White Paper: Location Technologies and Privacy

Roger Ford
Information Law Institute
New York University School of Law
roger.ford@nyu.edu

Introduction

It’s like a scene from a dystopian novel: people carrying devices that track their every move, recording their activities in real time and send that information to third parties to be collected and aggregated. The privacy implications of such devices are obvious. They could let law enforcement track suspects’ movements — or everyone’s movements — or gather lists of potential suspects who were near crime scenes. They could let companies track their customers and learn things about them that the customers do not want to share. They could let jealous spouses, or malicious stalkers, track their victims. And depending on the devices’ design, all these uses and more could happen without users ever knowing.

Of course, pervasive tracking devices are not a fiction; today most people carry devices — smartphones and other gadgets — that contain location-tracking technologies such as GPS chips. Far from creating a dystopian nightmare, these devices and technologies have greatly benefited users, letting them take advantage of numerous applications and uses that would have been impossible without location technologies. Today, users routinely use location technologies to get turn-by-turn directions, find nearby restaurants and businesses, learn about the world around them, and connect with strangers and friends in the real world. Companies use location technologies to provide services that would otherwise be difficult or impossible to provide, such as real-time traffic information. And government actors use location technologies to make the public safer, for example by finding 911 callers before it’s too late.

Like many new technologies, then, location technologies are tremendously useful and yet profoundly troubling, enabling amazing new applications while presenting substantial privacy questions. The challenge for the technology industry, users, policymakers, and other stakeholders will be to craft approaches to privacy that permit and encourage these beneficial new uses while protecting users’ privacy. To date, public policy has not yet caught up with the growth of location technologies, and there is little consensus about the best ways to encourage innovative new uses while protecting privacy.

This paper aims to assist policymakers and others confronting the privacy issues presented by location technologies to match appropriate regulatory schemes to privacy issues. Specifically, it (1) discusses the privacy interests implicated by location technologies and the potential harms to users from use of those technologies; (2) describes several questions that must be answered to determine whether any particular use of location technologies implicates privacy concerns; (3) presents three models of regulating these
privacy issues and protecting consumers; and (4) offers recommendations for approaching location-privacy issues and applying these regulatory models.

I. Location Information and Privacy Interests

Location technologies are technologies by which a mobile device, such as a smartphone or tablet computer, can determine its own location (and thus its user’s location). Different technologies, including GPS, A-GPS, Wi-Fi, and IP-based tools, can be used to determine a device’s location, but under FCC regulations every modern cell phone in the United States has some form of location technology. (This paper focuses on privacy issues presented by the use of location technologies in smartphones and other wireless devices; other uses of location technologies, such as the use of other GPS devices and facial recognition in law enforcement, are beyond the scope of this paper.)

Location technologies are critically important to the wireless industry, since they are the backbone of vital services like E-911 services. Increasingly, location technologies are enabling new uses for wireless devices, from maps and up-to-the-minute traffic information to local restaurant recommendations and real-world social networks. These new uses have undoubtedly provided benefits to users.

Location technologies also have the inherent capacity to compromise users’ privacy interests, however. Technologies that reveal a user’s location provide a direct connection to the user in the real world, making him or her vulnerable to threats that would not be possible in the electronic world. They also reveal a great deal about a user — where he or she goes and when. This data may be linked to sensitive or confidential information, such as whether a user attends AA meetings or visits an AIDS clinic, and even when it isn’t, it can reveal a mosaic of information that, in the aggregate, says a great deal about a person. And this information can be stored, linked to other personal information, or transferred to third parties, making it possible to build increasingly sophisticated and detailed profiles of individual users and communities.

