be made available to providers of value added services with the user's informed consent. Any location data should be deleted when no longer necessary for the provision of the service.
9. A provider must not make the rendering of a service or the terms of the service conditional upon the consent of the user to the effect that his or her personal location data may be processed where such data are not necessary for the provision of the service.

3.1.4 The Telecommunications Directive, and the "draft Directive"

The guidelines above can in some parts be derived from the Telecommunications Directive[65]. This directive, which imposes wide-ranging obligations on carriers and service providers to ensure the privacy of users' communications, is being updated to cover the new technology advances in the telecommunications sector. Telecommunication companies are, according to the directive, not allowed to give away information to third-party advertisement companies. They may, however, use the information to advertise their own services.
With the new telecommunications directive[66] (hereinafter *the draft Directive)* it will be possible for telecommunication companies to sell information about their customers, provided that consent is given from the customer. This would give network carriers a good return on investment, considering the amount of money spent on building the new 3G-networks. Other key provisions in the draft directive are the use of *traffic data* and the protection against *unsolicited communications.*

[65] Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector.
[66] Commission Proposal, COM (2000) 385 final. *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.*

Traffic data refers to any data processed in the course of or for the purpose of the transmission of a communication over an electronic network. Such data will be used by service providers to provide certain services. It is clear that such data should only be used if made anonymous, or with the consent of the subscriber. Moreover, it is proposed under the draft Directive that subscribers should be fully informed about the type of data which is being processed and the purposes for which this is being done. Accordingly, a positive duty to inform the subscriber of the personal data that is being collected is proposed.

The draft article 13 proposes the granting of a right to all subscribers to refuse unsolicited communications for direct marketing purposes in respect of *all forms of electronic communications* (and not merely to voice telephony calls as under the telecommunications directive). This will include e-mail or other new forms of communications.

3.2 U.S. Legislation, the sectoral approach

While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a very different approach to privacy than that taken by the European Community. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation.

The U.S. Constitution does not explicitly use the word "privacy", several of its provisions protect different aspects of this fundamental right. The strongest protections arise from the Fourth Amendment[67], which safeguards individuals in their persons, homes, papers, and effects, from unreasonable searches and seizures. The constitutional right to privacy protects against intrusions by the government, however, not by private corporations[68].

The regulatory and legal framework governing online privacy practices is rapidly evolving[69]. In the U.S., the Federal Trade Commission (FTC) functions as the chief federal regulator and enforcement authority of online privacy issues. The FTC derives its enforcement authority from the Federal Trade Commission Act[70].

[67] Privacy protection from the constitution can also be found in the first, fifth, ninth and fourteenth amendments.
[68] Rustad & Daftary, p 387.
[69] www.privacyheadquarters.com/legwatch/state.html , legislative watch, listing all new privacy bills in Congress.
[70] 15 U.S.C. §§44, 45.

3.2.1 Fair Information Practices

In 1977, at the beginning of the computer revolution, the federal government developed a set of Principles of Fair Information Practices that have been agreed upon by governments, privacy experts and industry groups. The Principles are intended to foster individuals' control over their personal information, limit data collection, and place responsibilities on data collectors. These Principles are the basis for current data protection and online privacy views, laws and policies[71].

Central to the aim of Fair Information Practices are the goals of transparency and fairness. Transparency means that when organizations collect information about individuals they should make known to the individual the information that is collected and how it is used. Fairness means that information is used only for the purpose for which it is collected. If the organization wishes to use personal information for additional purposes, it is obligated to obtain the explicit permission of the individual involved.

The core principles of the Fair Informaition Practices are[72]:

Notice

The most fundamental principle is notice. Users should be given notice of a company's information practices before any personal information is collected from them. Without notice, a user cannot make an informed decision as to whether and to what extent to disclose personal information. Notice should be given the user in three forms of identifications;

- identification of the company collecting the data
- identification of the uses to which the data will be put
- identification of any potential recipients of the data

In the Wired context, notice can be accomplished easily by the posting of an information practice disclosure describing a company's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the user. It should also be unavoidable and understandable so that it gives users meaningful and effective notice of what will happen to the personal information they are asked to reveal.

