1-1-2011

Issues in the Development of Location Privacy Theory

Robert Minch
Boise State University

Issues in the Development of Location Privacy Theory

Robert Minch
Boise State University
rminch@boisestate.edu

Abstract

Issues in the development of location privacy theory are identified and organized based on both technological considerations and more general privacy theories. Three broad categories containing six issues are described: location (including sensing methods and location properties), privacy (including definition and subject identification), and information flows (from location information acquisition through storage, use, and sharing). An influence diagram model is presented which relates these issues in context and may serve as a basis for further theory development, empirical research, and public policy discussion.

1. Introduction

It is now commonplace for a person's location to be sensed and recorded via surveillance cameras, RFID (Radio-Frequency Identification) tags, location-aware cellular telephones, and other technologies. Market penetration of mobile devices, most now location-enabled, is out-pacing non-mobile technologies. These trends will increase the likelihood that a user may be located and tracked countless times during a lifetime, raising significant privacy issues.

Location privacy as a distinct subset of general privacy has been recognized, particularly in the context of modern location-sensing technologies, for some 15 years (e.g. [1]). As a simple indication of increasing research interest in the area, Google Scholar searches for "location privacy" report less than 10 works before 1995, approximately 800 between 1995 and 2005 inclusive, and approximately 2500 from 2006 through August 2010.[1]

While theory development for privacy in general has been active (e.g., [2] [3] [4] [5]), theory specifically addressing location privacy is called for but has been slower to emerge. Palen and Dourish [6] state: "We recognize when our systems introduce 'privacy issues,' but we have few tools for understanding exactly what those issues are." (p. 129). As noted in [7], "Thirteen privacy issues related to the collection, retention, use, and disclose [sic] of location information and technologies [8] provide a full spectrum of understanding of location privacy. The privacy issues could be used as a foundation to build up a theory of LBS (Location-Based Services) privacy as part of a general theory of privacy in the information age [4]." It is the aim of the current research to help move us toward such a theory of location privacy by building upon other privacy theories and identifying and organizing relevant issues specific to location privacy.

Location privacy theory development will be important for a number of reasons. An obvious initial benefit, as with theory development in general, is to define terms, organize concepts, and frame issues for further study. Location as a component of personal information is of vital importance to personal safety, and is highly interrelated with other components of privacy in general. Location-aware technologies are among the most rapidly developing and most widely implemented, particularly in light of facilitating technologies such as GPS and legislative/regulatory mandates such as E911. Theory development will be necessary to allow the scientific process to perform logical deduction, form hypotheses, and interpret the results of hypotheses tests in empirical research. It will be essential to provide a framework for future legal, regulatory, and policy progress. In order to achieve and provide location privacy, it must first be defined and understood.

The following sections will discuss theory development, privacy theory, and location, followed by a synthesizing proposal for what issues should be addressed in a theory of location privacy. Examples are included for selected topics in these sections. Following this is a section describing the applications of location privacy theory. A concluding section

[1] Based on a 8/29/2010 search using http://scholar.google.com for the exact phrase "location privacy" with specific article publication date ranges as indicated.

discusses limitations and suggestions for future research.

2. Theory Development

Theories are key components in scientific knowledge. They are encouraged for a discipline's conceptual development [9] and help achieve the following five desirable goals (reproduced from [10]):

1. A method of organizing and categorizing "things," a *typology*;

2. *Predictions* of future events;

3. *Explanations* of past events;

4. A sense of *understanding* about what causes events. And occasionally mentioned as well is:

5. The potential for *control* of events.

Several strategies may be used to construct theories, including the following [11]:

1. A cause-effect strategy seeking causes of a phenomenon.

2. A cause-effect strategy seeking effects of a phenomenon.

3. A compositional strategy searching for properties, components, and processes (an endogenous approach).

4. A compositional strategy describing a context or background within which the phenomenon exists (an exogenous approach).

5. A classificatory strategy seeking a taxonomy of elements both within and outside the phenomenon.

In early stages of theory development, classification approaches are particularly important and necessary as a prerequisite for other strategies [12] and may have continued usefulness even after theory matures (examples include the biological classification and taxonomic rank system of species, genus . . .).

Theory development may be seen in the broader scope of the scientific process with the help of Figure 1, reproduced from [11]. We are primarily concerned with the left half of the diagram ("Theory Construction") and more specifically with the upper left quadrant ("Theorizing"). In the context of location privacy theory, the process we will use is guided by the components and relationships in Figure 1 from observations to theories in the following manner:

Observations: The issues related to location privacy are cataloged. Privacy issues include defining privacy, review of privacy theories from differing perspectives, considerations of related concepts such as identity and anonymity, and the impact of modern technologies on privacy. Location issues include defining location and the scope of interest for location (in this case, limited to the location of persons rather than geographical features, inanimate objects, etc.) and the methods and technologies available to determine location.

