

Chapter 6

The Diffusion Landscape: Barriers and Promoters

“The collection of geographic location information creates a huge new privacy problem that we have little experience dealing with. Never before has the specific location of millions of individuals been available in a way that is so easy to collect and disseminate,” says Alan Davidson, general counsel for the Center for Democracy and Technology, a privacy organization in Washington, D.C. (Cleary, 2001)

Introduction

As the social informatics perspective suggests, the societal context of technology is vital to understanding its effects within society, i.e. how it is used and adopted. Mobile phones, for example, have certain societal effects, for instance the breakdown of public and private geographies. Consequently, societies may therefore view and utilize this technology differently. The same is true with retail LBS. The societal context of retail LBS is likely to make a profound difference to whether or not the vectors, i.e. mobile phones, effectively aid in the diffusion and adoption of this technology. Diffusion promoters, such as an innovative and technologically adept society, will aid in the diffusion of retail LBS, whereas barriers, such as privacy concerns, may impede its diffusion and adoption (Interviewee-2, 2003). Although there are many potential barriers and promoters to the diffusion of retail LBS, the issue widely discussed by both academics and journalists concerns privacy, perhaps the crucial barrier impeding widespread retail LBS diffusion.

This chapter proceeds as follows: first, I briefly introduce the concept of privacy, while defining privacy and personal information. Secondly, I examine particular privacy and data control policies, industry associations, and advocacy groups in the US acting as potential barriers or promoters of retail LBS diffusion. Next I analyze the same types of regulations and actors in the EU and Germany. Lastly, I review differences in privacy policies between the US and EU (particularly Germany). Throughout these discussions, I introduce perspectives of individuals I interviewed or surveyed on the subject of retail LBS.

The Issue of Privacy

Privacy issues are inherently important in the adoption of certain technologies and are often topics of discussion in the media. Recent examples where privacy issues have been discussed concern file-sharing (Madden and Lenhart, 2003), radio frequency identification (RFID) (Thomas, 2004), online security (Dubash, 2003), location privacy (Cantos *et al.*, 2001), and GIS (Divis, 2000). The collapse of public versus private geographies has also been studied in relation to mobile phone use. One such study was

done by Context-Based Research Group, an organization of anthropologists and ethnographers studying consumer trends.

The study found that due to mobile phones, communities are no longer limited by geography or their immediate physical surroundings (Context-Based Research Group, 2002). Mobile phones can be taken anywhere and individuals can communicate irrespective of geography - a frequent complaint of subjects in the study (Context-Based Research Group, 2002). Communication regarding “geographical locating”, as Eric Laurier terms it, is frequently observed during mobile phone calls (Laurier, 2001, p 485). Laurier claims that geographical locating, telling someone where you are while on your mobile, occurs because you do not share the same time or space with that person (Laurier, 2001), as, for example, when you are on a bus in Washington DC and your friend is on a business trip in Düsseldorf. Geographical locating therefore attempts to bridge the disconnection between person and place (Laurier, 2001), also referred to as “disconnected urbanism” (Goldberger, 2003). Cities, a place where people from different walks of life come together, have changed due to the proliferation of mobile phones and the fact that “half of [the people] are elsewhere” (Goldberger, 2003). The outcome is that public spaces are becoming increasingly private spaces (Goldberger, 2003); a significant effect within society.

In contrast, location-based services (LBSs) raise concerns about the loss of privacy - a concern that private information is becoming increasingly public. The fact that someone other than the individual with the mobile device knows where that person is located and has the ability to track the individual is widely considered disconcerting (Anonymous, 2001b; Cantos *et al.*, 2001; Divis, 2000; Hamblen and Brewen, 2001). The same concern for privacy involved with LBSs was declared by twenty-five of 29 survey respondents.

According to a study done on consumer interest in LBSs by the Driscoll-Wolfe Marketing & Research Consulting firm (discussed in Chapter 5), subjects also stated their concern over the potential loss of privacy (Barnes, 2002). The potential ‘big brother’ effect with the use of LBSs has some consumers worried (Driscoll, 2002). The same concern of ‘big brother’ was brought up by four respondents to my survey – each stating

that consumers are likely to worry about this aspect of LBS. One US respondent specifically stated that ‘big brother’ would be a “huge concern for consumers.” Yet, according to Clement Driscoll, in relation to the Driscoll-Wolfe study, most people feel that the “potential benefits outweigh the drawbacks” and are “receptive to the notion of location-based advertising, if it is not intrusive and will reduce their service fees” (Driscoll, 2002). A fee reduction would be a potentially positive feature for retail LBS diffusion, or location-based advertising, with 11 of 15 US respondents and six of 11 EU respondents to my survey claiming that people are likely to pay for LBS in their country (see Appendix B). Overwhelmingly, all but two respondents asserted that companies would promote retail LBS even if there was an initial lack of consumer demand for the service.

