PEOPLE, NOT PLACES

A Policy Framework for Analyzing Location Privacy Issues

Masters Memo Prepared for the Electronic Privacy Information Center

by

James C. White

Candidate – Master of Arts

Terry Sanford Institute of Public Policy

Duke University

Spring 2003

James C. White is currently a Litigation Associate with

Moore & Van Allen.

http://www.mvalaw.com/

SUMMARY

The law has long recognized that there is no reasonable expectation of privacy in a public place. Location-tracking technologies raise important issues that call into question just what expectation of privacy an individual who is in public should have. While one must expect to surrender some privacy in a public space, location surveillance and processing technology has the potential to invade an individual's privacy to such a degree that even maintaining anonymity becomes impossible. To attempt to understand what the reasonable expectation of privacy in the case of location-tracking technology, one can ask these three questions: (1) Would it have been possible to obtain the same information without using the technology in question?; (2) If so, would it have been possible to use the data without additional computer processing?; and (3) If the alternate means of obtaining this information had been employed, or if the additional data processing had been performed, would either have constituted unreasonable surveillance?

All technologies that raise location privacy issues involve three basic location privacy processes: (1) location identification, (2) data processing, and (3) value-added use of the location information. The presence of all three of these characteristics is what distinguishes location privacy issues from other, related privacy issues. Likewise, when one looks at how much choice the subject has had in the use of the technology that is tracking her location, the issues can be placed into one of three categories along a spectrum: (1) active use, in which the individual is a willing participant, (2) passive, which occurs without the individual's knowledge or permission, and (3) flexible, which covers devices whose use has the unintended consequence of tracking location information.

There are three principal active tracking technologies: mobile telephones, automobile-based telematics devices, and the rapidly growing field of "WiFi" Internet devices. Passive technologies include biometric devices, automated methods of recognizing a person based on a physiological or behavioral characteristic, such as surveillance cameras equipped with facial recognition software. Credit cards and supermarket discount cards are examples of flexible technologies.

Location privacy issues arise because of not only the use of this location-tracking technology, but also because of data processing and the value-added use of the location information which data mining provides. Data mining is the search for patterns and trends in existing masses of data. While the value of data mining is apparent, there are two significant limits to its capabilities. First, while the principal value of data mining is its ability to reveal patterns and relationships between data, data mining cannot reveal the value or significance of the data to the user. Second, and perhaps more importantly, data mining sheds no light on issues of causation. While a computer-generated correlation can show relations between location and behavior, it is incapable of revealing the reason behind that relationship.

The Federal Government's largest data-mining project is Total Information Awareness, a division of the Defense Research Projects Agency. Its goal is to identify

terrorists and prevent terrorist attacks by creating the tools that would allow analysts to "data-mine an indefinitely expandable universe of databases." While some have questioned whether it is even possible for TIA to meet its ambitious technological goals, certainly the scope of this data-mining enterprise raises major privacy questions.

Business has embraced "M-Commerce," predicated on the use of location information for the creation of content whose value comes from knowledge of where a user physically is, such as traffic or weather information. Even if one accepts the value of these specific business uses of location information, there are numerous downstream uses of that information that must raise concerns.

Regulators and lawmakers have reacted to growth of these location-tracking technologies in a number of ways. Not surprisingly, cellular telephones, the most heavily regulated of the location-tracking technologies, have attracted the most attention from policy-makers. The E911 initiative, an attempt to create location-based emergency service for cellular telephones by permitting the phones to pinpoint the location of their users, has spurred the development of location-based services. Congress, in the Wireless Communications and Public Safety Act of 1999, explicitly addressed fears that wireless customers, by facing government-imposed mandatory location tracking devices, would be signing away rights to their personal location information. The 10th Circuit's ruling in *U.S. West*, and subsequent actions by the FCC, however, call the effectiveness of these protections into question. The Location Privacy Protection Act of 2001, never enacted, offered broad location privacy protections. Its standards were not limited to existing wireless technology, but rather, it took a technology-neutral approach to privacy issues.

The fundamentals of information privacy protection advanced by the Federal Trade Commission offer a summary of principals to consider when analyzing privacy issues. Although the FTC has not used these criteria specifically in the context of location privacy issues, they provide a useful analytic framework. The FTC's five principals are (1) notice, (2) choice, (3) access, (4) security, and (5) enforcement.