Empirical generalizations: Empirical generalizations will consist of summarizing location and privacy issues as they intersect and relate. Because of the psychological and sociological aspects of privacy concepts and the social science nature of these components as well as the immature state of location privacy theory, measurement and parameter estimation will not be as well developed as it might be for a physical sciences context.

Theories: Moving from empirical generalizations to theory is the challenge we are most interested in for the present research, investigating issues in the development of location privacy theory. Both descriptive and normative issues will be considered (i.e., where location privacy *is* the case versus when it *should be* the case). In the process of concept and proposition formation and arrangement, a large number of factors related to context, identity, location, and privacy come together.

Other aspects of the scientific process in [11] will be treated as outside the scope of the current research. The testing of particular hypotheses will largely be left to others and later research.

The research strategy used here is consistent with that used in other fields [13] and emphasizes discovery and description, where the key research questions are "Is there something interesting enough to justify research?" and "What are the key issues?" in both cases with categorization proposed as a procedure to be employed [13] (page 324).

3. Privacy Theory

Privacy theories have a rich history from many perspectives. One of the earliest relevant works is the 1890 Harvard Law Review article by Warren and Brandeis, "The Right to Privacy," [14] lamenting the privacy-invading advent of "instantaneous photographs and newspaper enterprise" and referring to earlier court decisions treating the right of privacy as the right "be left alone" (p. 195). Since that time there has been continuous change in law, technology, and social convention related to privacy, with corresponding development of theories of privacy.

An exhaustive examination of privacy theories is beyond the scope of the present research, however a review of major developments is important as it is proposed here that *location* privacy theory is a subset of *general* privacy theory. Because many issues related to location privacy arise because of, or are exacerbated by, information and communications technologies (ICT), emphasis will be given to information and technology-related aspects of privacy theory. A significant portion of our privacy theory discussion draws upon [2], which is particularly useful because of its comprehensiveness and implications for ICT.

3.1 Definitional Issues

Theories of privacy may be defined in terms of nonintrusion, seclusion, boundaries, control, and limitation [2]. Warren and Brandeis decry the potential intrusion of newspapers into otherwise private lives and fear that "what is whispered in the closet shall be proclaimed from the house-tops." [14] (p. 195). From a privacy-as-seclusion definition, "perfect privacy" is being "completely inaccessible to others" [15] (p. 428). We cannot help but note that the natural analog to this in location privacy is the definition of "perfect location privacy" as being "completely un-findable by others." Privacy defined in terms of boundaries, control, and limitation is consistent with Altman's [16] concept of privacy as the "selective control of access to the self" (p. 67) where privacy is a context-dependent boundary regulation process. As further emphasized in following sections, here we are addressing the privacy of *persons* in the context of other persons who may directly or indirectly violate that privacy. Beginning immediately below, location privacy theory issues will be summarized after sections of text that introduce and describe them.

Location Privacy Theory Issue 1: Privacy may be defined in terms of:
Intrusiveness
Seclusion
Boundaries, control, and limitation

Privacy theories may address natural or descriptive aspects (what *is* private, such as sunbathing in a remote wilderness area), and normative or prescriptive aspects (what *should be* private, such as a skin cancer screening by a physician). Privacy may be rights-based or interests-based, with the former often associated more with individual rights and the latter with the balancing of rights among groups. Accessibility privacy (which may be uncontrollable by the subject) may be contrasted with decisional privacy (at least partly dependent on choice of the subject) [2]. The context of privacy is not limited to private or secluded circumstances, as advances in technologies such as electronic surveillance have brought increased attention to the issue of "privacy in public" [17] as well. While privacy is a universal *concept* in all cultures, the *regulation* of privacy is dependent upon culture and context [16]. Finally privacy has physical aspects associated with direct interactions, and informational aspects which may be more abstract and further removed in space and time (addressed later).

Location Privacy Theory Issue 2: Privacy has properties that may be:
Natural/descriptive or normative/prescriptive
Rights-based or interests-based
Access-based or decisional
Public or private
Universal or culturally-dependent
Physical or informational

3.2 Identity Issues

From both a philosophical and technical perspective, identification (ID) is a critical concept in privacy. We are concerned with identification of persons (rather than inanimate objects, for example) because a person is a locus of rights, including any associated right to privacy. There is a substantial existing knowledge base in identity management (IDM), some of which is reviewed in [18] as it relates to privacy.

A person may be identified by sets of attributes including not only obvious identifiers such as name but also any attribute that helps to distinguish them from others (hair color, home town, etc.). Subsets of these attributes, called partial identities, may be disclosed in different contexts and for different purposes (e.g., at a cocktail party or when applying for a job). In some cases no name is associated with a partial identity (anonymity) and in other cases one or more names are associated with one or more partial identities (pseudonymity).