Despite these positive responses concerning LBS growth, a report by the ARC, cited in Chapter 5, stated that uncertainty surrounding privacy issues made operators cautious about deploying LBSs (PR Newswire, 2002). Wireless carriers, LBS providers, and technology providers all struggle with the privacy issue regarding LBSs (VanderMeer, 2002a). In particular, they grapple with who owns and has access to the location of a wireless user (VanderMeer, 2002a). One survey respondent commented, “The question about who has access to the location information is clearly undetermined today.” The uncertainties of location ownership and privacy concerns are perhaps what prompted over half of US and EU respondents (8/15 US and 8/11 EU) to respond ‘no’ when asked whether or not they would personally subscribe for retail LBS on their mobile phones.

Defining Privacy and Personal Information

The notion of privacy is complex and somewhat intangible, with no straightforward definition (Bagby, 2003; Curry, 1998; Marcella and Stucki, 2003). Privacy applies to “information-handling practices of an organization and the processing of personal information through all stages of its (the information’s) life cycle, including collection, [...] consultation and use, [...] and erasure and destruction” (Marcella and Stucki, 2003, p xii). Privacy can also refer to “several distinct interests, individual expectations, legal rights, and [personal identifiable information] data practices” (Bagby, 2003, p 443). It

has also been defined as “a concept that relates to individuals, and their desire to guard against intrusion, appropriation, or breach of confidence” (Goodchild, 2001). Personal identifiable information (PII) can include a person’s name, address, phone number, social security number, etc., allowing a person to be contacted, located, and identified (Marcella and Stucki, 2003, p xii). Individual information combined with household data collected by the census has been referred to as ‘*geodemographic* information’ (Curry, 1998), using the prefix ‘geo-’ to signify location information. Increasingly, such information concerning individuals has been made available for government and corporate use (Curry, 1998).

Regulating Privacy

Ways of regulating privacy differ due to geography and subsequently societal context. This distinction becomes apparent when comparing privacy regulations in the US and EU. The US has traditionally shied away from creating all-encompassing privacy protection laws for its citizens and has instead established reactive policies (Bagby, 2003, p 442; White, 1997, p 232-33). This may be explained by cultural lag theory, which claims that government regulations generally lag behind technological development and advancement (mentioned in Chapter 3). In contrast, the EU has preempted technological adoption with comprehensive consumer rights protection, also called the omnibus method to privacy concerns (Bagby, 2003, p 442; White, 1997, p 232). Thus, we might expect technological innovation and diffusion of retail LBS to advance quickly due to little regulation, as in the US, and limited by laws already in place, such as in the EU.

US Privacy Laws

To quote John W. Bagby, Professor of Business Law at The Pennsylvania State University:

US Privacy Law Protection is a hodge-podge, patch-work of sectoral protections, narrowly construed and derived from constitutional, statutory, and regulatory provisions of international, federal, and state law. (Bagby, 2003, p 442)

It seems therefore, that there are no clear, strict laws concerning privacy. Businesses and some government interests generally oppose the idea of stronger, more comprehensive

laws protecting an individual's right to privacy (Bagby, 2003; Curry, 1998). Despite their similar interests, distinguishing between the private (or business) sector and the public sector (which includes the government), is important in understanding privacy restrictions.

The Fourth Amendment was the first fundamental proclamation by the US government protecting the privacy of US citizens. It states that people have a right to be protected against “unreasonable searches and seizures” (US Government, 1789). The Fourth Amendment, however, focused on privacy concerns in relation to the government, while the focus has since shifted to include private parties as well (Bagby, 2003, p 446). With the steady use and increase of wireless communications, laws have been created to safeguard electronic communications, including signals, images, sounds, and data transferred via wire, radio, and electromagnetic systems, among others (Bagby, 2003, p 482). The **Electronic Communications Privacy Act (ECPA) of 1986** protects the confidentiality of all voice and data transmissions on wireless networks. The ECPA also protects against illegal access to stored communications, i.e. accessing information in computers, but there are exceptions (“Electronic Communications Privacy Act,” 1986). The government, for example, may require the electronic communications provider to disclose the contents of an electronic communication (“Electronic Communications Privacy Act,” 1986). In addition, the contents of the communication may be revealed to “a person employed or authorized or whose facilities are used to forward such communication to its destination” (“Electronic Communications Privacy Act,” 1986). Thus, electronic communications are considered the property of the wireless carriers (not the customer), as their facilities are used to forward a wireless communication.