Privacy is a concept with many meanings, and legal and technology scholars have identified numerous privacy interests that can be compromised using location technologies. Daniel Solove describes four types of actions that can invade privacy interests: information collection, information processing, information dissemination, and invasion. The use of location technologies implicates all four of these categories. Location technologies make it possible for third parties, including wireless service providers, device makers, operating-system makers, and app developers, to gather information about users, process that information for their business purposes, and transfer it to third parties. They can also make it easier to invade a user’s personal solitude, since a user who knows, or thinks, that his or her movements are being tracked may feel less comfortable in his or her personal life or may forgo normal activities. Indeed, in the wrong hands the information that location technologies make accessible can lead to invasion of the user’s physical world, since someone who knows where to find a user can more easily disturb him or her.
Not all uses of location information that fall into these categories are bad, of course; many are beneficial to all involved, including users and third parties. Some of them do lead to harm, however. The scholarly literature describes two basic categories of privacy harms: harms to the individual user and harms to society as a whole.

Privacy harms can stem from the unauthorized, unwanted, or unanticipated collection, disclosure, or use of information about users, or from authorized collections, disclosures, or uses that cause harm to the user. Not all collection, disclosure, and use of information will cause harm to all users, and some activities may harm some users but not others. For instance, the use of location information to provide real-time maps may harm no one, while the disclosure of that information to malicious actors may harm every user exposed to the problem.

Social harms can arise when the collection, disclosure, or use of location information has negative effects on social systems or values. For example, the widespread collection, disclosure, and use of location information may create uncertainty about how one’s location information will be used. In response to this uncertainty, users may curtail their use of mobile devices, use overly restrictive privacy-protection mechanisms, or refuse to consent even to beneficial uses. This sort of chilling effect can itself be a privacy harm even if it results only in underuse of location technologies.

The critical takeaway is that the use of location technologies can affect different privacy interests, and that while many uses are beneficial to users, some can cause harm. Distinguishing between these types of uses is an important first step toward protecting privacy while promoting beneficial uses of location technologies.

II. Uses of Location Technologies

Since location technologies are used in numerous contexts and for numerous purposes, the details of how a particular technology use is designed and implemented matter greatly in evaluating the privacy implications of that use. To evaluate a particular technology, one should ask several questions, including:

- **Who has access (authorized or otherwise) to a user's location information?**
- **What information is collected, and to what other information can it be connected?**
- **Why is location information being collected, and what uses are being made of that information?**
- **How is the location information and other personal information used, maintained, and secured?**
These questions correspond to *who, what, why,* and *how.* (We could also describe *when* and *where* a location technology uses data, but these questions are less interesting from a privacy perspective.) A comprehensive system for regulating information technologies must consider each of these questions.

A. **Who has access?**

Numerous separate entities have the potential opportunity to access and use location information:

- *Service providers,* such as Verizon Wireless or T-Mobile;
- *Handset and device makers,* such as Apple, HTC, or Samsung;
- *Operating-system makers,* such as Apple, Google, or Microsoft;
- *Application makers,* such as Yelp or Foursquare;
- *Users;*
- *The public,* or subsets thereof;
- *Others with physical access to a device,* such as police officers, family members, and thieves; and
- *Malicious actors,* such as malware developers and hackers.

Not all of these actors can use location information in all circumstances; instead, the location technology must make it possible for the actor to access the location information. Technologies that provide greater access to location information — authorized or otherwise — have greater privacy implications.

B. **What information is included?**

At its most basic, a unit of location information could consist of as little as a single location, perhaps with a timestamp. This location could be vague or specific: it could indicate that a device was in a particular city, neighborhood, or cell tower’s range, or specify an address or location with sub-meter resolution. Generally, location data becomes more useful as it gets more specific: users, businesses, and government actors can do much more with a precise location than with a neighborhood or a city. But with added specificity comes greater privacy implications, since the more-specific data point reveals far more about a user’s movements.
Location information can also include much more than pure locations. A tracker of location information might be able to connect location readings to the particular device identifier or to a user’s name or other personal identifier. The system could then match a location where a user was spotted to the user’s other personal information, such as his or her history of movements, the specific action undertaken when the location reading was created, or a profile containing personal interests or shopping preferences. As before, the more specific the information, the greater the privacy implications: a piece of location data that cannot be associated with an individual user reveals much less than one that can be linked to a user’s detailed profile.