Important privacy issues arise when one considers the spectrum of possibilities with individuals and groups falling on an anonymous to identified continuum and employing pseudonyms. The anonymity continuum results from the practical consideration that a person is not typically fully anonymous, but rather a member of an anonymity set, within which she cannot be identified but whose overall membership may be known to outsiders.

Pseudonyms pose additional challenges to privacy. A person may choose multiple pseudonyms for multiple partial identities (and indeed, further assign pseudonyms across multiple activities and multiple contexts). These may all initially be distinct from each other and from the person's full identity, however the possibility of linkability between identities must be considered. Any released information about any of a person's pseudonyms may be used to reduce the size of her anonymity set, with persons often unaware of the extent to which they are inadvertently increasing their identifiability. For example, because Web browsers send "User Agent" and other information to Web servers, and because there are so many unique combinations of such information attributes, it has been estimated that on average only one person in 1500 will have the same attribute set as a given Web user [19]. Set theoretic issues in privacy, anonymity, and pseudonymity can all be seen in the following natural language statements:

1. "It's me, anonymous, again."[2]
2. "Just call me User1234 in this group."
3. "I'm not one of the complainers."
4. "I've never spoken up before."

Location Privacy Theory Issue 3: Privacy is dependent upon identification, which in turn is dependent upon:

Personal attributes
Partial identities

3.3 Informational Privacy

Informational privacy is a prominent part of most privacy theories, and the aspect to which we devote the most attention. It is especially relevant as ICT and technologies related to location evolve (the latter variously referred to as location-aware, location-based, and location-enabled applications and systems). One of the earlier works to explicitly recognize privacy in terms of information was Weston more than four decades ago in describing privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [20] (p. 7). Indeed the author also noted the need to address input, storage, and output aspects of privacy as evolving computer systems stored personal information, and suggested that such personal information should be defined as a property right [20] (p. 324). The centrality of information to privacy is also evident in control and limitation theories of privacy. Although some argue these are distinct [2], both involve decisional ability of a subject to allow collection of (or not) and restrict use of (or not) selected information in particular contexts. This includes individuals being able to control information "leaks." While there may indeed be important underlying conceptual distinctions between control and limit approaches, to an ICT system both are implemented essentially as security and database access policies—with considerable ability to implement any levels of control granularity desired. The privacy in public versus private venues leads to an informational corollary of public personal information (PPI) versus non-public information (NPI).

After reviewing the issues above and more, the author in [2] proposes a Restricted Access/Limited Control (RALC) theory of privacy, revised from an earlier approach [21]. RALC distinguishes between descriptive conditions of privacy and normative rights to privacy, and notes that the particular situation (activities in locations, storage or access of information, etc.) of the subject is important. Furthermore, even in private situations it distinguishes between naturally private situations (where observation is impossible or improbable) from normatively private situations (where observation is prohibited).

Although the brief review above may lead the reader to assume that control of privacy is generally considered desirable, privacy itself is not monotonic and more is not always better—we may voluntarily disclose information in private to promote intimate relationships and in public to maintain a public persona [6]. Economic considerations are important, as individuals may be willing to trade location privacy information for non-trivial but not particularly large monetary sums [22].

Informational privacy is naturally dependent upon the flow of information from sources to sinks, along with intermediary storage, use, and possible transformations. Where location information is involved, informational location privacy is influenced by this flow of information. Many of the relevant issues are cataloged in [8] and so are only selectively reviewed below.

Location information acquisition/ determination. The volume of information acquired for location-related applications tends to be many orders of magnitudes larger than for many other typical privacy-sensitive transactions. For example, while the average US consumer makes credit card purchases at the average rate of approximately one per day [23], GPS devices can easily and automatically acquire location data at many times per second, leading to the acquisition of several million data points even for relatively modest and short-term travel studies [24].

Location information retention/storage. The storage of location information makes it available to viewers not only in the present but in the future as well [6]—turning a recording surveillance camera into a visual time machine as well. It has been noted that there is a simple method to increase privacy in the

[2] Observed by the author in a blog comment—there had been several non-anonymous comments and exactly one anonymous comment previously.

digital age—merely re-introduce the notion of forgetting by placing expiration dates on information [25].

Location information application/use. Some uses of stored location information pose no immediate privacy risk—for example, a person storing her hike's starting location in her GPS to assist in finding the way back. When the information is stored by third parties or with inadequate controls, however, issues rapidly emerge. Most mobile phone carriers, for example, have few limitations on the uses they themselves make of customer location information. Even without sharing it with any other parties, they may still analytically exploit the information for a wide variety of marketing and competitive purposes.

Location information disclosure/sharing. This area typically generates the most concern among privacy advocates. Once location information is shared with others, control by the original owner rapidly erodes. Legal considerations and privacy-enhancing technologies, discussed in Section 6, are important control and limitation mechanisms related to location information disclosure/sharing.