Other US laws also deal with communications privacy. Regulations made by the Federal Communications Commission (FCC) under the **Telecommunications Act of 1996** require phone companies to “guard the privacy of consumer proprietary network information (CPNI) to their parties” (Bagby, 2003, p 462). At the time of this act, CPNI did not include consumer location, but only incorporated time and date of call, duration of the call, and the number dialed (Ackerman *et al.*, 2003). There were no regulations specifying the type of customer consent required for CPNI, i.e. whether the customer

must express consent prior to use of the information ('opt-in') or express prior consent *not* to use the information ('opt-out') (Ackerman *et al.*, 2003). This has since changed (2000).

Consent policies significantly affect the proportion of participants; opt-in consent policies generally have low numbers of participants, while opt-out consent systems have high numbers of participants (Figure 6.1) (Bagby, 2003, p 461).

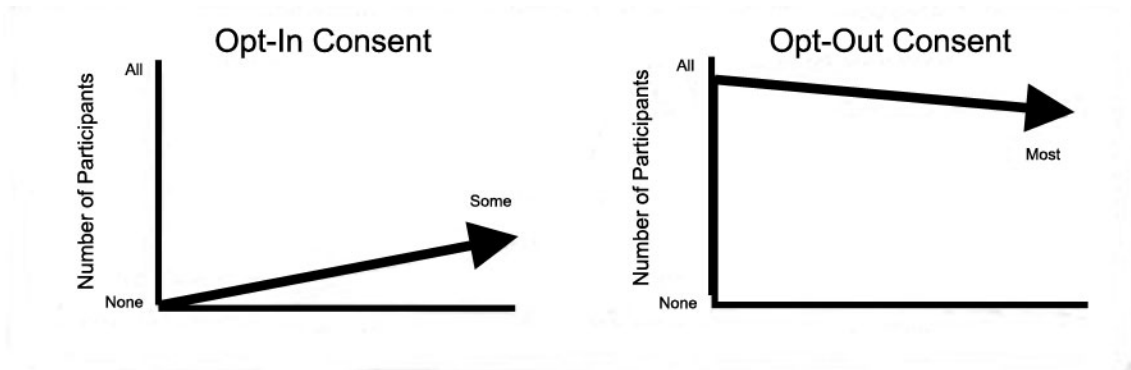


Figure 6.1. Proportion of participants: opt-in versus opt-out (from (Bagby, 2003, p 461))

The two systems affect the degree to which individuals can protect their private information. In an opt-in situation, people are given an agreement up front when subscribing for services and hence there are few privacy concerns with this method (Interviewee-4, 2003). In general, US privacy laws favor self-regulation and businesses' rights to collect data on individuals (Bagby, 2003; Interviewee-3, 2003). The Clinton Administration, the Federal Trade Commission, and a group of Internet advertisers, embraced the self-regulation plan requiring consumers to opt-out to protect their own privacy (Fox *et al.*, 2000, p 6) – meaning that consumers are required to take action to *prevent* collection and use of PII, while opt-in requires an action to *permit* the gathering of PII (Bagby, 2003, p 459). The opt-out system is the one used by many US businesses (Bagby, 2003).

The **Wireless Communication and Public Safety Act (WCPSA) of 1999** modified some of the vague rules of the 1996 Telecommunications Act, including the system used to protect consumer information (opt-in vs. opt-out). With the passing of the WCPSA, also called the E911 Act (Ackerman *et al.*, 2003), *location* information became

incorporated into the definition of CPNI (Bagby, 2003, p 483; CTIA, 2000). CPNI is now defined as “information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer” (Bagby, 2003, p 483). The WCPSA allows wireless network operators to make public a mobile user’s geographic location in emergency situations (Goodchild, 2001), but it must get the approval of customers (opt-in) before using and revealing location information to third parties for marketing purposes (Bagby, 2003 , p 483; Cleary, 2001). However, nowhere is it stated in the WCPSA that the government can be prevented from seizing customer details (Cleary, 2001).