We can think of the information revealed by a location technology, then, as falling at a point in two dimensions, with the axes corresponding to the resolution of the location information and the resolution of the personal information:

As a location technology provides information that is more detailed and specific in the locations described, it moves to the right in the diagram; as it provides greater and more specific links to individual users, or becomes easier to identify individual users, it moves up in the diagram.

There are two critical points that follow from this formulation.

First, moving to more specific information in either dimension creates greater privacy implications. We can see this by starting with the scenario presenting the fewest privacy problems, in which a location technology collects what I call pure “point data,” at the neighborhood level. In this scenario, mobile devices provide individual location data points at the neighborhood level, perhaps with time stamps, that are unconnected to personally identifiable information or information about what device they come from. The technology
provider can aggregate these data points, but since they are not connected to individual users or devices, the privacy implications are limited. Such technologies can provide information about the overall use of a network or service, but otherwise have relatively limited uses, such as determining where new cell sites are needed or predicting location-specific trends.

It’s easy to see how providing more information about individual users or devices increases the privacy implications. Even using low-resolution location information, such as neighborhood data or anonymous location identifiers, a technology that matches such location information to individual users provides much information about individual users that would be impossible to obtain from pure point data. Knowing that a user was in a specific city on a certain day can reveal sensitive personal information, even if it does not reveal where exactly he or she visited. And if a technology maintains what I call “path data” — information about a user’s movements over time — the possibility that it will reveal sensitive data is even greater.

More subtly, providing detailed and specific point data can also increase a technology’s privacy implications, even if the location information is not connected to any information about individual users or devices. For example, a technology that stores locations at a sub-meter resolution could disclose that a device was observed in a specific home or business at a specific time. Even without containing any personal or device information, such information could reveal sensitive information — for instance, that someone was in a home when all its occupants were supposed to be at work, which might reveal that someone is having an affair, or that someone was in a business overnight, which might reveal that an employee is committing crimes or getting ready to quit.

The second important point is that aggregated information about a particular device — and especially path data — can present privacy issues even if it does not appear to contain any links to personal information. This means that efforts to “anonymize” data are risky, since aggregated data can frequently be linked back to an individual user.

For example, a location technology that tracked mobile devices using anonymous ID numbers might record that an individual device frequently travels from a specific house to a specific office. (Even without a link to any personally identifiable information, this might be useful to a service provider tracking movement within a network or collecting aggregate demographic information.) It would be no great leap, however, to determine that that device belongs to the user who lives at that house and works at that office, even if the system maintains no link between the “anonymized” location information and other personal information.

The privacy implications of such “anonymized” location technologies are less severe than those for technologies that use personally identifiable information, since it will be more difficult and costly for a service provider to identify individual users. But if a provider has reason to try to identify an individual user, relies on a flawed approach to
anonymization, or allows insufficiently secured location information to fall into the hands of a malicious actor, then individual users can be vulnerable to privacy invasions.

C. What uses are made?

The entities listed above make numerous uses of location data. We can place the most common uses into four basic categories:

- **Necessary and expected business uses**, which could also be called location-product uses, are uses for which location data is central to the benefits a user expects to receive from a product or feature. Such uses are those for which the user would understand and expect that the product or feature uses his or her location information while he or she uses the product or feature. Examples include maps and navigation services, location-enabled social-networking apps like Foursquare, and location-based “deals” apps like Groupon and Living Social, all of which must know a user’s real-time location to provide the desired service.

- **Other business uses** are uses of location information for business purposes that are not central to the purpose for which the user uses an app. These uses include marketing uses, infrastructure uses like improving network performance, and analytic uses like deciding where to locate a retail store or outdoor advertisement.

