Article No 2

Location-Based Communication Systems
A Look at Intelligent Networking and Privacy Concerns

Laurie Thomas Lee, Ph.D.
College of Journalism and Mass Communications
University of Nebraska-Lincoln

Keywords
Location-based systems, intelligent networking, privacy, mobile phones

Abstract
Location-based networks are quickly becoming an integral feature of today's intelligent networking landscape. They are transforming how people and government communicate. Global positioning satellite systems, Wi-Fi, and other such decentralized networks make it possible to track and physically locate users and pair that information with location-based information from and about others, such as friends, products, and services. This paper examines the nature of location-based systems in the context of intelligent networking, where various technologies, pathways, and information repositories operate in a decentralized environment for the purpose of providing location-specific communication and information. Different types of technologies, routes, and databases are described and discussed. Privacy issues are of particular concern, given that the advanced features of an intelligent network make it easy and economically compelling to track individual locations without the person's knowledge or consent. Other problems include the ability to invade privacy in a manner that is continuous, global, and permanent.

Introduction
Location-based networks are quickly becoming an integral feature of today's intelligent networking landscape. They are transforming how people and government communicate. Global positioning satellite systems, Wi-Fi, and other such decentralized networks make it possible to track and physically locate users and pair that information with location-based information from and about others, such as friends, products, and services. Users with smartphones, for example, can access local maps, check out nearby restaurant specials, notify friends as to their whereabouts, find others, and get information on local traffic alerts, events and landmarks, all by accessing the various types of networking systems and applications that rely on location tracking.

Location-based systems present considerable economic efficiencies and other advantages. Researchers predict phenomenal growth for the "geolocation" business, with revenues topping $4 billion by 2015 (With Location-Tracking, 2010). Yet this type of intelligent networking also poses serious security and privacy concerns, as location may be easily tracked and disclosed without knowledge or permission and with economic and other consequences.

This paper examines the nature of location-based systems in the context of intelligent networking, where various technologies, pathways, and information repositories operate in a decentralized environment for the purpose of providing location-specific communication and information. These different types of technologies, routes, and databases are described and distinguished as they pertain to location-based networking. The various types of users involved

are also identified because of their contributions to the intelligence of location-based networks. Finally, because intelligent networks by their nature present both advantages and disadvantages, the opportunities of location-based networks as well as specific problems such as location privacy violations are discussed.

LOCATION-BASED NETWORKS AS AN INTELLIGENT NETWORK

Location-based networks constitute an example of an intelligent network, which is essentially a series of networks designed to enhance the communication of its users on a local or global scale (Noam, 2001). An intelligent network is capable of organizing, transmitting, and displaying information for strategic purposes (Gershon, 2011). In this case, location-based networks are capable of tracking and communicating the whereabouts of a user to other users across different and complex networks and platforms in an instant. Decision-making capability and analysis are also a part of location-based networks, whereby intelligence is added by the contributions and actions of the various users on the networks. As with organizational intelligence (Liebowitz, 2000), knowledge is created and strategically used for a benefit, such as improved organizational performance.

The Technology

Networking intelligence is readily apparent in the architecture of location-based networks. A complex array of networks is used to track, record, store, re-transmit and display location information. The information pathways and routing techniques vary across platforms, as well as the storage systems and the types of terminals involved, such as consumer cell phone handsets and business computers. Automated intelligence is demonstrated by the ability to monitor a user's position, process that location information, and determine how the information is shared and with whom.

Transmission Technologies.

Location technologies include cellular identification, GPS, wireless positioning, and IP identification (Tsai et al, 2010). Some services use several technologies, such as Loopt, which partners with cellular carrier AT&T (Tsai et al, 2010). Cellular telephone technologies are obviously involved in much—although not all—of the tracking and transmission of location data, using a combination of GPS and cell tower triangulation techniques. Cell phone carriers do so because of the Federal Communication Commission's Enhanced 911 (E911) regulations that required carriers to provide precise location information by 2003 and a fully implemented wireless call location system in place by 2006 (In the Matter, 2002). Although carriers already kept track of cell site location information for purposes of billing and assessing roaming charges, the E911 requirements called for more detailed information. At the time, carriers were to select either a handset-based technology or a network-based technology for this automatic location information (Lee, 2003). Today, wireless carriers using CDMA networks, such as Verizon Wireless and Sprint Nextel, tend to use embedded GPS technology. AT&T and T-Mobile comply with the E911 regulations by using network-based technology that computes a phone's location using signal analysis and triangulation between towers (McCullagh, 2011).