In 1998, before the passing of the WCPSA, the FCC was in the process of deciding whether or not telecommunication carriers must protect CPNI at all (Ackerman *et al.*, 2003; CTIA, 2000). Initially in 1998, use of location information was restricted by opt-in consent (Ackerman *et al.*, 2003; WLIA, 2001c). Yet, a court case (US West v. FCC) challenged the limits put on the use of CPNI, stating it was in violation of the First Amendment¹ (Ackerman *et al.*, 2003; Bagby, 2003; CTIA, 2000; WLIA, 2001c). The 10th Circuit Court of Appeals decided that opt-in consent for use of CPNI was a restriction on a carrier’s First Amendment rights to free speech (Ackerman *et al.*, 2003; Bagby, 2003; CTIA, 2000). In essence, the court viewed the phone company’s use and disclosure of CPNI as protected under free commercial speech², included in the First Amendment (Bagby, 2003). Thereafter, in 2001, the FCC ruled that opt-in consent is not required and in 2002, it decided that either opt-in or opt-out systems could be used by telecommunications companies for CPNI, which now included location information (Ackerman *et al.*, 2003).

US Associations and Technology Interest Groups

In the absence of clear-cut federal regulations prohibiting the use of personal location information, industry associations as well as technology interest groups have suggested

¹ The First Amendment protects an individual’s freedom of religion, freedom of speech or press, freedom to peaceably assemble, and freedom to lobby the Government to rectify grievances (US Government, 1789).

² Commercial speech is categorized as that used to facilitate marketing, i.e. commercial solicitation (Bagby, 2003).

self-regulatory measures. The existence of such groups and their purpose were noted by various survey respondents. The Cellular Telecommunications and Internet Association (CTIA), an international trade organization of the wireless communications industry including wireless carriers such as Cingular, T-Mobile, Verizon, petitioned the FCC to address ambiguities about the use of location information created by the WCPSA (CTIA, 2000). The association requested that the FCC implement CTIA's proposed privacy principles (Ackerman *et al.*, 2003), which include: informing the consumer about how location information is collected, allowing the user to have control over authorization prior to data collection (opt-in), requiring that LBS providers securely retain location information, and regarding all LBSs as equals whether the service utilizes network- or handset-based solutions (CTIA, 2000).

The Center for Democracy and Technology (CDT), a non-profit organization committed to furthering individual liberties in new means of communications (CDT, 2004a), also supported the CTIA's petition and submitted comments before the FCC as well (CDT, 2001). It, as well as the CTIA, believed that wireless location information "pose[s] uniquely sensitive privacy concerns" (CDT, 2001), which needed to be acted upon immediately. The CDT also believed that the rulings made by the FCC in the WCPSA in 1999 and those made by the Court of Appeals in 2001 did not provide clear language about nor enough protection concerning the privacy of a customer's location information (CDT, 2001).

Despite attempts made by the CTIA and CDT to request the FCC to establish clearer and more stringent guidelines concerning location information, the FCC declined the CTIA's petition (Ackerman *et al.*, 2003). The FCC stated its reasons as: 1) the importance of location information for the E911 Act, 2) the E911 Act clearly protected the consumer, and 3) they "[did] not wish to artificially constrain the still-developing market for location-based services" (FCC, 2002). In addition to this impediment for location privacy protection, several bills sent to Congress also requiring opt-in consent never made it to the floor and hence were never voted upon (Ackerman *et al.*, 2003). One such bill was the **Location Privacy Protection Act of 2001**, introduced by Senator John Edwards on July 11, 2001, (Interviewee-3, 2003; "Location Privacy Protection Act,"

2001). This Act specified guiding principles concerning the “collection, use, disclosure of, retention of and access to customer location information” (Cantos *et al.*, 2001). In addition, the bill would require the providers of LBSs to obtain explicit authorization before using the location information or passing the information on to third parties (Cantos *et al.*, 2001). A similar bill introduced in 2001, the **Wireless Privacy Protection Act of 2001**, would also require “informed customer consent to the provision of wireless call location and crash information” (“Wireless Privacy Protection Act,” 2001). However, neither bill was passed nor has either been made into law. Even an attempt by Washington State to obtain a ruling on opt-in consent for the use of CPNI has proved ineffective (Ackerman *et al.*, 2003). Because of these unsuccessful attempts at regulation, the CTIA in September 2003 proposed self-regulation through the use of a “consumer code”, which asks companies to endorse their own privacy policies (Ackerman *et al.*, 2003).