Although this memo focuses on U.S. location privacy issues, it is useful to look at various international standards for privacy protection. Privacy International has identified four major models for privacy protection. In various countries, different combinations of these models are used to offer privacy protection: (1) comprehensive laws that govern the collection, use, and dissemination of personal information by both the government and private sector; (2) sectoral laws governing, for example, videocassette rentals and financial or medical privacy, an approach that tends to offer spotty privacy protection; (3) various forms of self-regulation in which industry adopts codes of self-regulation and engages in self-policing; and (4) technological self-help through methods such as encryption, anonymous remailers, proxy servers and various digital payment methods.

Privacy protection in the United States has tended to focus on protection of the individual from an intrusive government, while in other countries, such as those of the European Union, the emphasis is on protection of personal information from third-party users. The U.S. has taken a more *laissez faire* approach to markets, and regulation is

often avoided unless there is a market failure and government intervention is considered likely to improve matters.

How does one assess the benefit to society of technologies and weigh the countervailing costs of lost privacy? The economic arguments concerning privacy can be reduced to arguments about the existence and alienability of property rights in personal information. By valuing those property rights, and comparing them to an assessment of the cost of privacy regulation to business, they claim, one can assess the relative costs and benefits.

Recommendations:

- Location privacy practices should be technology-neutral, and based on future, rather than current, capabilities of technologies.
- Support creation of an opt-in regime for location information.
- Support the re-introduction of the Location Privacy Information Act.
- Support the enactment of reasonable restrictions on the Government's use of data-mining technologies.
- Urge the FCC to reconsider its refusal to enact location privacy regulation.
- Support the enactment of similar measures on the State level.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF CHARTS

I. INTRODUCTION

It's far, far away and way, way afar,
It's over the moon and the sea,
And wherever you're going, that's wherever you are,
And nobody knows it but me.
- Chevy Tahoe Ad[1]

What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.
- Supreme Court Justice Potter Stewart[2]

In the past decade, the use of wireless services has exploded, with the number of mobile telephone subscribers alone totaling 109.5 million.[3] Because of the federal E911 initiative, each of those phones will soon be capable of offering cellular providers the location of each of their subscribers, sometimes with pinpoint accuracy.[4] GPS-powered telematics devices such as *OnStar*, two-way systems capable of providing drivers with directions as they navigate unknown city streets, are also capable of revealing a driver's location at any time. While it is taking time for these systems to catch on—about half of *OnStar's* customers drop the system in the first year of use—most analysts predict continued growth in the use of telematics, with estimates of nearly six million telematics-equipped vehicles on the road in 2009, up from less than 100,000 in 2001.[5] Cameras at street corners and in sports arenas, some equipped with face-recognition software, scan traffic and crowds, noting the location of unwitting passersby.[6] Credit cards and shoppers' discount cards record buyers' locations as readily as they track purchases.[7] Subway fare cards, toll road "FasTrak" systems and red-light cameras all record the locations of travelers.[8] A growing body of devices and systems continuously keep track of the many places we each pass though on a given day—some operating with our express permission, others with neither our permission nor our knowledge.

The law has long recognized that there is no reasonable expectation of privacy in a public place.[9] And yet, these new location-tracking technologies raise important issues that call into question just what expectation of privacy an individual who is in public should have. While one must expect passersby to watch her walk through a public park, one does not reasonably expect that she will be stalked and followed. Of course one must surrender some privacy in a public space—but location surveillance and processing technology has the potential to invade an individual's privacy to such a degree that even maintaining anonymity becomes impossible.

Most analysis of location privacy issues tends to be technology-specific.[10] And there is good reason for that: Different regulatory bodies oversee different technologies—the Federal Communications Commission ("FCC") currently regulates cellular telephones, but not other wireless devices; the Federal Trade Commission

("FTC") currently regulates telematics and other wireless devices. The uses to which these technologies are put vary widely—cell phone tracking devices are designed to locate accident victims, red-light and security cameras to track law breakers, shoppers' discounts cards to identify buying patterns. And yet, regardless of technology or regulatory body, all location issues raise similar questions. By concentrating on similarities rather than differences, it becomes possible to create a technology-neutral framework for analyzing location privacy. Location privacy issues can be analyzed, not only by the technology employed, but also by the nature of the invaded privacy interest, and by looking at these issues through appropriate filters, such as the FTC's fair information privacy practices, it becomes possible to weigh different technologies that affect location privacy and to effectively assess their impact.

All technologies that raise location privacy issues involve three basic location privacy processes: (1) location identification, (2) data processing, and (3) value-added use of the location information. Part II of this memo argues that the presence of all three of these characteristics is what distinguishes location privacy issues from other, related privacy issues. Likewise, when one looks at how much choice the subject has had in the use of the technology that is tracking her location, the issues can be placed into one of three categories along a spectrum: (1) active use, in which the individual is a willing participant, (2) passive, which occurs without the individual's knowledge or permission, and (3) flexible, which covers devices whose use has the unintended consequence of tracking location information. Isolating these characteristics of location privacy issues also facilitates further analysis of those issues.