The tracking of mobile phones is then relatively simple. Whenever a cell phone is turned on and any time it moves around—whether it is actually making or receiving a call—the wireless provider tracks the current base station with which the phone is associated, checking in every seven seconds or so ("ECPA Reform, 2010; Cohen, 2011). It determines the nearest tower so as to most efficiently route calls. A cell tower knows the general direction of a mobile phone because many cell sites have three antennas pointing in different directions. If the phone is "talking" to multiple towers, triangulation yields a rough location fix, the accuracy depending in

part on the density of the cell sites. The FCC's E911 rules then allow carriers to transform these rough estimates into precise coordinates (McCullagh, 2011a).

Cellphone companies then record, for billing purposes, where a call is coming from and how long it lasts (Cohen, 2011). The records of what tower is in use when a call is initiated or answered are generally stored for six months to a year, depending on the company (McCullagh, 2011a). Providers reportedly tend not to retain moment-by-moment logs of when each device contacts a tower, in part because there is no business reason to store the data and because of storage costs (McCullagh, 2011a).

The most prominent location tracking technology that is visible to the end user is GPS, which makes use of the global positioning system satellites that allow a device with a satellite receiver and a view of the open sky to calculate its location based on latitude and longitude. GPS has much higher accuracy, with equipment available now that can locate a device within about 10 meters of accuracy or less ("ECPA Reform," 2010). With GPS, this is done by a device and with no other infrastructure than the ability to receive satellite signals. The latest generation of cell phones has a separate GPS receiver and some mapping software and other tracking software ("ECPA Reform," 2010).

Wireless positioning is another common technology used in this intelligent network, relying on personal and public Wi-Fi access points that can map users according to their location relative to the access points (Tsai et al, 2010). This works through the process of "war-driving" access points and mapping each to a GPS location. Then companies such as Skyhook Wireless create large databases with fairly high location accuracy (Tsai et al, 2010). The locations are not always as precise as GPS, but the capabilities are great given the increasing and widespread use of Wi-Fi. Wi-Fi hotspot triangulation is a commonly used method of determining location on smart phones as GPS may not always work in urban locations, and cell-tower positioning can be inaccurate (Krazit, 2010).

Another means of locating a user's device is by an IP address. When devices are connected to the Internet, the associated IP address may be associated geographically to the extent that a user may be mapped to a particular city. This limited use makes IP location tracking mostly a fallback when other means are unavailable (Tsai et al, 2010).

Database Storage Systems.

Another important component of an intelligent network is the ability to organize, process, and store the data. Here, there are several platforms that may be used to pull, process, and save location information across the intelligent network. One method involves user-installed software that collects and then stores the location information in a database or sends it to the location-sharing application either automatically (i.e., a ping every five minutes) or when "pushed" by the user (Tsai et al, 2010). Web browsers with location-finding plug-ins may also be used. Another option is for third party apps to simply work through existing providers and their databases (Tsai et al, 2010).

There are even cloud-based geospatial databases available to location app developers. SimpleGeo Storage is an example of an on-demand database available for web, Android, iOS, and Windows Mobile 7 platforms (Grove, 2011). Developers can use the storage site to store real-world data and access the database from any mobile device or server via an HTTP API. The database can support longitude/latitude, IP address, or physical street address queries.

Many handset devices themselves also collect and store location information that is ultimately transmitted to a third party (see, e.g., Lowensohn & Mills, 2011). A pair of researchers recently found that Apple collects location information in its iOS products that carry a 3G antenna and stores the information in a database file called "consolidated db." The information contains longitude, latitude, and time stamp information that are stored on the phone, but due to the iOS

device backup system in iTunes, will also end up on one's computer when synced. The log information can also extend across multiple devices as long as those devices use the same restore point. Apple then receives the data every 12 hours when a user is connected to a Wi-Fi network (Lowensohn & Mills, 2011). The result is a large, anonymized crowd-sourced database of Wi-Fi hotspots and cell towers that surrounded an iPhone (Lowensohn & Mills, 2011).