The CTIA and the CDT are not the only organizations striving for more rigorous privacy regulations. Another such association, the Wireless Location Industry Association (WLIA), was founded in December of 2000 by eight principal companies involved in the wireless location industry in the US, Canada, and the EU (Leite and Pereira, 2002). It provided an environment in which to develop self-regulation privacy policies as well as to provide information about the wireless location industry to the public and policy-makers (Leite and Pereira, 2002). In addition, it established guidelines for companies to protect the privacy of wireless subscribers (Interviewee-3, 2003; WLIA, 2001a). This organization, due to heavy financial burdens (Interviewee-3, 2003) has since disbanded and the Cellular Telecommunications and Internet Association (CTIA) is now working on similar issues.

In addition to the CTIA and CDT, other technology interest groups share the same concern for privacy. EPIC, the Electronic Privacy Information Center, is a public interest research center in Washington, D.C. established in 1994 (EPIC, 2004). EPIC attempts to focus “public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values” (EPIC, 2004). The Electronic Frontier Foundation (EFF) is another such organization. EFF collects donations from members in

order to work “to protect our fundamental rights regardless of technology; to educate the press, policymakers and the general public about civil liberties issues related to technology; and to act as a defender of those liberties” (EFF, 2003). EFF also initiates and defends court cases to preserve individual rights (EFF, 2003). These industry associations and technology interest groups have been active in providing the private sector with industry guidelines due to the lack of straightforward governmental privacy regulations.

US Corporate Data Policies

Despite the definitions of privacy mentioned above, it seems that “in the [US] business context, privacy has no absolute meaning” (Bagby, 2003, p 443) and is established by and limited to a balance between theory (public policy) and practice (Bagby, 2003). While most fundamental rules for protecting privacy, e.g. the 1980 OECD Privacy Guidelines (OECD, 1980), are generally agreed upon, “the principles are *not* legally imposed against the commercial and private sectors in the US” (Onsrud, 2003). Businesses, therefore, are not under the jurisdiction of the rules (Masser, 1998; Nelson and Rendleman, 2001; Onsrud, 2003).

Title 15 of the US Code on Commerce and Trade acknowledges that the role of the Federal Trade Commission (FTC) is to enforce the privacy promises made in the marketplace (Legal Information Institute, No date). Laws, such as the Privacy Act of 1974, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act, describe certain rights to privacy for the individual within certain areas of the market, i.e. protecting government information, consumer finance information, credit information, and children's online activities, respectively, and are under the authority of the FTC (Bagby, 2003; Legal Information Institute, No date; Marcella and Stucki, 2003). In other sectors of the commercial market however, “the FTC encourages a voluntary regime of protecting consumer privacy” (Legal Information Institute, No date).

Because businesses are not forced to abide by certain laws and therefore self-regulate through their own privacy standards, it is fairly easy for the private sector to collect information about individuals, access it, and sell it to marketing companies for use

in direct marketing (Divis, 2000). Companies, such as grocery stores, offer ‘shopper club cards’ to customers and ultimately are able to store and use the data collected to direct advertisements to consumers (Divis, 2000; Terdiman, 2003). In addition, certain companies have already developed business plans around the WCPSA legislation, which allows companies to access and use location information. For example, Profilium Corp., a Canadian company, has developed software to profile, track, and communicate with mobile users (Cleary, 2001).

In addition to the freedom given to the private sector when dealing with personal data, new laws have also given more control to the government to obtain location data. The passing of the **Homeland Security Act of 2002** (CNN, 2002) permits the creation of a “Total Information Awareness” (TIA) database, now called “Terrorism Information Awareness” (DARPA, 2003), designed to track a variety of data concerning American citizens (Abernethy, 2003/2004; Marcella and Stucki, 2003, p xx). The database will eventually gather data concerning: credit card purchases, Web sites visited, telephone calls made, travel data, financial records, and emails among others (Marcella and Stucki, 2003, p xx-xxi). However, amid public controversy, the further development of the TIA by the Pentagon's Defense Advanced Research Projects Agency (DARPA) has been slowly disappearing from public view (McCullagh, 2002). Even the former Web site of the TIA [<http://www.darpa.mil/iao/>] (CDT, 2004b) no longer functions. It is unclear if the project continues under another guise.