[71] www.ftc.gov

[72] As set up by the FTC in their report to Congress entitled "Privacy Online: Fair Information Practices in the Electronic Marketplace", May 25 2000.

In the wireless context, this is difficult to achieve. The special problems concerning well informed notice will be discussed in the next chapter.

Choice

The second widely-accepted core principle of fair information practice is user choice or consent. At its simplest, choice means giving users options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information (uses beyond those necessary to complete the transaction).
Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.
Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in require affirmative steps by the user to allow the collection and/or use of information; opt-out require affirmative steps to prevent the collection and/or use of such information[73].

Choice can also involve more than a yes/no option. Companies can, and do, allow users to tailor the nature of the information they reveal and the uses to which it will be put. Thus, for example, users can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily accessible way for users to exercise their choice. As with notice, this can also be somewhat difficult to do in a wireless context.

Access

Access is the third core principle. It refers to an individual's ability both to access data about him or herself. To be meaningful, access must cover timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or user objections can be added to the data file and sent to all data recipients.

[73] This is the main difference between Europe and the U.S. The E.U. directive clearly sets up a opt-in regime, whereas the U.S. gives the choice of opt-in / opt-out to the company collecting personal data.

Security

The fourth widely accepted principle is that data be accurate and secure. Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Although security is a significant issue in both wired and wireless environment, I will not go into data security in this essay since it falls outside the delimitation of the thesis topic.

Enforcement

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. If there is no way of enforcing the fair information practices, they will become suggestive rather than prescriptive.
The alternatives for enforcement are industry self-regulation and/or government enforcement through civil and criminal sanctions.

Self-Regulation

A self-regulatory system should provide the means to investigate complaints from individual users and ensure that they are aware of how to access such a system.
If the self-regulatory code has been breached, users should have a remedy for the violation. Such a remedy can include correction of any misinformation and compensation for any harm suffered by the user. Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.
Debate over the capacity of self-regulation and market forces to adequately address privacy concerns is common in the privacy and consumer protection arenas. Advocates often take the position that self-regulation is inadequate due to both a lack of enforcement and the absence of legal redress to harmed individuals. Industry tends to strongly favor self-regulation, stating that it results in workable, market-based solutions while placing minimal burdens on affected companies[74].
Numerous efforts at self-regulation have emerged[75]; one of the most successful is TRUSTe[76], who award a seal to Websites that adhere to established privacy principles and agree to comply with TRUSTe's oversight and consumer resolution process.[77]

[74] Wired News article, June 5, 2001. www.wired.com/news/ebiz/0,1272,44309,00.html
[75] For example the Better Business Bureau's Online Privacy Program (BBBOnLine), and the Online Privacy Alliance.

Government Enforcement

Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers. Whether enforcement is civil or criminal will likely depend on the nature of the data at issue and the violation committed. Corporations that breach the fair information practices code may face liability for the common law tort of invasion of privacy. A company that sells consumers' personal data to another company is subject to the Federal Trade Commission enforcement actions, tort lawsuits, and unwanted publicity.[78]

3.2.2 Location information in mobile services

Sectoral legislation relevant to this essay is for example the Location Privacy Protection Act. This Act has not yet been passed by the house (as of July 15th 2001) If passed it will require companies that provide wireless location-based services to notify users when they collect information about their location. The bill also prohibits the use or sale of the information without permission of the user. Under the provisions of the bill, users must be told what information was collected, and be provided with a way to correct errors.

This bill would not, according to Senator John Edwards who introduced the bill to the Senate, hamper collection of location information for public safety[79].

According to regulations passed last year by the Federal Communications Commission (FCC), wireless carriers have until October 1st 2001 to begin selling new cell phones that provide 911 operators a wireless caller's phone number and nearest cell site. According to the new rule, all phones sold after December 31st, 2002, must be equipped with 911-location technology. Under the FCC's "Enhanced 911" plan, wireless devices will begin transmitting the precise location of a caller, accurate to within a few feet[80].