Location Privacy Theory Issue 4: The informational aspects of location privacy relate to:

Information acquisition/determination
Information retention/storage
Information application/use
Information disclosure/sharing

4. Location

To the lay person, location may be the simple notion of "where I am." In a modern technological environment of context-aware location-based services, however, location has much more complex meaning. In this section we begin enumerating location-specific issues that affect the development of location privacy theory. A survey and taxonomy of location systems for mobile-computing applications [26] contains an excellent overview of location properties, and the discussion in this section closely follows that framework.

Location of a person or a device (or one by implied association with the other) can be sensed via triangulation, scene analysis, or proximity. Sensing technique is important and distinct from location properties (discussed later) because it involves process and feasibility rather than only information properties. Triangulation is used by the Global Positioning System (GPS), some cellular telephone location approaches, and other methods.

Scene analysis uses visual or other environmental cues to place an object in context related to other objects with known locations (e.g., a person standing in front of a unique architectural landmark). Examples of scene analysis range from simple security cameras whose images are interpreted by humans, to automated systems such as Google Goggles (http://www.google.com/mobile/goggles/) which can identify landmarks from mobile phone images.

Proximity determines location by detecting when an object is near a sensor, e.g., it physically touches a pressure-sensitive device, establishes communication with a wireless access point or Bluetooth device, or interfaces with a device such as a credit card scanner. Examples include commonly-used RFID and NFC (Near Field Communication) systems in pass cards for public transportation systems. It should be noted that with proximity location, as well as triangulation methods where a device rather than a person is the object directly located, the linkage of device to person is of critical importance. For example, a burglar could lend his mobile phone to an innocent friend in order to disguise his true location while committing a crime.

Location Privacy Theory Issue 5: Location privacy theory must recognize that location can be sensed or determined through:

Triangulation
Scene Analysis
Proximity

Ultimately more important than the methods of location used, for theory development we must define the relevant *properties* of location. For the present research the more relevant of these involve physical versus symbolic location, absolute versus relative location, local versus external location computation, accuracy and precision, and time. These properties are a subset of those enumerated in [26], where additional issues of scale, cost, and various technological limitations are also discussed. Recognition is included as a location property in [26], but can also be treated as identification as discussed earlier.

The distinction between physical position and symbolic location is important because the former is essentially raw data, while the latter is generally more interpretable and useful information. Physical position is typically reported according to a coordinate grid such as latitude and longitude, while symbolic location relates an object to a meaningful context such as in or near a particular city, landmark, or other object of interest. Transformations between physical positions and symbolic locations are possible where additional information can link to or compute one from another.

Absolute versus relative location is intriguing because all locations are inherently relative. The distinction is that absolute locations are all assumed to be relative to the same single frame of reference (e.g., GPS coordinates are all relative to the physical planet Earth) while the relative locations of objects are defined with respect to an arbitrary number of other objects (e.g., a bus is 500 meters from its next stop). As was the case with physical and symbolic locations, transformations between absolute and relative locations are possible if additional information is available—in this case a linkage between frames of reference used. In the examples above, if the GPS coordinates of the bus and its next stop are both known, the distance between them may be computed.

Local versus external location computation is a distinction which inherently affects location privacy. In local location computation, of which GPS is an example, the located device computes its location without any external assistance except a unidirectional flow of information into the device. The resultant location information does not then need to be transmitted to any other entity (indeed no other entity even knows it has been computed), and is thus inherently private. In systems with external location computation, such as non-GPS triangulation-based cell phone location systems, the located device must communicate with an external infrastructure (such as cell towers) and bi-directionally exchange information that makes disclosure of at least some location information inevitable. In the extreme case of external location computation, the located device is unable to access its own location and only the external infrastructure maintains the computed location information.

The expected resolution of location fidelity can be described in terms of accuracy and precision [26], where accuracy is measured in distance between estimated and true position, and precision is expressed in terms of the probability of achieving a given level of accuracy. Thus location can be described by a statistical distribution, with inferences such as a GPS receiver's location determination being accurate to with 10 meters in 95 percent of samples.

An additional aspect of location that is increasing in importance but is treated in [26] primarily in a technical method sense (e.g., signal latency used to compute distance) is time. Time is important in at least three senses: (1) time(s) associated with initial location data collection; (2) time(s) of actual location determination, if delayed compared to the data collection time(s); and (3) intervals of time between locations of the same or related objects.

Times associated with location data collection are of obvious significance for real-time scenarios and applications where contemporaneous or synchronized processes are involved. Timing of actual location determination has a more subtle importance because in many instances specific locations are not or cannot be computed until well after the fact. This may be the case where frequently-sampled locations of vehicles are transmitted to a dispatching center, for example, but specific vehicle locations are not closely examined except on an ad-hoc, as needed basis. The possibility of new issues not originally anticipated arises from the capability of re-analyzing data collected long ago before all uses could be foreseen. This is analogous to the surprise that early 1980s posters to Usenet News found when Google announced some 20 years later the availability of a searchable archive (http://www.google.com/googlegroups/archive_announce_20.html) now covering almost three decades and over a billion postings.