- **Public uses** are uses for nonbusiness purposes such as law enforcement, civil judicial proceedings, and public safety, including E-911 service. Public uses can benefit individual users (for example, by using a cell phone’s GPS to locate a 911 caller) or society as a whole (for example, by tracking cell phones located near a crime scene).

- **Personal and malicious uses** are uses unauthorized by users or service providers, including uses by family members, abusive spouses, hackers, and malware developers.

The distinction between necessary and expected business uses and other business uses matters because only the former are uses of which, simply by using a product or service, a user should reasonably be placed on notice that his or her location information is being disclosed and used. While it is possible to provide most mobile products or services without using location information, services that require their use, and would be understood by users to do so, present lesser privacy concerns since users can be presumed to consent to such uses of their location information.

Various uses within a category can present greater or lesser privacy concerns. For instance, marketing uses can present greater or lesser privacy concerns depending on what location information they use and how the use is structured:
- Aggregated market research, the use of aggregated location information of many users to target ads on a non-individualized basis or create generic user profiles, presents relatively minimal privacy concerns since it does not make individualized use of location information.

- Behavioral marketing, the use of a user’s location information to build a profile for that user that is then used to show targeted ads, presents greater privacy concerns since it uses an individual user’s location information in a way to which the user may provide consent, or even understand.

- Real-time marketing, the use of a user’s real-time location information to show ads for nearby products or services, can present even greater privacy concerns if it makes users vulnerable to physical intrusions in the real world.

Likewise, even necessary and expected uses can pose greater or lesser privacy concerns, depending on the details of the use.

**D. How is location information used, maintained, and secured?**

How location information, like any person information, is used, maintained, and secured can make a big difference for users’ privacy interests.

How location information is used matters because there are usually several ways to accomplish a given task, with different tradeoffs and different privacy effects. For example, a map application could load map content on the fly over the network, based on a device’s real-time location, or it could store the same map information locally on the device. Each system has its advantages. The network-connected app can more easily provide the most up-to-date map information since it gets its information from a central server, and it can avoid storing large volumes of data on a device with limited storage. The network-connected app will not work, however, unless it has an active network connection, and it must provide its location to a server, disclosing potentially private information to obtain the benefits the network connection makes possible. Neither design is inherently better; they involve different balances between privacy and other considerations.

Privacy tradeoffs are particularly common in the advertising industry, since advertising is pervasive in apps for mobile devices and since advertising systems that target users may make more money than ones that don’t. For obvious reasons, advertisers try to target users who are likely to be interested in the goods or services being advertised. There are various ways to do this, with different privacy implications. Historically, ads have been targeted based on the demographics of consumers of a particular medium; for example, ads in *Maxim* target a different set of consumers than ads in *National Geographic*, and ads on *Monday Night Football* are unlikely to be confused with those on *Oprah*. This sort of demographic targeting also works with mobile apps; users who download the Angry Birds app will probably respond to different ads than those who download the *New Yorker*
app. But mobile devices also make it possible to create profiles of *individual* users and target them with relevant ads. As with map apps, there are tradeoffs: targeted ads may be more profitable for advertisers and developers, funding better apps that benefit consumers, and they may prove more relevant and valuable to users than ads targeted using traditional demographic methods. But individually targeted ads come at a privacy cost, since they rely on users’ personal information.

How location information is maintained and secured is also important, since it helps determine the scope of any privacy problem. How long information is kept, where it is kept, who has access, what security measures are used to protect it, and what measures are used to ensure it is accurate can all affect users’ privacy. By minimizing the amount of information that is maintained and applying strong security and fidelity measures, companies can help ensure that location information is not leaked or used in unanticipated or unauthorized ways.

**III. Regulatory Approaches**

To address these privacy issues, some system for protecting users’ privacy — a regulatory system, in the broadest sense of the term — is needed. Such a regulatory system could be left to self-regulation by companies that collect, use, or disseminate location information; regulation by social norms and market pressures, including user demand and negative publicity from consumer groups and the media; regulation by technology measures, including the use of privacy protections or self-help by users; or government regulation by statute, administrative regulation, or judicial decision-making.