Like iOS devices, Android phones collect location information in a local file, although the information is reportedly erased relatively quickly. The Android phones regularly connect to Google.com and unload a miniature data dump that includes time down to the millisecond, current and recent GPS coordinates, nearby Wi-Fi network addresses, and two 16-letter strings representing the unique device ID (McCullagh, 2011b). Windows Phone 7, supported by manufacturers including Dell, HTC LG, Nokia, and Samsung, does not store the data on the device in a local file like the iPhone (Lowensohn & Mills, 2011), but it nonetheless transmits to Microsoft a miniature data dump that includes a unique device ID, details about nearby Wi-Fi networks, and the phone's GPS-derived latitude and longitude (McCullagh, 2011b).

The Users

Location-based systems also owe their networking intelligence to the different users on the system who request or provide the geopositioning data as well as related location-specific information. These users, including providers, contribute to the intelligent network by analyzing and making decisions as to what is shared, when, how, and to whom, using the software and hardware features of the system. Location-based networks provide users with added value, and this value, as well as the power of the networks, is increased as more users utilize them.

Location-based networks allow, for example, user queries based on the nearest neighbor, developer-defined geographical region, and radial location. They also provide a wealth of information to users (and providers) to spur further decision-making and subsequent analysis. An example of this would be a user, such as an advertising record label, that uses a database like SimpleGeo to record transactions and chooses to analyze trends around how, where and why people buy music (Grove, 2011).

Many players are involved in the decision-making and analysis of location data. At one level, manufacturers of handsets devices such as the Palm Pre are capable of secretly and routinely sending GPS location information to their respective carriers (FTC Roundtable 2010). Location-based apps are major players at the software level as they create and promote their features and choose to gain access to the specific devices, collecting and storing not only location data but other user information. Cell phone carriers and others involved in the transmission process possess detailed billing information and system information that can track subscribers, plus may know what apps are downloaded if they are providing the billing (FTC Roundtable 2010). Websites are lesser-known participants but nonetheless have the potential to gain access to mobile location information more easily now, thanks to standardization in the way websites can ask web browsers for location information (FTC Roundtable 2010). And of course consumers themselves may be engaged in making decisions as to which location apps to download and activate, what location information and other data to provide, and when and with whom (including which social media outlets) the data is disclosed and given permission to share.

The types of decisions made and analyses employed range considerably, depending on the application. The best known location apps and web services include foursquare, Google Latitude, Gowalla, Shopkick and Facebook Places (Miller & Wortman, 2010). These apps essentially let users report their physical location online in order to connect with friends or receive certain benefits such as coupons. Some services rely on location information, such as Google Maps, and other services only link to or make use of location information, such as Twitter. Services may be text-based or map-based (i.e., showing where a user is located), and are now more frequently automated (Tsai et al, 2010).

In just a matter of months, the number of location-based apps has grown exponentially while the power of these apps and their networks has also increased, quickly adapting to the demands of users (Etherington, 2011). This tendency to change and adapt is characteristic of an intelligent network (Monge et. al., 2008). Some apps. now require considerable network intelligence as they incorporate greater levels of interactivity. For instance, location-based gaming is emerging and considered by some to be the next killer app (Steen, 2011). One example is a popular Finnish iPhone game called "Shadow Cities" that recently debuted in the United States and allows players to roam their neighborhoods casting spells and taking over city blocks while engaging others by teaming up or fighting over territory. Even the popular "Angry Birds" is expected to include location-based features so that players can compete with one another on a unique leader board tied to specific locations, such as bars and coffee shops (Steen, 2011). "My Town" is another example of a location-based game where players buy and sell locations they check in at, much like Monopoly, and products are integrated through barcode scanning to unlock virtual goods and manufacturer promotions (Steen, 2011).

A new wave of location-based apps adds intelligent assistance features, possibly marking a paradigm shift in how such networked services are used by consumers (Gross, 2011). For example, an app called "Alfred" allows users to feed information about their favorite places while a mustached robot butler provides suggestions for similar spots nearby. The app uses a Web-crawling algorithm to pull information together while recognizing the difference between positive and negative chatter about a place (Gross, 2011). It essentially works as an assistant or chaperone in seeking and figuring out what matters to a user while using location information.

BENEFITS OF LOCATION-BASED NETWORKS

What advantages does the intelligence of location-based networking provide to the marketplace? How are businesses, government, and consumers helped by the tracking and sharing of location data and related information?