Finally, intervals of time associated with the same or related objects obviously introduce the capabilities of computing speed, direction, extrapolation and prediction of future location, etc.

Location Privacy Theory Issue 6: Location properties may be:
Physical or symbolic
Absolute or relative
Locally or externally computed
Accuracy and precision
Time (in both static and dynamic senses)

Work on technical aspects of location systems continues, including localization from mere connectivity [27], vision-based approaches [28], dead reckoning [29], tracking people using mobile robots [30], etc. but these approaches still fall into the basic categories outlined above.

Many location specifications are combinations of, or may be computed from, locations of multiple objects and/or supplemental data from external sources. To motivate the rich variety, context, and application of possible location specifications, consider the following natural language assertions:

1. "I'm at work."
2. "I'm five minutes away from John."
3. "I have never met Sue in person."
4. "I'm somewhere I've never been before."
5. "I'm waiting where we met last time."[3]

These statements illustrate the complex interactions of a lay person's notion of "where I am" with the many important and distinct formal properties of location.

[3] From the title of [31], which explores many additional everyday positioning practices.

5. Theory of Location Privacy

We have assumed that location privacy theories must be a subset of privacy theories and carry with them the issues of those theories as well as the implications of location and applications of location-related technologies. Six location privacy theory related issues have been identified. In order to organize these issues and begin the initial steps toward a location privacy theory, the influence diagram model shown in Figure 2 is posited. It contains a substantial number of components, following the prescription that at this stage it is better to err in favor of including too many factors [32]. Arrows in Figure 2 represent influences, dependencies, and/or information flows but are not individually or formally specified in detail.

The top right box in Figure 2 indicates that context is a primary influence on location privacy. This context includes the activities a person is engaged in and their environment, which may have technological, social, and other characteristics. Context also includes a myriad of personal preferences as well as cultural and other factors. Context affects identification in terms of what personal attributes are recorded (which in turn affects the feasibility of location sensing), and privacy properties including whether the context is public or private, affecting norms and user expectations.

The left column of five boxes in Figure 2 shows information flows from initial sensing of signals or data resulting in location acquisition/determination through retention/storage, application/use, and possible disclosure/sharing. Identification information also flows into the location acquisition process, which is necessary to associate a location with an entity (in our case, individuals or groups being the entity of interest). Information flows are affected by the possibility of linkability between identity and location information, and provide a means for defining privacy-enhancing technologies in terms of unlinking, interrupting, or introducing ambiguity into information flows.

Two additional important influences on location privacy are the particular properties of location and properties of privacy. Location properties are shown in the middle column of Figure 2. They can greatly affect location privacy depending on whether and how they are specified. For example an absolute location may be later combined with other information in much different ways than relative location information may be (consider that if my location is recorded as being near a coffee shop sometime last week, this is much different than being recorded as located at the intersection of 5th and Main at 7:30 AM.)

Privacy properties are likewise critical as they affect privacy in general, which in turn affects location privacy specifically. A prescriptive (normative) privacy property affects general privacy and subsequently becomes a prescriptive property of specific location privacy. For example, the prescriptive requirement that a student attend class becomes a prescriptive property of that student's location privacy.

Explanation of location privacy is afforded in Figure 2 by laying out the influence relationships between components. It specifies, for example, that factors of time affect location privacy directly. Prediction is facilitated in the model in part due to the influences specified, as well as the logical deductions that may be made based upon those relationships. Noting the different characteristics of local versus external location acquisition, for example, makes it possible to predict the effects of a change from one to another in location privacy.

Guidance for future research is key to theory in that it informs and motivates generation and testing of hypotheses to confirm, refine, and extend the theory. As shown in Figure 1, this provides a feedback loop that allows interpretation, further observation, measurement, and other empirical research activities leading to further theorizing and possible improvement of the theory based on evidence. The testing of hypotheses about the theory itself promotes additional logical inference for conceptual theory building and refinement.

6. Location Privacy Theory Applications

In this section we consider applications of location privacy theory with examples related to research from diverse perspectives including behavioral, legal, and technological approaches. In some cases, research efforts may fit entirely within the model shown here, and in some cases they may include additional exogenous factors.