In the private and public sector, and specifically related to LBS, an important question emerges: who owns a mobile user’s location data? This same question was also posed by several survey respondents. In the realm of LBSs, the privacy of the location data falls under the jurisdiction of the wireless carriers (Hamblen, 2000a; Interviewee-2, 2003; Interviewee-3, 2003). However, one survey respondent in particular explained that “wireless service providers (or the location-determining entities) will need to allow the consumer/subscriber to retain some control of how/when their location is determined/monitored via their wireless device.” But because there are always marketing groups lobbying for access to data, the location data could be sold broadly (Hamblen, 2000a; Interviewee-2, 2003; Thibodeau, 2000). Businesses have said that they will allow

wireless subscribers to opt-in to a service sending digital coupons of a nearby store to a mobile phone (retail LBS), thereby respecting a user's privacy (Hamblen, 2000a). These methods of opting-in however are not yet defined, primarily because it would be hard to read a potentially detailed privacy policy on a small cell phone screen (Hamblen, 2000a). Even with opting-in, wireless spamming has also been a concern due to the accessing and selling of mobile users' location data. One survey respondent wrote, "I have enough trouble with SPAM e-mail without signing up for SPAM SMS." Other respondents also wrote that they would not accept unsolicited information or push marketing on their mobiles.

A spokesman for AT&T, Ritch Blasi, was quoted as saying, "We don't know how location data will be managed or who is going to retain the information, because the technology is not even fully widespread for commercial availability" (Hamblen, 2000a). Yet, perhaps preparing for LBS deployment is a worthwhile reason to figure out who *is* going to manage and maintain the data. Regardless of privacy concerns, companies still believe that a portion of consumers "wants to be alerted to sales opportunities when they are in proximity to a store" claims the director of digital communication services for Best Buy Inc. in Minneapolis (Hamblen, 2000b). This was found to be the case in various survey respondent comments as well. One respondent in particular claimed that if retail LBS was of "direct and personal interest" to him, giving the example of being downtown and being alerted of a Starbucks nearby, he would sign up for the service.

However, other research has stated that the hazards involved with retail LBS are real and are not being sufficiently addressed by the industry (Hamblen, 2000b). Still others, such as the executive vice president of SignalSoft Inc, an LBS software company, assert that there have not been criticisms over privacy simply because carriers are protecting the location information and not forwarding it to advertisers (Hamblen, 2001). Companies such as OnStar and BMW, both offering LBSs, are said to be cautious about infringing on US consumer privacy (Nelson and Rendleman, 2001). BMW says it does not share data with third parties and OnStar only accesses location data if a driver presses a button to connect with the OnStar center (Nelson and Rendleman, 2001). But, as already demonstrated, there is nothing that legally binds these companies to keep

consumer information private and according to one survey respondent, “This [privacy] issue has been quite prolific [sic] in the US.” Perhaps the privacy concern can be explained by the lack of regulation. Only eight of 15 US survey respondents claimed to be aware of any privacy restrictions concerning the access and use of personal information. However, the same impression is not observed Europe; nine of 11 EU respondents were aware of EU government restrictions concerning privacy. Possibly explaining why one respondent wrote that in Europe, “people seem to see [LBSs] as providing them an advantage vs. an invasion of privacy.”

EU Privacy Laws

In contrast to the US’s self-regulation policies, the EU and its member countries have straightforward, overarching regulations concerning privacy. US privacy regulations “have been hindered by a strong anti-regulation tradition” (Curry, 1998, p 111), while Europe has seen a strong influence from the commercial sector in the dissemination of privacy regulations (Curry, 1998, p 111). Article 8 of the European Chapter of Human Rights (European Parliament, 2001), establishes the fundamental right that EU citizens own their private information and that must be protected by law (Divis, 1999; Goodchild, 2001). The Council of Europe with the Convention for the Protection of Human Rights and Fundamental Freedoms agreed to Article 8 – Right to Respect for Private and Family Life, which states:

Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except...in accordance with the law and (as) is necessary in a democratic society. (Council of Europe, 1998)

These fundamental rights along with subsequent EU directives inclusively protect the privacy of EU citizens’ personal information across all industries and all member nations (Bagby, 2003, p 464).