As with intelligent networks in general, the opportunities presented by location-based networks are phenomenal. Some prime benefits of intelligent networks are the ability to evolve and improve existing services, introduce new services rapidly, provide service customization, create open interfaces and vendor independence, and develop new sources of revenue (IEC, 2011). Indeed, the inherent decentralization of location-based networks provides users (and providers) with the means to control and develop new features and uses that may be customized to meet consumer needs and interests as they evolve. These new capabilities can also be more efficiently and rapidly introduced into a location-based intelligent network and made competitive in the marketplace.

One overall benefit of intelligent networks is the ability to enhance the evolution and development of new services for users (WiFiNotes.com). Location-based networks, while relatively new, have certainly grown and demonstrated the ability to adapt. Changes have been made to the system at all levels, in fact, from how handset devices record GPS information, to how cellular telephone signals are transmitted, to the speed at which Wi-Fi systems operate, and to how software applications assess location data and add value. Along this same line is the ability of intelligent networks to launch new services rapidly (IEC, 2011). As mentioned, the number of location-based apps has exploded, with most introduced within the last year or two as smart phone adoption has taken off.

Intelligent networks are also capable of hosting a range of complex features and enhanced services. They create the means for service customization, with service providers being able to change the service logic rapidly and efficiently, and customers getting their demands met for control of their services (IEC, 2011). With location-based networks, the result has been a wealth

of increasingly sophisticated location apps that have been customized for specific social media, advertisers, and businesses. These range from friend-finding services like foursquare and Facebook Places, to travel games like Gowalla (Lowensohn, 2010) and commercial services like Shopkick (Miller & Wortman, 2010). Some new services, like Trover and Crowdbeacon, are geared to place-based discovery and interactivity, with again more intelligent assistance features becoming incorporated (Gross, 2011).

Another overall benefit of intelligent networks is the ability to increase market competition by producing or arranging these new services (WiFiNotes.com). Network intelligence helps to create competition in the business of supplying the network infrastructure, where network operators, service providers, and consumers are not locked in to specific choices (ITU, 1995). Vendor independence is an important advantage, where software can be inexpensively developed and easily interfaced with other vendors' products, thanks to another benefit of intelligent networks--open interfaces (IEC, 2011). The service logic is also under the provider's control, making it easier to create services in a cost-effective manner (IEC, 2011). Indeed, with location-based networks, developers are able to create new services in part because they can access the many commonly used consumer services that track location data. Better manageability also occurs with intelligent systems, where a modular environment along with some standards enables operators to manage services responsibly, reducing costs and improving customer service (ITU, 1995).

Location-based networks certainly promote these benefits to network operators, service providers, and consumers alike, as they are decentralized, relatively open, and economical. The geolocation industry can boast that it is competitive, funded, and well-positioned to succeed, with tech companies building the platforms, marketers eager to develop advertising, and venture capitalists providing the cash (Brustein, 2010). With much of the infrastructure in place, development costs are low and services can be created at relatively little cost, while consumers enjoy a vast selection of apps that are often free to download. Companies like foursquare and Gowalla have had no trouble raising money from investors (Brustein, 2010). In fact, the National Venture Capital Association says venture capitalists poured $115 million into location start-ups by 2010 (Miller & Wortman, 2010). Advertisers are also on track to spend $1.8 billion on location-based marketing in 2015, according to ABI Research, a technology market research firm. Location based advertising, or LBA, is in big demand, with ads tied to location being much more lucrative than other ads (Helft, 2011). Not only are ads pushed directly to consumers at a site, but location information can be valuable in other ways. For example, a retailer with eight outlets in a city might use data about walking patterns to determine where to open its next outlet (Helft, 2011).

PROBLEMS WITH LOCATION-BASED NETWORKS

While location-based networks have seemingly endless advantages, there are also some disadvantages inherent to intelligent networks. By definition, intelligent networks have permeable boundaries which allow information to flow in and out of the system. Permeability is an important feature because it allows network providers to easily introduce new software and hardware, developers to create new services for the network, and users to easily access the network. Unfortunately, this also creates a "permeability predicament," whereby an open system allows for a number of unwanted influences and outcomes that can affect network design and critical infrastructure (Gershon, 2011). In the case of location-based systems, the unintended consequences of intelligent networking include issues associated with 1) network control, 2) security, and 3) privacy.