3.2.3 CTIA's Fair Location Information Practices

The Cellular Telecommunications Industry Association (CTIA) has established a set of guidelines regarding Location Information Practices[81]. These guidelines have been presented to the FCC, and could eventually be turned into formal rules. CTIA sets up four guidelines; Notice, Consent, Security/Integrity, and Technology neutral principles. The guidelines are

---

[76] www.truste.org

[77] www.truste.org/about/truste/about_faqs.html

[78] Rustad & Daftary, p. 387c.

[79] article on www.allnetdevices.com, July 13, 2001.

[80] www.fcc.gov/e911

[81] CTIA's petition before the FCC can be found at www.wow-com.com/pdf/ctia112200.pdf

more or less a copy of the above stated Fair Information Practices, but there are some exceptions. Consent should be given prior to any data collection activity. If the guidelines would become formal rules[82], U.S. companies would have no choice whether they should use an opt-in or opt-out approach to their data collection practices. Privacy Advocates, for example David Sobel general counsel for EPIC[83], thinks it's a "good start", whereas industry leaders believe it is to early to adopt an opt-in regulation; Jerry Cerasale from the Direct Marketing Association thinks that it's still very early where the applications are, and therefore regulations might kill some applications they may want[84].

3.2.4 The E.U. directive and its implications for the U.S.

The E.U. directive facilitates a single information market place within Europe through a harmonized set of rules, but also provide the U.S. with some implications. In this context, the lack of legal protection for privacy in the United States threatens the flow of personal information from Europe to the United States. At the same time, the Directive is having an important influence on privacy protection around the world[85].

With the high level of legal protection, Europeans do not face the same privacy obstacles for m-commerce that currently threaten the American experience. The culture of legal protection in Europe provides European companies with a competitive privacy advantage doing business in Europe over the many American companies that are unaccustomed to applying such stringent fair information practices to personal information.

3.3 Safe Harbor Agreement

The Safe Harbor data-privacy agreement, negotiated between the United States and the European Commission, took effect on November 1, 2000. It is the result of collaborative efforts between the U.S. Department of Commerce and the European Commission to govern the flow of data between the United States and the European Union.
The agreement creates a procedure to certify those companies collecting electronic data from European site visitors under privacy protection standards that meet the requirements established under the E.U. directive.

---

[82] The FCC is currently reviewing replies from the telecommunications industry.
[83] Electronic Privacy Information Center, www.epic.org
[84] Wired News article, June 5, 2001. www.wired.com/news/ebiz/0,1272,44309,00.html
[85] Other countries, for example Australia, have adopted the provisions in the directive as a frame for their personal data protection legislation.

The Safe Harbor is intended to bridge the gap and provide a way for U.S. companies to continue their business dealings in the E.U. The compromise is set higher than those imposed within the United States and mean that a company's decision to enter into the Safe Harbor will likely result in changes to the company's data collection practices respecting U.S. customers. Companies entering the Safe Harbor must agree to comply with the following requirements[86]:

Notice: A data-collecting organization must inform individuals about what types of personal information it collects about them, how it collects that information, the purposes for which it collects such information, the types of organizations to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language that is readily understood and made available when individuals are first asked to provide personal information to the organization. This provision is more or less a copy of the FTC's fair information practices first principle. Put in a wireless context, the problem with clear and conspicuous disclosures on small screens withstands.

Choice: An organization must give individuals the opportunity to choose (opt-out choice) whether and how personal information they provide is used (where such use is unrelated to the uses for which they originally disclosed it). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For certain kinds of sensitive information, such as medical information, they must be given affirmative or explicit (opt in) choice. As with the *Notice* provision, opting out of the release of unrelated information will be difficult in the wireless context.

Onward Transfer: Individuals must be given the opportunity to choose whether, and the manner in which, a third party can use the personal information they provide (when such use is unrelated to the uses for which the individual originally disclosed it). When transferring personal information to third parties, an organization must require that third parties provide at least the same level of privacy protection as originally chosen by the individual. This is, as I see it, the main difference in the Safe Harbor agreement compared to FTC's fair information practices. Putting the burden of evidence on the organization that transfer the data, as opposed

[86] The Safe Harbor provisions can be found at the U.S. Department of Commerce website; www.export.gov/safeharbor

to the organization receiving the data, it is likely that organizations will be more reluctant to supply third parties with personal data about their users.

Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the principles and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include

(a) A readily available and affordable independent remedy mechanisms by which individuals' complaints and disputes can be resolved;
(b) Systems for verifying that the assertions businesses make about their privacy practices are true and privacy practices have been implemented as presented; and
(c) Obligations to remedy any failure of compliance of the adopted principles.

Sanctions must be sufficient to ensure compliance by organizations and must provide individuals the means for enforcement. Organizations may satisfy the requirements through compliance with private sector developed privacy programs that include effective enforcement mechanisms; or through compliance with legal or regulatory supervisory authorities; or by committing to cooperate with data protection authorities located in the European Community.

The agreement also includes provisions on Security, Data integrity, and Access. Since these provisions do not differ from their "counterparts" in the Fair Information Practices set up by FTC, I will not go in to these further.

Organizations that participate in the Safe Harbor will be deemed to comply with the European adequacy standards (and the E.U. member nations will be bound by this decision). These companies are no longer required to obtain separate approvals from the E.U. member nations, as any such requirements will be deemed waived or automatically granted.

As of August 16, 2001, 88 organizations have signed the Safe Harbor agreement[87].

The Safe Harbor applies to companies that are regulated by the Federal Trade Commission and Department of Transportation. Other industries, including the Telecommunications industry, are not required to enter into the Safe Harbor to continue data collection practices in the E.U. The telecommunications sector though, is, as mentioned earlier, forced to comply with very stringent rules. The Safe Harbor agreement will, however, be applicable to other actors on the wireless scene, such as content- and service providers.

[87] http://web.ita.doc.gov/safeharbor/shlist.nsf

4. Analysis

4.1 The consent of the user

Central for privacy protection is whether or not the data subject agrees to having his or her personal data collected and processed. After an agreement is made, and personal data is collected, the protection will be a matter of security instead of privacy.

Whether a company collects personal data from European or American users, notice and choice regarding their collection practices must be given. Apart from the opt-in regime of Europe and the self-regulatory opt-in / opt-out regime of the U.S. there are some fundamental similarities. Data processing is limited to the consented purposes; for different purposes a new consent is necessary, furthermore there must be a possibility to withdraw the consent at any time for the whole service or for parts of it.
The user must be informed about which data will be collected, for what purpose they will be used and when they will be deleted.

With all the consents, there is likely to evolve something one could call "consent management". Every company that build user profiles; need to include the users privacy preferences into the profile. This will be especially true if the company collects personal data from different touch points (e.g. cell phones, wired computers, direct mail campaigns etc.)[88].

4.1.1 Consent "on the spot" – point and click

In the wireless environment, user consent can be exercised by clicking a box on the screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The wireless environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, users could be required to specify their preferences regarding information use before accessing a mobile website, thus effectively eliminating any need for default rules (see P3P below).

The legality of so called "point-and-click" agreements, where the user by clicking "ok" on his or hers cell phone agrees to something, is difficult to give a quick answer to. The traditional nature of a two-party agreement is not respected since the terms of such agreements are typically non-negotiable, and the user indicates acceptance or rejection by simply clicking a

[88] Forrester, *Customer Context Servers*, p9.

button, easily meeting the conditions that make such agreements enforceable. When it comes to collecting personal data from a user, one could argue whether or not an agreement is made. In Europe there should be an agreement, since businesses in most cases need to obtain consent from the consumer before processing personal information. In the U.S., it is enough to inform the user about the data collection practices. Whether or not the company needs to obtain consent from the user, the information about their data collection must be presented to the user. In the wired world, most companies have a privacy policy stated on their website, informing the user about their personal data collection practices. This statement is very seldom read by the website visitor[89], and this will not likely change in the wireless world. In the wireless context, there are some new dimensions to this problem to acknowledge. First of all, time; I don't believe that the average mobile user takes time to read a privacy policy before accepting the terms (in part because of the limited screen size as mentioned below). The second is money; it is more expensive to access the web from a cell phone than from a wired computer at home. If users don't read privacy policies at home, why should they bother paying to do so when they are mobile? The main obstacle though, is the limited screen size on mobile devices. It is not always easy, even for a lawyer, to understand a company's privacy policy when read on a 17" monitor. Reading it on a 4-line cell phone screen would be a real challenge, even for the most enthusiastic m-commerce lawyer. It is unlikely that mobile phones with limited text capabilities would provide an adequate mechanism for obtaining properly informed consent, although an extra "pop-up" agreement containing the most important information could be enough in some cases[90].