EU Directives

An EU Directive established in July 2002 entitled **The Directive on Privacy and Electronic Communications (2002/58/EC)** presents ‘technology neutral’ legal

principles for the protection of privacy when processing personal data for all electronic communications (Ackerman *et al.*, 2003). Article 9 of the directive concerning location data requires unequivocal opt-in consent for the use of a customer's location data:

Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

(European Commission, 2002b)

A Finnish survey respondent reconfirmed this by stating that “EU regulation is formulated to give the end user the right to decide whether his location information is available, to whom it is available and even more he has to have control transaction by transaction.” In addition to granting opt-in consent for the use of location data, Article 9 of Directive 2002/58/EC also grants customers the right, free of charge, to withdraw consent for the collection and use of location data at any time (European Commission, 2002b). This was acknowledged by one survey respondent who wrote, “I am allowed to check what information has been recorded about me. I can forbid the use of my personal information for marketing purposes.” Article 10 of the directive also gives power to EU member countries in deciding how to obtain or withdraw consent from consumers for the use of location information (European Commission, 2002b).

Directive 2002/58/EC has replaced **Directive 97/66/EC**, created in 1997 (European Parliament, 2001). The 2002 Directive has updated terminology, extended rules of protection applying to surveillance, confidentiality, direct marketing, etc. to include electronic communications, and accepted the opt-in system for “unsolicited direct marketing messages sent by electronic mail, faxes and automated calling machines” (European Parliament, 2001). Directive 2002/58/EC works in tandem with **Directive 2000/31/EC**, the **Directive on Electronic Commerce**, which requires commercial communications, i.e. advertisements, to be clearly identified as promotional messages

(European Commission, 2000b). The 2002 Directive was supposed to be implemented by all member countries by the 31st of October, 2003, but as of November 2003, only Denmark, Finland, Spain, and Sweden have signed it into law (Ackerman *et al.*, 2003).

The EU **Directive 95/46/EC** is the **Personal Data Protection Directive** and concerns the processing of personal data. Personal data is defined as any information that is used to identify a person, including his “physical, physiological, mental, economic, cultural or social identity” (European Commission, 1995). Processing of personal data concerns operations performed upon personal data “such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, [or] erasure” (European Commission, 1995). In relation to the citizen, “personal data may be processed only if the data subject has unambiguously given his consent” (European Commission, 1995). Articles 10 and 11 of the Directive state that the data subject must know who is collecting the data and the purposes for which the data is being processed (European Commission, 1995). According to Articles 12 and 14 of the Directive, the data subject must be able to easily object and prevent the use of data in direct marketing (European Commission, 1995).

Discussion of data retention within Directive 95/46/EC also clearly proclaims that private information must be safeguarded and may not be held for longer than is necessary or without good reason (BBC, 2002, 2003a; Divis, 1999). For example, data concerning telecommunication exchanges are kept only as long as needed for bill generation (BBC, 2002). The 1995 directive states that personal data must be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed” (European Commission, 1995). In addition data must be “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed” (European Commission, 1995). European companies cannot, therefore, demand personal information about an individual person for a service or product. These requirements sharply contrast with US industry’s practice of self-regulation.

A dispute in January 2003 underscored these privacy differences between the EU and the US computer firm, Microsoft. Microsoft requires users to supply personal information, such as name, address, etc. when accessing their Passport³ system online (BBC, 2003a). To be in accordance with European data laws when using Passport, EU citizens must only be required to designate themselves as EU citizens and subsequently decide for themselves how much additional information they wish to share (BBC, 2003a). Microsoft has agreed to make significant adjustments to the system, which are due to take effect by the middle of 2004 (BBC, 2003a). A similar, more recent example is found regarding preservation of EU airline passenger data by the US Department of Homeland Security due to post-September-11 security precautions. The US has demanded that personal details of EU passengers be given at check-in for all flights to the US, while the EU parliament protested over the loss of privacy (BBC, 2003c). A compromise has been made and the US is allowed to retain the data for 3.5 years, while there are certain restrictions as to who has access to the data (BBC, 2003c).

In terms of receiving information, such as direct marketing of unsolicited communications, EU directives also clearly dictate what is and is not allowed. Article 13 of **Directive 2002/58/EC** states that unsolicited communications for use in direct marketing, in cases other than marketing similar products to which the person has already agreed to and has the opportunity to opt-out, “are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation” (European Commission, 2002b). The widely adopted system in the EU in which consumers opt-in to a privacy policy, automatically gives privacy protection unless specified otherwise by the consumer (Bagby, 2003, p 461; Fox *et al.*, 2000, p 6). This gives EU citizens unambiguous control over what aspects of their personal data is collected.