Behavioral research in privacy and location privacy considers user characteristics (such as personality traits, cognitive style, and personal preferences), task characteristics (such as structuredness), and technology characteristics (such as location-awareness and ease of use) as well as combinations of factors (such as task-technology fit). These can be related to privacy considerations (actual, perceived, and desired) and focused on location privacy if desired. An example is [33], which reviews other research and proposes empirical research methods. Behavioral research provides examples of exogenous variables flowing into the model proposed in Figure 2, in ways which are consistent with the model. User characteristics flow into context and privacy properties (e.g., personal preferences and cultural factors into decisional privacy properties and into control considerations). Technology characteristics are incorporated into sensing and location acquisition components when location-related, with additional exogenous variables being part of larger systems which incorporate other functionality in addition to location-relate features.

Legal and ethical considerations are important to location privacy, and have been discussed in works such as [34] which considers the context of employee location monitoring. These considerations are relevant to and incorporated within Figures 2's left column (information flows) and right column (privacy context and properties) in that there may be legal or ethical requirements and constraints on any technologies, activities, and processes involved. For example, OECD guidelines [35] specify a number of requirements limiting the collection and use of information, including location information.

Privacy-Enhancing Technologies (PETs) are "technical and organizational concepts that aim at protecting personal identity" and "give direct control over revelation of personal information to the person concerned" [36] (p. 125). The technical aspects of PETs can be used to control the information flows in the left column of Figure 2, while the organizational aspects would affect the user environment, decisional privacy properties, and other informational privacy issues in the right column.

Many hypotheses may be generated and/or tested by considering various combinations of components and influences in Figure 2. For example the following propositions might be further investigated:

1. Individuals' perceptions and preferences of location privacy may differ from their perceptions and preferences for other forms of privacy (e.g., while Web browsing).
2. Enforcing location privacy may be most successful when done earlier rather than later in the sequence of information acquisition through disclosure.
3. Location privacy may be enhanced by deliberately introducing ambiguity into any of the location property determinants (ID, absolute location, time, or activity). [37]
4. Individuals may not be able to accurately predict the present or future linkability of ID and location information. [38]

7. Conclusions and Recommendations

Location technologies are rapidly advancing, and through their ability to track users are creating a myriad of associated privacy issues. Existing privacy theories provide a strong base from which to frame these issues, but do not provide the specific structure and guidance to deal with all emerging challenges. A theory of location privacy is needed to clearly define concepts, organize relationships and discourse, and to guide additional research.

The present research identifies major issues involved in location privacy theory and organizes these into a model that can form the basis for theory. It posits necessary components and relationships between them, with major sections involving information flows, location issues, and privacy issues. These form a model of location privacy that is general enough to address broad conceptual issues yet sufficiently specific to highlight particular emerging technologies and the challenges they introduce.

The model presented here represents an initial organization of components. Its usefulness should be measured in terms of how it aids in explanation, prediction, and guidance for future research. It makes modest yet significant gains in these areas, particularly in the context of the current paucity of other comprehensive and universally accepted theories.

It is hoped that the model introduced here may be examined in further research, refined, and enhanced. Validation of relationships may be conducted through hypothesis tests that may further specify influences in terms of directional, causal relationships and other more precise structures. A sound theoretical base can serve to not only guide research but also inform policy making and technology development for the future.

8. References

[1] Charles E. Perkins, Andrew Myles, and David B. Johnson, "The Internet Mobile Host Protocol (IMHP)," 1994.

[2] H. T. TAVANI, "PHILOSOPHICAL THEORIES OF PRIVACY: IMPLICATIONS FOR AN ADEQUATE ONLINE PRIVACY POLICY," *Metaphilosophy*, vol. 38, no. 1, pp. 1-22, 2007.

[3] L. Floridi, "Four challenges for a theory of informational privacy," *Ethics and Information Technology*, vol. 8, no. 3, pp. 109-119, Jul. 2006.

[4] J. H. Moor, "Towards a theory of privacy in the information age," *SIGCAS Comput. Soc.*, vol. 27, no. 3, pp. 27-32, 1997.

[5] A. Acquisti, *Digital privacy : theory, technologies, and practices*. New York: Auerbach Publications, 2008.

[6] L. Palen and P. Dourish, “Unpacking "privacy" for a networked world,” in *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 129-136, 2003.

[7] B. Jiang and X. Yao, “Location-based services and GIS in perspective,” *Computers, Environment and Urban Systems*, vol. 30, no. 6, pp. 712-725, Nov. 2006.

[8] R. Minch, “Privacy issues in location-aware mobile devices,” in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 2004.

[9] R. Sutton and B. Straw, “What Theory Is Not,” *Administrative science quarterly.*, vol. 40, no. 3, p. 371, 1995.

[10] P. Reynolds, *A primer in theory construction.* Indianapolis: Bobbs-Merrill, 1971.

[11] W. Wallace, *The logic of science in sociology*. Chicago: Aldine·Atherton, 1971.

[12] E. Nagel, *The structure of science problems in the logic of scientific explanation.* New York: Harcourt Brace & World, 1961.