The user consent provision in the E.U. directive has no user age-limit. Any person who can understand what he or she consents to is bound by this consent. If an underage user can or cannot understand the information, must be decided from case to case[91]. In the context of understanding a privacy policy stated on a mobile website, I don't think anyone really can understand everything stated in the policy. Similarly, I don't think anyone can put together a privacy policy covering the personal data collection practices in two paragraphs that all users can understand. It is my belief that consent must be given through a different channel, at a different time.

---

[89] For example, the second largest retail site on the Web, www.americangreetings.com, has a click-through rate on its privacy policy link of 0.009%, according to a Zdnet article (www.zdnet.com, article posted September 11 2000).
[90] Hultmark, p74.
[91] Datainspektionen, FAQ. www.datainspektionen.se

4.1.2 Problems regarding evidence

The limited screen capacity is, as I see it, the main obstacle. There are others too; from an evidence perspective it could be difficult to prove what the user agreed to at the time the "click" was made. The contracting party can easily change the provisions of the agreement from day to day, if they want to. It is, as mentioned above, easy to see that users are likely to "click ok" before reading the agreement. The company supplying the point-and-click agreement must have the technical means and routines to be able to prove what the agreement was at the point when the "ok click" was made[92]. If the burden of evidence should change for some reason[93], it will be difficult to find experts that can untangle the gateway or service providers' site log files.[94]

4.1.3 User consent given prior the use of m-commerce services

If user consent is not given "on the spot", it must be given prior to the personal data will be collected and processed. The question then is, to whom should the user give his or hers consent? Should it be given to the network carrier, the gateway, the service/content-provider, or all of the above?

When it comes to user location data, consent given to the network carrier is obvious. It is the only place where location information can be derived from.

The gateway will need user consent if it collects personal information and not only works as a conduit, transforming websites to mobile device readable languages. As will the content or service providers need user consent, if they collect personally identifiable information about their users.

A user accessing a website through his or hers cell phone, are as mentioned above, not likely to fully understand that websites privacy policy. An agreement could be made with the network carrier, which in turn only have agreements with content providers that have identical privacy policies.

The problem then is that users will get stuck within the carriers "walled garden", and only be able to access certain selected websites. Such an agreement could also be made with a gateway. By signing an agreement with the gateway, the user puts his trust within that organization. He or she will only have access to certain sites, but in turn will be sure (as long as he/she can trust the gateway) that the personal data will be processed in a beforehand

[92] Hultmark, p.75
[93] In a business-to-business relationship for example.
[94] Forrester, Branding divorces advertising, p15

known way. These agreements would probably be very general in their provisions. It is likely that the contracting company (network carrier, gateway, or service/content provider), will request a broader consent than they initially need to carry out their services. Why? Because it would be very difficult to get back to each and every user as soon as consent is needed for each individual service.

4.2 Implications for U.S. companies when dealing with European users

While user consent generally is needed when companies collect and/or process personal data in Europe, it is as earlier mentioned not required in the U.S. However, under the E.U. directive U.S. companies will have to respect European legal mandates. Unless American companies doing business in Europe chose to flout European law, U.S. multinational businesses must provide stringent privacy protections to data of European origin when processing that data in Europe or in the United States.

Concurrently, American law and practice allows those same companies to provide far less protection, if any, to data about American citizens. This is a particularly troubling aspect of U.S. opposition to the European Directive's standards. American companies will either provide Europeans with better protection than they provide to Americans or they will treat Americans in accordance with the higher foreign standards and disadvantages those citizens doing business with local U.S. companies.