Each of these potential regulators could pursue one or more models of privacy regulation. These models fall into three basic categories:

- **Market-promoting regulations** are regulations that promote or facilitate agreements between companies and users concerning the use of location technologies. Such regulations might mandate disclosure when location technologies are used, require opt-in or opt-out consent for uses of location technologies, and/or require privacy audits and reporting. These regulations are agnostic about the location technologies that are used and the purposes for which they are used; instead they aim to ensure there is a meeting of the minds between users and companies on what location technologies are used. Market-promoting regulations are the most common form of privacy regulation in the United States.

- **Substantive regulations** are regulations that impose specific substantive limits on what location technologies can be used and how they are to be used. Such regulations might permit, for example, the use of location technologies for necessary and expected uses or for public uses, while imposing greater restrictions on marketing uses or requiring efforts to minimize data storage and use. Substantive regulations are rarer in the United States than market-promoting
regulations, though they are common in fields with sensitive privacy issues, like health care and financial services.

- Instrumental regulations are regulations that give companies incentives to design location technologies in ways that meet certain goals. Such systems might, for example, impose restrictive safe-harbor rules (e.g., “no use of location technology for marketing purposes”) that a company can escape by demonstrating that users understand how their location information is used, or provide benefits for system designs that retain location information for shorter time periods or store it locally on devices instead of on a centralized server. Instrumental regulations are particularly suited to fields with fast-moving technology, since it can be hard for regulations to keep up. Instrumental regulations are an underexplored avenue for privacy regulation and are rare in the United States, although they have been used in other fields with complex technological problems. For example, makers of electronic voting systems must demonstrate that users will understand a system and be capable of voting accurately, giving manufacturers freedom to design systems to accomplish that purpose.

Because there are so many uses to which location data can be put, so many entities that have access to such data, and such distinct privacy interests at stake in various scenarios, crafting a one-size-fits-all location-privacy rule is likely impossible. Accordingly, regardless of who crafts and enforces the rules, any reasonable approach to location privacy will require a mix of approaches, and the hard part is figuring out which approach is best in each scenario.

IV. The Way Forward

Going back to first principles can help us move forward in determining what regulatory scheme makes sense in any given scenario. In the privacy context, the FTC has set forth five Fair Information Practice Principles that represent widely accepted principles guiding the collection and use of users’ personal information. The principles include:

- **Notice/Awareness:** Users should be made aware of what a business’s information practices are, including what data is collected, the uses to which it will be put, any third-party recipients of the data, the steps taken to ensure security and integrity of the data, and so forth. This disclosure should be clear, understandable, and tailored to the privacy interests at stake.

- **Choice/Consent:** Users should have options about how their personal information is used, and especially about uses that are unnecessary to complete the contemplated transaction. Through opt-out or opt-in consent, users should be able to give consent, or not, for such secondary uses of their personal information.
- **Access/Participation**: Users should have access to data about themselves and be able to contest that data’s accuracy and completeness, so they can ensure the data is accurate and complete.

- **Integrity/Security**: Users should be able to have confidence that their personal information is maintained accurately and securely. Devices and applications that use location information should be secured to prevent unauthorized parties from accessing that information. Similarly, companies should take technological and managerial steps to protect against data mistakes, corruption, and insecurity.

- **Enforcement/Redress**: There should be some mechanism to enforce these principles, whether through self-regulation, a private right of action, or some form of government enforcement.

These principles are akin to market-promoting regulations in that they are largely agnostic on the question of what personal information companies collect, use, and disseminate, and the uses to which they put such information. To these principles we would add a sixth, describing a substantive limitation on the use of location information:

- **Balance**: The benefits of using location information, and the techniques by which the information is used, should be balanced with privacy interests in that location data. Uses that have greater privacy consequences should require greater disclosure, consent, or substantive limits than uses that have minimal privacy consequences. Likewise, uses that are unnecessary to provide products or services may require more disclosure or consent than those that are critical to providing products and services.