[13] R. Handfield, “The scientific theory-building process: a primer using the case of TQM,” *Journal of operations management.*, vol. 16, no. 4, p. 321, 1998.

[14] S. Warren, “THE RIGHT TO PRIVACY.,” *Harvard Law Review*, vol. 4, no. 5, p. 193, Dec. 1890.

[15] R. Gavison, “Privacy and the Limits of Law,” *Yale Law Journal*, vol. 89, no. 3, p. 421, 1980.

[16] I. Altman, “Privacy Regulation: Culturally Universal or Culturally Specific?,” *Journal of Social Issues*, vol. 33, no. 3, pp. 66-84, 1977.

[17] H. Nissenbaum, “Protecting Privacy in an Information Age: The Problem of Privacy in Public,” *Law and Philosophy*, vol. 17, no. 5, pp. 559-596, Nov. 1998.

[18] S. Clauβ, D. Kesdogan, and T. Kölsch, “Privacy enhancing identity management: protection against re-identification and profiling,” in *Proceedings of the 2005 workshop on Digital identity management*, pp. 84-93, 2005.

[19] “Browser Versions Carry 10.5 Bits of Identifying Information on Average | Electronic Frontier Foundation.” [Online]. Available: https://www.eff.org/deeplinks/2010/01/tracking-by-user-agent. [Accessed: 13-Jun-2010].

[20] A. F. Weston, *Privacy and Freedom*. New York: Atheneum, 1967.

[21] J. H. Moor, “Towards a Theory of Privacy in the Information Age,” *Computers and Society*, pp. 27-32, 1997.

[22] G. Danezis, S. Lewis, and R. Anderson, “How Much is Location Privacy Worth?,” *ONLINE PROCEEDINGS OF THE WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY SERIES (WEIS 2005*, 2005.

[23] R. Litan, *Moving money : the future of consumer payments*. Washington D.C.: Brookings Institution Press, 2009.

[24] C. A. Quiroga and D. Bullock, “Travel time studies with global positioning and geographic information systems: an integrated methodology,” *Transportation Research Part C: Emerging Technologies*, vol. 6, no. 1, pp. 101-127, Feb. 1998.

[25] V. Mayer-Scho□nberger, *Delete : the virtue of forgetting in the digital age*. Princeton: Princeton University Press, 2009.

[26] J. Hightower and G. Borriello, “Location systems for ubiquitous computing,” *Computer*, vol. 34, no. 8, pp. 57-66, 2001.

[27] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz, “Localization from mere connectivity,” in *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking \&amp; computing*, pp. 201-212, 2003.

[28] D. Lo´pez de Ipin˜a, P. R. S. Mendonça, A. Hopper, and A. Hopper, “TRIP: A Low-Cost Vision-Based Location System for Ubiquitous Computing,” *Personal and Ubiquitous Computing*, vol. 6, no. 3, pp. 206-219, May. 2002.

[29] J. Torres-Solis and T. Chau, “Wearable indoor pedestrian dead reckoning system,” *Pervasive and Mobile Computing*, vol. 6, no. 3, pp. 351-361, Jun. 2010.

[30] T. Germa, F. Lerasle, N. Ouadah, and V. Cadenat, “Vision and RFID data fusion for tracking people in crowds by a mobile robot,” *Computer Vision and Image Understanding*, vol. 114, no. 6, pp. 641-651, Jun. 2010.

[31] A. Weilenmann and P. Leuchovius, “I'm waiting where we met last time: exploring everyday positioning practices to inform design,” in *Proc. NordiCHI*, 2004.

[32] D. Whetten, “What Constitutes a Theoretical Contribution?,” *The Academy of Management Review*, vol. 14, no. 4, pp. 490-495, 1989.

[33] I. Junglas, “A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services,” *PROCEEDINGS OF THE ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES*, no. 38, p. 180, 2005.

[34] G. Kaupins, “Legal and Ethical Implications of Employee Location Monitoring,” *PROCEEDINGS OF THE ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES*, no. 38, p. 133, 2005.

[35] “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.” [Online]. Available: http://www.oecd.org/document/57/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. [Accessed: 14-Jun-2010].

[36] P. Agre, *Technology and privacy : the new landscape*. Cambridge Mass.: MIT Press, 1997.

[37] B. Gedik and L. Liu, “Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms,” *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1-18, 2008.

[38] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, and Muthuramakrishnan Venkitasubramaniam, “l-Diversity: Privacy Beyond k-Anonymity,” 2006.