Network Control Issues

Because the intelligent network is the ultimate distributed system, there is no single point of failure and therefore its function to remain constantly available is historically met (ITU, 1995). Nonetheless, the immense size and complexity of the distributed controlling software can

effectively ignite small fires across a broadly networked landscape. Telecommunication carrier outages can and do occur, satellite communications often face disruption, and Internet Service Providers constantly grapple with congestion. Acts of terrorism, computer hacking, and denials of service are also clearly possible with intelligent networks. Because of reliability issues, service providers are sometimes forced to turn to nonintelligent networks to maintain some level of service (WiFiNotes). These problems could certainly affect location-based networks. Users relying on location-based information may, for example, lose GPS mapping ability while traveling, fail to load location-specific weather reports during stormy weather, and miss important business and social meetings.

Network Security Risks

Because users are able to access and participate in the distributed and relatively open network, breaches in the network may be exploited. What is otherwise an advantage of the open system can become a disadvantage, depending on the vulnerability and oversight at the various gateway points. Apple's apps, for example, are available and carefully controlled through their App Store, and Apple will scrutinize and reject apps that developers create (Raphael, 2009). Yet as noted earlier, Apple and other handset devices themselves were recently identified as storing location data in a "consolidated db" database file that ends up on the handset owner's computer when synced. The researchers showed how this information is accessible to anyone with access to a synced computer and demonstrated how the data might be used by creating an iPhone tracker as an open-source app that produces a map of the phone's physical movements. Indeed, if users "jailbreak" their smart phones by installing apps not approved by Apple and therefore undermine the built-in protections, there is a chance some malicious app could copy location data from the unencrypted consolidated db and transmit it to someone else. Although precise locations are not produced by the data, the information may nonetheless be of interest to not only hackers, but a thief, a jealous lover, a tenacious advertiser, an attorney with a subpoena, and police ("Those Snoopy," 2011).

Privacy Concerns

These network security risks further point to larger consumer privacy concerns. Intelligent networks by their very nature help facilitate privacy invasions. The enhanced features make it easy and economical to capture and distribute location data without consumer knowledge or consent. Location-based networks are also worldwide, sharing what may be private with virtually anyone. In addition, the tracking can be continuous, meaning that the location data is complete with no down time for privacy—even if the transmitting device is turned off. The ability of the intelligent network to consolidate and store data also means that location data may never be deleted, potentially encroaching on privacy interests well into the future.

The economic and management advantages presented by location-based networks turn into disadvantages when they invite misuse and abuse of the system, leading to privacy invasions. On the one hand, government access to and interest in location information has become unsettling. For example, in 2009, Sprint indicated that it received a shocking number of requests from law enforcement for GPS location data revealing the location and movements of Sprint's customers (Bankston, 2009). The requests did not include legal requests from civil litigants or foreign intelligence investigators, or even the less-precise location data based on cell phone towers. There are concerns that the government might use such information to keep track of what political meetings people attend. In Germany, for example, one party candidate discovered that Deutsche Telekom had recorded and saved his longitude and latitude coordinates more than 35,000 times over a six-month period (Cohen, 2011). Profiling can also take place as computer algorithms assessing behaviors kick in and red flags go off.

Businesses including advertisers may also use location data for less noble purposes, spurred on by competition and marketplace demand. For example, employers might check on employees to see what they are doing when on break or vacation. Location data might also be merged with

other data to profile potential clients and customers. Insurance companies, for example, may find useful information that could be used to raise premiums or deny coverage (Blumberg & Eckersley, 2009).

On the one hand, there are information privacy concerns as consumers fear a loss of control over what they sometimes see as personal information. Information that should be secured may be sold without permission, leaked or hacked. On the other hand, there are concerns about privacy intrusion when unsolicited advertising is pushed like spam. Google and Apple use location data not only to improve the accuracy of their navigation and other location-based services, but to help push advertising aimed at people who may or may not have consented. Opt-in and opt-out are options that an intelligent network can provide, but such options are not always made available.

Even misuse of the data by private individuals is a real concern. Stalking is easily facilitated. Criminals can more easily burglarize a home when they know home-owners are away ("Location-Tracking," 2010). Pedophiles can more readily locate and track targeted victims. One example that highlights the privacy risks is a geolocation aggregator called "Creepy," which is a free application that allows anyone to gather data from social networking platforms and image hosting services, such as Twitter and Flickr, and have it presented on a map with longitude and latitude coordinates. Essentially, users may be able to track the location of anyone who tweets from a mobile device (Delman, 2011).