We can draw several conclusions from these principles.

First, these principles can help us determine which regulatory model makes the most sense in a given scenario. For instance, some scholars have argued that it may be impossible for users to gain a full understanding of how companies use their location information, especially in the confines of a device with a small screen. If so, then it becomes harder to fulfill the Notice/Awareness principle and ensure a true meeting of the minds between companies and users. As a result, the regulatory system may need to shift away from market-promoting regulations and toward substantive and instrumental regulations.

Likewise, people designing privacy policies often face a choice between opt-in and opt-out rules, which differ based on the default choice. The Notice/Awareness, Choice/Consent, and Balance principles give ways to decide between these rules, based on what the typical user would expect to be necessary and in a way that balances the notice required with the magnitude of the privacy interests at stake. For instance, a use of location data that is necessary and expected to use a service, or one that presents relatively minimal privacy
concerns, may require opt-out consent, while a secondary use with much greater privacy implications may require opt-in consent.

Second, it follows from the Notice/Awareness principle that we should distinguish between uses of location data that are necessary and expected to provide a product or service from those that merely provide business or other benefits to the service provider. When a use is necessary and expected, a certain degree of awareness can be presumed, since a user who deliberately uses the product or service can infer that it will use his or her location data. For instance, it is expected that a wireless device would need to disclose a user's location to provide information about nearby restaurants. But this does not mean that a user will infer that every use of location information is essential and necessary; it would not be expected that a service provider would need to maintain location information indefinitely to provide restaurant recommendations. So that users can understand the uses to which their location information will be put and make informed decisions about whether to use such services, unexpected uses may require a greater degree of disclosure and consent or more privacy-protective default settings.

Likewise, it follows from the Balance principle that we should tailor privacy regulations to the specific information collected, used, or disclosed by a company. Location technologies that use high-resolution location data, or that link location information to personal information, require greater privacy regulation than those that use lower-resolution location data with no links to personal information, since the former involves much greater privacy concerns.

Third, today many uses of location information fail to live up to one or more of these principles:

- Service providers and other wireless-industry stakeholders have violated the Notice/Awareness principle by disclosing only that location information is collected, not the specific uses to which that information is put. System design can exacerbate this problem. For example, Apple’s iOS prompts for consent before an app is permitted to use location information, but provides no information about the purposes for which the information is needed.

- Even when they do disclose the uses to which information will be put, companies have sometimes failed to describe clearly and precisely what data is stored or all the purposes for which that information will be used. For instance, Verizon recently announced that it would use customers’ location information for marketing purposes, but provided minimal details about how the system would work or whether third parties would receive location information. Likewise, it is generally difficult or impossible to know what steps service providers take to anonymize location data.
Companies have violated the Choice/Consent principle by failing to give users choices about how their location data is used. For instance, it is sometimes impossible to use a service without consenting to the use of location data, even when that data is unnecessary to the operation of the service.

Companies have violated the Access/Participation principle by failing to provide access to data the companies maintain about users and failing to provide any avenue to contest the accuracy and completeness of that data. Indeed, companies rarely provide such access without legal compulsion.

Companies have violated the Integrity/Security principle by failing to protect users’ information and by failing to update their software promptly when security flaws become known. For instance, numerous Android phone makers have failed to support older handsets with software updates, including security updates, even when those handsets are still under contract to many purchasers.

Companies have violated the Balance principle by using one-size-fits-all privacy policies that fail to distinguish between uses of location information with greater or lesser privacy consequences, or uses that are more or less necessary.

Given the importance of the privacy interests at stake, and the central role wireless devices play in society today, developing a system of concrete rules to protect location privacy consistent with these principles is a central challenge for industry, government, and users in the coming months and years.