Part III provides a factual overview of some of the issues raised by location privacy technology from cellular telephones to red-light cameras, and looks at the impact of data mining on location privacy, while Part IV explores the relevant legal and regulatory environment. Part V is a brief look at selected best practices gleaned from domestic and international examples, and Part VI looks at how to assess a location privacy issue, using the expectation of privacy and the analytical tools discussed above as a guide and, through a series of case studies, looking at how this location privacy framework can help one conduct cost-benefit analyses of potential location privacy problems. The final part of the memo examines the results of this analysis of location privacy issues, and uses it to offer several tentative policy recommendations.

II. A LOCATION PRIVACY POLICY FRAMEWORK

A. The Reasonable Expectation of Privacy

1. Technology and the Expectation of Privacy

In 1967, a Los Angeles man placed bets in Boston and Miami over a public telephone. His calls violated a federal law against using a "wire communication facility" to transmit a wager.[11] Without first obtaining a warrant, the Federal Bureau of Investigation had attached an electronic listening device to the public telephone booth from which the man placed his calls and recorded them, and the conversations were

introduced at trial.[12] In *Katz v. United States*, the Supreme Court threw out the FBI's evidence, holding that the government's eavesdropping was a violation of the privacy which the man should have assumed attached to his conversations, even though the conversations took place in public, and that the eavesdropping constituted a "search and seizure" within the meaning of the Fourth Amendment.[13] Further, the court held that the Fourth Amendment protects "people, not places," and that whatever a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[14]

Katz established a straightforward test—does the individual have "an expectation of privacy that society is prepared to recognize as reasonable."[15] In *Katz*, and in the line of cases which followed, the Supreme Court recognized that the use of technologies capable of violating a person's privacy potentially exceeds that individual's reasonable expectation of privacy in situations where, absent that technology, the expectation would not exist. The Court's recent decision in *Kyllo v. United States* confronted the issue of this transformative nature of technology even more directly.[16] In *Kyllo*, the FBI used heat-sensing technology to discover whether the heat emanating from the walls and roof of a suspected marijuana grower's house was sufficient to indicate the presence of the high-intensity lights necessary for the plant's indoor cultivation. To find the heat, the FBI employed a heat-sensing device, and it used the result of that high-tech search to obtain a warrant. As Justice Scalia framed the question: "[W]hat limits [are] there . . . upon this power of technology to shrink the realm of guaranteed privacy?"[17]

In both *Katz* and *Kyllo*, the Court decided that basic constitutional protections do not disappear in the presence of a new technology.[18] In fact, the *Kyllo* Court spelled out how the *expectation* of privacy can change when one is faced with a new technology.[19] The expectation of privacy one has when in public is certainly not absolute. And yet, there *are* reasonable expectations of privacy one can have even when in a public place. And the presence of technology can alter that expectation. If FBI agents stationed outside Kyllo's house had noticed, say, unusual patterns of melting snow on the roof and sides of the house and from those patterns deduced the presence of heat lamps, Kyllo could not have had a reasonable expectation of privacy. The agents, after all, were in a public place, and it would not have been reasonable for Kyllo to expect his house to remain unseen. Nor would it have been reasonable to expect the FBI agents to refrain from drawing inferences from those things they had observed. Hence, deducing the presence of lamps from patterns in melting snow would have been acceptable. Yet, by using a technological device to enhance their perception, enabling them to "see" things one would not expect to be visible in public, the FBI violated what would have been a reasonable expectation of privacy.

2. The Expectation of Privacy in a Public Place

Neither *Katz* nor *Kyllo* directly addressed the expectation of privacy in a clearly public space. Rather, both concerned the intrusion of new surveillance technologies into the traditionally protected "private sphere." But a well-known case from the late 1960s demonstrates how that expectation of privacy does indeed extend to individuals in public.