³ This system allows users to sign up once and utilize the same password to access services online by various businesses.

German Privacy Laws

As an EU member country, Germany must comply with all EU directives. After being taken to court by the European Commission in 2000 due to a failure to implement EU Directive 95/48/EC (European Commission, 2000a), the German government in 2001 and 2002 adopted larger amendments to its Federal Data Protection Act and implemented the Directive (Bundesbeauftragten für den Datenschutz, 2004a). However, well before the formation of the EU, Germany had strict laws concerning the privacy of personal information of its citizens. The tight German restrictions regarding private information was identified by one US survey respondent. In addition, Germany's privacy regulations were also acknowledged by all four German survey respondents.

Germany's original privacy protection regulations appeared in the German Constitution, created in 1949. The Constitution of the Federal Republic of Germany contains the *Grundgesetz*, or Basic Law, which protects every German citizen's right to privacy. Article 10 of the Basic Law states that citizen's have the unfringeable right to privacy of letters, posts, and telecommunications (Deutscher Bundestag, 1949). These laws were created after the Second World War in order to avert an "all-knowing totalitarian state from ever emerging again" (German Embassy, 2003).

Since 1970, data protection has also been established in relevant rulings enacted in German states, or *Länder* (European Foundation, 2004c). In addition, Germany passed the Federal Data Protection Act, or *Bundesdatenschutzgesetz*, in 1978, amended in 1990, which applies to both public and private sector organizations (Bundesbeauftragten für den Datenschutz, 2004b). The specific mention of data protection, or *Datenschutz*, protects individuals from the consequences of any form of processing, specifically computer processing, of personal data, and safeguards the right of self-determination over personal data, explained below (Bundesbeauftragten für den Datenschutz, 2004b; European Foundation, 2004c; Interviewee-1, 2003). It is also stated in the Act that the German Federal Data Protection Commissioner is required to keep records of computerized databases containing personal information (Bundesbeauftragten für den Datenschutz, 2004b). Being the principal privacy protection regulation for Germans, the *Datenschutzgesetz* was specifically mentioned by two of the four German survey respondents.

The German government, specifically the court system, has taken these privacy practices one step further and placed additional safeguards on the authorized use of personal information (Walton, 2002; White, 1997, p 232-33). In 1983 the Federal Constitutional Court established the concept of ‘information self-regulation’ (European Foundation, 2004c). This concept ensures individuals “the freedom to decide for themselves whether data concerning their person may be disseminated” (European Foundation, 2004c). The idea formed when the government recognized that more and more electronic data was being distributed (European Foundation, 2004c). Because of this trend, the German Court “guaranteed every individual the right of self-determination over the disclosure and use of data concerning their person” (European Foundation, 2004c). This right is however subject to justifiable interests of the state or third parties, if for example, there is a criminal investigation data may be stored without awareness or consent of the individual (European Foundation, 2004c).

Conclusion

The regulations set forth by US, EU, and German governments clearly emanate from different perspectives concerning governmental regulation, self-regulation, and a citizen’s right to privacy. US and European regulations and methods of data collection and privacy protection are in stark contrast to one another. The US allows for self-regulation in the private sector and allows industries to utilize either an opt-in or opt-out system regarding personal data processing. In the absence of clear-cut guidelines for industry conduct, industry associations and technology interest groups have attempted to provide some stability. In the EU and Germany, however, the opposite is true. They have explicitly adopted the opt-in policy allowing individuals to decide for themselves whether they want their personal information used for direct marketing or other services. Private information is protected and EU citizens are given explicit rights to personal privacy. Germany has taken extended EU directives by bestowing on its citizens the right to self-regulation over their own personal data.

These distinct privacy protection strategies of the US and EU have direct consequences for the diffusion and adoption of retail LBS. Survey responses regarding

this matter were in agreement – seven of 15 US respondents and well over half (eight of 11) of EU survey respondents claimed that governmental policies concerning information privacy would affect retail LBS growth. Retail LBS is undeniably a non-neutral technology. It creates serious concerns of privacy protection, especially as it relates to the potential tracking and surveillance of individuals, in addition to the potential for unwanted direct marketing. Privacy, as a dimension of the distinct societal contexts of the US and Germany, will therefore have an explicit effect on the diffusion and adoption, of retail LBS.