In effect, the creation of European style data protection measures around the world means increasingly that American citizens will be left with second-class privacy in the United States and afforded greater privacy protection against American companies outside U.S. borders[95].

4.3 Technical alternatives for privacy protection.

An appropriate legal framework for privacy protection is necessary, but not sufficient.
The practical problems are hard to overcome with legislation, especially since there will be loads of different national legislation governing these issues. There also have to exist technical means for this kind of consent-management.
Luckily, personal integrity is not only protected by legislation.

[95] Reidenberg, p7f

Guidelines from different agencies, and technical solutions for integrity protection have a major impact on m-commerce.
This is, as been shown in previous chapters of this essay, especially true in the U.S., but will most likely play a big role in Europe in the future as well.[96]
A technical solution to the consent-management problem could alleviate the tension between Europe and the U.S. in the matter of data protection. If a common set of rules were set out in the very architecture of m-commerce solutions, it would guarantee that both Americans and Europeans are treated equally. One of the most seriously made attempts for such a technical solution is P3P.

Platform for Privacy Protection (P3P)

The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see[97]. P3P simplifies the "informed consent" problem by providing a mechanism for better informing the user about the privacy policy of a web site.

P3P answers two distinct problems[98]:

- The business problem; How can a business express their privacy practices in such a way that users can quickly and easily make trust decisions about their website.
- The user problem; How can users quickly and easily determine if a web site abides by their privacy preferences.

[96] Lindberg/Westman p.109, examining the E.U. Directive §27.
[97] World Wide Web consortium, www.w3.org/p3p
[98] WAP-W3C workshop, Paper issued by Marc Le Maitre from Nextel

By arming the user with a tool that can machine-read a web site's privacy policy, P3P allows the user to match a site's privacy policy with their pre-determined preference list.
When areas of conflict arise between user preference and web site policy the user tool (browser plug-in) alerts the user who can then take appropriate actions, such as deciding not to provide data to the site.
P3P is not yet applicable in the mobile environment, but is likely to be so in the future[99].
As with all new technology, there is a backside. Although solving a lot of problems, P3P creates a few new ones. E.U. officials think there is a risk that P3P could mislead European based operators into believing that they can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data) if the individual user consents to this as part of the online negotiation[100]. And there is of course the small screen problem. Once the user has programmed his or hers privacy preferences into the browser, its unlikely that he or she will change these settings in the future. It would be a hassle to change privacy preferences on the go, and therefore users are, in my opinion, likely to set their privacy preference setting somewhat low in order to be able to surf the wireless web without too many "privacy alert" messages popping up on the screen.

[99] WAP-W3C workshop, final report.
[100] Working party, Opinion 1/98

5. Conclusion

Privacy means different things to different people, and can be invoked in many contexts. Privacy for me, in the context of this essay, means the protection of personal data from being used in a manner I have not given my consent to. Standards for the transfer of data are, as I see it, the most important issue in the m-commerce privacy debate. Companies that track cell phones, and who build user profiles, should use the data collected only for its intended and approved uses. It is clear that in the networked society, the individual's privacy is at risk. A side effect of global wired and wireless communication is that personal data of the users will be collected at different companies and be used to create user profiles.

Taking away the "or" and the question mark from this essays title will be a hassle in the wireless environment. Difficult as it may be, it should not be impossible.

Anonymous personalization will work in most cases. It is not always necessary to know the users identity in order to deliver a personalized service. What is necessary is to link a profile to always the same user. Both U.S. and E.U. law would permit this "pseudonymous profiling".

5. 1 Disclosing privacy preferences

In cases where anonymous personalization is not used, the users need to be able to disclose their privacy preferences in an easy manner. It is a difficult task for the actors on the wireless scene to solve this problem. As mentioned in almost every chapter of this essay, the small screens of today's wireless devices is the most difficult obstacle to overcome. It is not likely that the screens will be much bigger in the future than they are today. No one wants to carry a wireless device with a 12" screen. So how can privacy notices be presented in a way that would comply with E.U. and U.S. legislation? If a proposal is put forward to use a certain means of notice or a certain means of eliciting consent, maybe the lawmakers need to put those mechanisms in front of real users, and ask them "do you understand what is happening here, and do you understand what you are agreeing to?"