Thus, while location-based networks promise a world of opportunities, they also pose considerable concerns as location information may be collected pervasively, silently, and cheaply (Blumberg & Eckersley, 2009). Ubiquitous devices and applications are readily available to many parties who can query it, buy it, subpoena it, or steal it. Many consumers do not know that their location is being tracked when using the features of their mobile devices. And even when consumers have intentionally downloaded a location app or service that prompts them for permission, they remain largely unaware of how their location data is being collected, forwarded and used, and they are unaware of how to check and correct inaccuracies. An intelligent network alone does not guarantee that intelligent security and privacy protections will be provided.

CONCLUSION

Location-based networks are an example of the modern intelligent network, comprised of a series of networks created to enhance the communication of its users on a worldwide scale. Characteristics of an intelligent network are easily found in location-based systems where a complex collection of decentralized networks with various information pathways and routing techniques are used across a number of different platforms. Indeed, cellular telephone, Wi-Fi, GPS, and other means of transmission and distribution are employed and interconnected. Automated intelligence is a demonstrated feature of the location-based network. Networking intelligence is also found in the compilation and storage of location data. And like other intelligent networks, location-based networks attribute some of their networking intelligence to the various users who seek and contribute the geopositioning data and other location-related information.

There are many advantages of intelligent networks that are equally found in location-based systems. These include the ability to evolve and improve existing services, introduce new services rapidly, and provide service customization. Such networks also possess the ability to increase market competition with open interfaces, vendor independence, and manageability. Location-based networks exhibit these qualities as they are able to introduce new, enhanced, and customized services rapidly and efficiently. One benefit is the wealth of increasingly sophisticated location apps that have been introduced, customized for specific social media, advertisers, and businesses and meeting the demands of consumers.

For the same matter, location-based networks suffer from disadvantages because of and in spite of their networking intelligence. Issues associated with network control, security, and privacy may plague location-based communications systems. The size and complexity of a distributed system can result in network failures, and the open access feature of the intelligent network can lead to security threats and network breaches. Privacy issues are of a particular concern, given that the advanced features of an intelligent network make it easier and economically compelling to track individual locations without knowledge or consent. Other problems include the ability to invade privacy in a manner that is continuous, global, and permanent.

Despite these concerns, location-based networks have grown in prominence, becoming an important part of the telecommunications landscape that continues to interconnect users across the globe with creative and useful location-based services. Network providers and users are not likely to refrain from taking advantage of such an intelligent system with opportunities for services and revenues not yet realized. Like intelligent networks, location-based networks are growing, evolving and adapting to changes in technology and consumer demand. The geolocation business is booming, and interactive gaming and the recent addition of intelligent assistance should make this truly intelligent network interesting to track.

References

Bankston, Kevin (2009, December 1). "Surveillance Shocker: Sprint Received 8 MILLION Law Enforcement Requests for GPS Location Data in the Past Year," retrieved at http://www.eff.org/related/8459/blog.

Blumberg, Andrew and Eckersley, Peter (2009). "On Locational Privacy, and How to Avoid Losing it Forever," White Paper, Electronic Frontier Foundation, retrieved at http://www.eff.org/wp/locational-privacy.

Brustein, Joshua (2010, November 6). "Tag-Along Marketing," NYTIMES Online.

Cohen, Noam (2011, March 26). "It's Tracking Your Every Move and You May Not Even Know," NYTIMES Online.

Delman, Mark (2011, May 9). "New Application Illustrates Privacy Risks of Location-Based Applications," retrieved at http://www.markdelman.com/2011/05/location-data-privacy-risks.html

ECPA Reform and the Revolution in Location Based Technologies and Services Hearing, Before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Committee on the Judiciary House of Representatives, One Hundred Eleventh Congress, 2nd Sess., June 24, 2010.

Etherington, Darrell (2011, April 8). "How Location Sharing Went From Crazy to Compulsory in Just 2 Years," retrieved at http://gigaom.com/mobile/location-sharing-goes-from-crazy-to-compulsory-in-just-2-years/

FTC (Federal Trade Commission) (January 28, 2010). "Privacy Implications of Mobile Computing," Second Roundable on Exploring Privacy, Panel 4, pp. 238-297, available at http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.pdf

Gershon, R.A. (July 2011). "Redefining Business Space: Intelligent Networking and the Transnational Corporation," The 2011 International Association for Media & Communication Research (IAMCR) Conference, Istanbul, Turkey.