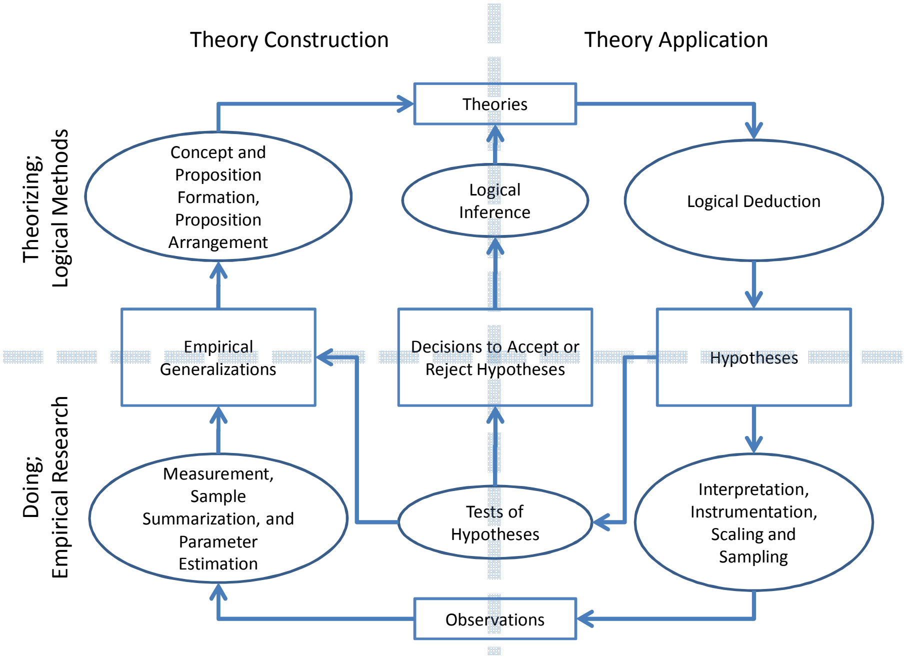
Theory Construction
Theory Application
Theories
Theorizing; Logical Methods
Concept and Proposition Formation, Proposition Arrangement
Logical Inference
Logical Deduction
Empirical Generalizations
Decisions to Accept or Reject Hypotheses
Hypotheses
Doing; Empirical Research
Measurement, Sample Summarization, and Parameter Estimation
Tests of Hypotheses
Interpretation, Instrumentation, Scaling and Sampling
Observations

Figure 1: "The Principal Informational Components, Methodological Controls, and Information Transformations of the Scientific Process." (Reproduced from [11])

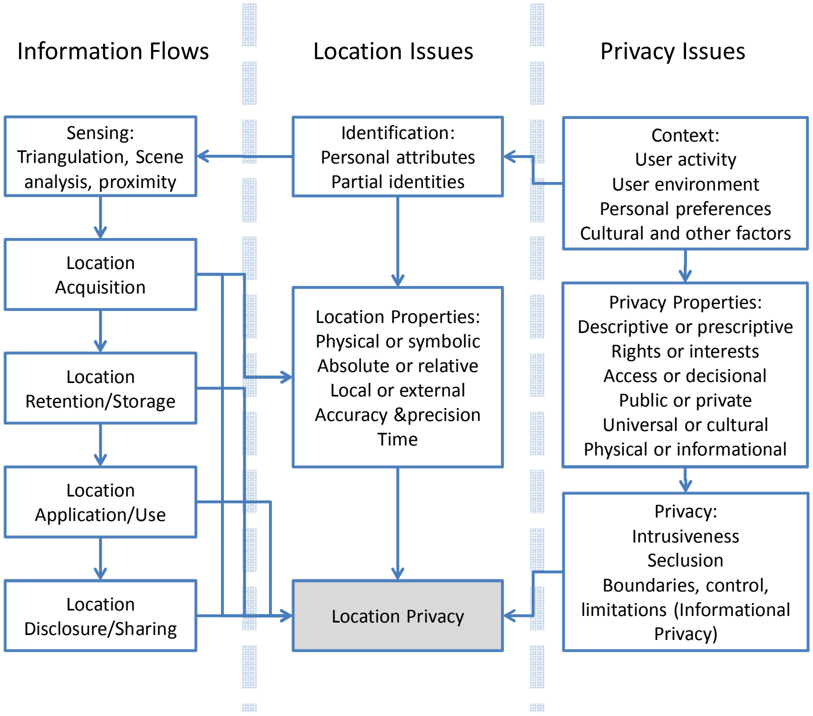
Information Flows
Location Issues
Privacy Issues
Sensing: Triangulation, Scene analysis, proximity
Identification: Personal attributes Partial identities
Context: User activity User environment Personal preferences Cultural and other factors
Location Acquisition
Location Properties: Physical or symbolic Absolute or relative Local or external Accuracy &precision Time
Privacy Properties: Descriptive or prescriptive Rights or interests Access or decisional Public or private Universal or cultural Physical or informational
Location Retention/Storage
Location Application/Use
Privacy: Intrusiveness Seclusion Boundaries, control, limitations (Informational Privacy)
Location Disclosure/Sharing
Location Privacy

Figure 2: Influence diagram model of location privacy theory issues