Device customization can help ensure that all information receives the proper placement and thus the proper attention from the customer, but there need to be a level playing field. No matter how effective the device customization is, there will be users with screens that are too small to read relatively long privacy notices.

If these privacy notices will pop-up from both the network carrier and all the wireless websites, will the average user know what he or she really has agreed to?

As I see it, there is a risk that users will get tired of getting notices as soon as information is about to be collected. Wireless communications should be quick and easy to use, is there time for worrying about integrity issues in the wireless environment?

5.2 Is privacy even worth protecting?

Does it matter if Espresso House knows that I drink on average two cups of Latte per week? Lets assume that Espresso House supplied this information to my insurance company, and apart from the "coffee information" they also received information about my recent beer purchases from the local liquor store. All of a sudden, the insurance company would have a somewhat extensive file about me, and could increase the cost of my life-insurance policy based on my not-so-healthy diet. If this would happen, then we are living in Orwell's world. To make sure we don't end up in a "Big Brother" situation, there must be clear guidelines and rules for the wireless industry to follow, and there must be ways of effectively enforce these rules.

Consumers must know their rights, and must learn to value their privacy. Personal data is, and will continue to be, hard currency in the personalization business. The trick to personalization is getting the user to reveal as much as possible about his or her preferences and habits. Consumers should guard their data because their information is worth money to companies, and that by disclosing it, they are more exposed to marketers intrusions. To get customers to "spend" this currency, retailers must explain how they will use the data and clearly present the benefits created for consumers. There is a risk that companies will try to obtain unnecessary amounts of personal data in exchange for different perks ("Fill out this survey, and you will get 2000 frequent flyer points").

5.3 Location information

With an always-on connection combined with tracking capabilities, smart phones may compromise the personal privacy of users by continuous pinpoint location tracking. This capability could virtually eliminate an individual's capacity to move freely without "surveillance". Without some way for cell phone users to control being tracked, users may fear they will be monitored without restriction.

It is important to ask a few questions about utilizing tracking technology:

- How, when, and why is tracking being used?
- How can users disable tracking?
- How would cell phone users know if they were being tracked?

The E.U. working party's guidelines on location information is an excellent start for solving these problems. It will be important to include standards for the use of wireless tracking capabilities to deliver personalized messaging. These standards should determine the level of permission needed to utilize tracking technology and deliver location-based messages. Notice should be given as to whether or not tracking technology will or could be utilized and what will be done with the information collected. The difficult question to answer, however, is who should be responsible for informing cell phone users about tracking capabilities? Upon selling a cell phone, perhaps the provider should include such notice as a general warning to the user. It should be the responsibility of the m-commerce industry to develop standards for education of the public on the benefits and potential risks of smart phones. But how will this be done practically? Once users are aware of the capabilities, they should have the opportunity to choose whether or not they should be tracked. In the case of the coffee coupon, a consumer may very well appreciate the benefits of tracking. However, no one should have the feeling of "Big Brother" watching every move.

5.4 Final thoughts

It is easy to focus too much on legislative measures. With network enabled tracking, the tracking cannot be disabled in an easy way. Users, who want to receive targeted advertisements, should not have to decide from time to time whether or not they should be available for these ads. It would be too much of a hassle to change ones settings on the wireless device "on the spot". With technical measures, such as P3P, it should be possible to "program" ones device to only receive ads from certain companies and at certain times of the day. But once the users want to change these settings, there will be a problem.

Besides, a lot of the "charm" about advertising is that the consumer is notified about something he or she might not have thought about before. That does not necessarily mean that the marketers are creating a need for the consumer, but that he or she is provided with options that otherwise might have been overlooked.