Gross, Doug (2011, July 29). "New Wave of Location-Based Apps Mark a 'Paradigm Shift,'" CNN.com, retrieved at http://articles.cnn.com/2011-07-29/tech/discovery.apps_1_android-free-app-hipstamatic/2?_s=PM:TECH

Grove, Jennifer (2011, March 28). "SimpleGeo Releases Database for Location-Based App Makers," Mashable, retrieved at http://mashable.com/2011/03/28/simplegeo-storage/

Helft, Miguel (2011, April 25). "Apple and Google Use Phone Data to Map the World," The New York Times (online), available at: http://www.nytimes.com/2011/04/26/technology/26locate.html

International Engineering Consortium (2011). "The Intelligent Network (IN)," Available at http://www.iec.org, retrieved at http://www.cs.utexas.edu/users/vin/Classes/CS386M-Fall04/Readings/AIN_overview.pdf

In the Matter of Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, Order to Stay, Fed. Comm. Comm'n, CC Docket No. 94-102, July 26, 2002.

International Telecommunications Union (1995). "Intelligent Networks," Available at: http://www.itu.int/TELECOM/wt95/pressdocs/ft-03-e.html

Krazit, Tom (2010, June 29). "Google Mobile Apps Collect Wi-Fi Location Data," CNET, available at HTTP://NEWS.CNET.COM/8301-30684_3-20009223-265.HTML?TAG=MNCOL

Lee, Laurie Thomas (2003). "Can Police Track Your Wireless Calls? Call Location Information and Privacy Law," 21 *Cardozo Arts & Entertainment Law Journal*, 381-406.

Liebowitz, Jay (2000). *Building Organizational Intelligence: A Knowledge Management Primer*, Vol. 1, Boca Raton, FL: CRC Press LLC.

Lowensohn, Josh (2010, August 18). "Facebook Unveils Location-Sharing Feature 'Places,'" http://news.cnet.com/8301-27076_3-20014068-248.html#ixzz1NsMHTt1a

McCullagh, Declan (2011a, March 22). "Senator Pushes for Mobile Privacy Reform," http://news.cnet.com/8301-31921_3-20045723-281.html

McCullagh, Declan (2011b, April 25). "Microsoft Collects Locations of Windows Phone Users," http://news.cnet.comm/8301-31921_3-20057329-281.HTML?TAG=MNCOL;TXT

Miller, Claire and Wortham, Jenna (2010, August 29). "Technology Aside, Most People Still Decline to be Located," NYTIMES Online.

Monge, Peter., Heiss, Bettina, & Margolin, Drew (2008). "Communication Network Evolution in Organizational Communities," 18(4) *Communication Theory*, 449-477.

Noam, Eli (2001). *Interconnecting the Network of Networks.* Cambridge, MA: MIT Press.

Raphael, J.R. (2009, February 22). "Rejected! 10 iPhone Apps That Didn't Make Apple's App Store," PC World, retrieved at http://www.pcworld.com/article/159887-2/rejected_10_iphone_apps_that_didnt_make_apples_app_store.html

Steen, Greg (2011, July 24). "Why Location-Based Gaming is the Next Killer App [Opinion]," Mashable, retrieved at http://mashable.com/2011/07/24/location-based-gaming/

"Those Snoopy iPhones"(Editorial), 2011, April 23, LA Times.com, retrieved at latimes.com/news/opinion/opinionla/la-ed-iphone-20110423,0,1609775.story

Tsai, Janice; Kelley, Patrick; Cranor, Lorrie, and Sadeh, Norman (2010). "Location-Sharing Technologies: Privacy Risks and Controls," 6 *Journal of Law & Policy for the Information Society,* 119-151.

WiFiNotes. "What are Intelligent Networks?" Available at: http://www.wifinotes.com/computer-networks/what-are-intelligent-networks.html

"With Location-Tracking Technology, Cell Users Paying Price of Privacy," 2010, June 22, retrieved at http://www.pbs.org/newshour/bb/science/jan-june10/cell_06-22.html.

About The Author

Laurie Thomas Lee, Ph.D., (Michigan State University) is a professor in the College of Journalism and Mass Communications at the University of Nebraska-Lincoln. Her research interests are in media law and media economics, particularly in the areas of privacy and new technologies.