For example, lets say I program my wireless device to only receive restaurant ads from Italian restaurants. I'm on an assignment from my company, and don't know anything about the city I'm in. Two blocks from where I'm standing is the best Thai restaurant west of the Himalayas. On the other side of town is a shabby Italian pizza-joint. I will receive an ad from the pizza place, and thereby missing out on a great Thai dinner.

It is likely that users will set their preferences somewhat low (or general), in order to be able to receive all kinds of ads. As long as this technology is not used for sending SPAM messages, I think it is a great thing. Advertisers are eager to use location services to alert you when you pass near a store that might be of interest. They're aware you may not want to see ads for McDonalds every time you pass by the golden arches. And Network carriers, who supply the information, don't want to annoy users because it is so easy to switch providers. With combined legislation, self-regulatory measures, and technical solutions, this could be a win-win situation for all parties involved.
Giving up some privacy will be necessary if one wants to enjoy all the benefits of personalized and location based services. Although legislation is necessary, it should not hamper the evolution of m-commerce. Before passing too rigorous privacy laws, lawmakers should ask themselves "do we really, really need this privacy protection?"

Bibliography

Literature

E-business legal handbook
Michael Rustad & Cyrus Daftary
2001, Aspen Law & Business, New York, NY, U.S.A

Elektronisk handel och avtalsrätt
Christina Hultmark
1998, Nordstedts Juridik, Stockholm, Sweden

Praktisk IT-rätt
Agne Lindberg & Daniel Westman
1999, Nordstedts Juridik, Stockholm, Sweden

European Union Directives, proposals, and common positions

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector.

Commission Proposal, COM (2000) 385 final. Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Working party on data protection. Common position on *Privacy and location information in mobile communications services*, February 2001.

Working Party on data protection. Opinion 1/98; Platform for Privacy Protection (P3P) and the Open Profiling Standard (OPS)

Report and Workshop transcripts

FTC report to Congress “Privacy Online: Fair Information Practices in the Electronic Marketplace”, May 25 2000. (www.ftc.gov/reports/privacy2000/privacy2000.pdf)

FTC, Online Profiling workshop, November 8-9 1999
(www.ftc.gov/os/2000/07/onlineprofiling.htm)

FTC, Wireless Web workshop "*Emerging Technologies & Consumer Issues*”, December 11-12 2000 (www.ftc.gov/bcp/workshops/wireless)

WAP Forum (WAP) and World Wide Web Consortium (W3C) workshop on *Position Dependent Information Services,* February 15-16 2000 (www.w3.org/Mobile/posdep-workshop)

Research Papers
Forrester Research, Branding Divorces Advertising, June 2000
Forrester Research, Customer Context Servers, October 2000
Forrester Research, Mobile Internet Realities, May 2000 (www.forrester.com)
Jupiter Research, Marketing Report, September 2000 (www.jmm.com)

Fact sheets
Information on the Personal Data Act, Ju 98.05 Fact sheet
Swedish Ministry of Justice

Interview
Interview with Mattias Malmnäs, Adaptlogic. August 4, 2001.

Other sources
Joel R. Reidenberg
Testimony before the Subcommittee on Commerce, Trade and Consumer Protection
United States House of Representatives
Hearing on the EU Data Protection Directive: Implications for the U.S. Privacy Debate March 8, 2001
(Transcript at http://energycommerce.house.gov/107/hearings/03082001Hearing49/ Reidenberg104print.htm)

Websites in alphabetical order. Websites visited at different occasions from March to August 2001.
http://web.ita.doc.gov
www.adaptlogic.com
www.allnetdevices.com
www.ccpp.org
www.cdt.org
www.cell-loc.com
www.datainspektionen.se
www.epic.org
www.ericsson.com
www.export.gov
www.fcc.gov
www.forrester.com
www.ftc.gov
www.gpsworld.com
www.hi3g.com
www.jmm.com
www.melody.se
www.nokia.com
www.nttdocomo.com
www.onstar.com
www.personalization.org
www.privacyalliance.org
www.privacyheadquarters.com
www.teliamobile.com
www.tinhat.com
www.truste.org
www.vindigo.com
www.w3.org
www.wired.com
www.wow-com.com
www.yale.edu
www.zdnet.com