After the publication of *Unsafe at Any Speed*, his book skewering the automobile industry, consumer activist Ralph Nader sued General Motors Corporation ("GMC"), charging that the motor giant had invaded his privacy.[20] He complained that, among other things, General Motors had tapped his telephone to gather incriminating information and had hired call girls in an attempt to catch him in a compromising position. He also charged GMC with "keeping him under surveillance in a public space for an unreasonable length of time."[21] This charge was based on the common-law tort of invasion of privacy. That tort, in turn, can be traced to the classic formulation by Warren and Brandeis of a right to privacy as a right to be left alone, with each individual "determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others."[22] The New York Court of Appeals in *Nader* discussed the liability that attaches to one who "unreasonably and seriously interferes with another's interest in not having his affairs known to others."[23] The court recognized that there is a difference between merely observing someone who happens to be in public and invading that person's privacy. Citing the example of someone who tailed Nader into a bank and watched him withdraw cash:

> A person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing. On the other hand, if [Nader] acted in such a way as to reveal that fact to any casual observer, then it may not be said that the appellant intruded into his private sphere.[24]

Clearly there is a pronounced difference between observing, even deliberately following, someone who happens to be in public and "intruding" into one's "private sphere."[25] In *Nader*, the court recognized that an invasion of privacy can happen in public as well as in private. As this memo will discuss, location privacy issues are distinct from other privacy issues because of a confluence of location tracking, data processing, and value-added uses.[26] But *location* issues become *privacy* issues only because of the reasonable expectation one has that her location will not be tracked, stored, and processed without her knowledge. Ralph Nader was kept under surveillance in a public space for an unreasonable length of time. Modern consumers face the very real prospect of being kept under surveillance in public spaces for the entirety of their lives.

3. Reasonable Expectation and Location Privacy

When James Turner rented a car from Acme Rent-a-Car, he signed a contract that had the following two sentences highlighted in bold type as a disclaimer across the top:

> Vehicles driven in excess of posted speed limit will be charged $150 fee per occurrence. All our vehicles are GPS equipped.[27]

This disclaimer, according to Acme, meant that Turner had contracted away any rights he might have had to any information about his location, as well as any information the company could glean about his speed and driving habits. Acme claimed the right to track

Turner and fine him any time the company's tracking device showed that he had violated the speed limit, whether or not the driver received a citation. In Turner's case, Acme billed him $450 for three alleged speeding violations—even though he had received no tickets from Connecticut state troupers, and had not been able to contest the allegations in court.[28] What reasonable expectation of privacy does a person have when renting a car? Surely one does not expect that he has contracted away information about his location and driving habits and permitted that information to be stored, processed and potentially sold to a third party simply because he has entered into a rental agreement with a car agency that contained the sentence "[a]ll our vehicles are GPS equipped."

The reasoning employed by the Court in *Katz* and *Kyllo* sheds some light on how to assess what the reasonable expectation of privacy should be concerning location issues. In both cases, the Court tried to discover what the expectation of privacy would have been absent the use of the technology in question. Therefore, to determine the reasonable expectation of privacy in the case of location-tracking technology, one can ask these three questions: (1) Would it have been possible to obtain the same information without using the technology?; (2) If so, would it have been possible to use the data without additional computer processing?; and (3) If the alternate means of obtaining this information had been employed, or if the additional data processing had been performed, would either have constituted unreasonable surveillance?

Could Acme have gathered the same information about Turner absent GPS technology? Yes, but to get that information Acme would have had to follow Turner throughout the rental period, noting where he went, what he did, and when his car exceeded the speed limit. The second question does not apply if all that Acme intended was to note incidents of speeding. However, if maintaining a complete record of Turner's trip was a goal, possibly to sell that information to another data compiler, or to provide the information to a government anti-terrorism agency,[29] then further processing was indeed necessary. Third, if Acme had assigned an employee to follow Turner for the purpose of determining if and when he was speeding, would that have been, in the words on the *Nader* case, "keeping him under surveillance in a public space for an unreasonable length of time?" The answer to this, most important, question seem to me to be a clear yes.

The introduction of new technologies has lowered the cost of surveillance, and permits practices that might otherwise be ludicrously expensive. As a result, genuinely invasive practices have become cost effective, allowing users such as car rental agencies to achieve comparatively mundane goals such as managing their fleet of rental cars through techniques that severely violate the privacy of their clients. The mere fact that technology is being used to track an individual, however, does not mean that its use necessarily will exceed her reasonable expectation of privacy. For example, if a trucking company such as United Parcel Service ("UPS") employed a system like Acme's on its trucks and used it for identical purposes, the expectation of privacy would be different. Even absent the introduction of this technology, an employee who drove a truck could reasonably expect that her employer would take steps to ensure that she drove a safe speed and that her employer would monitor how and where she drove the truck. The addition of tracking software, while increasing exponentially the employer's ability to

follow its employees, does not exceed the reasonable expectation of privacy of those employees. In the case of a UPS truck, even though the technology involved does raise location privacy issues, its use does not exceed the reasonable expectation of privacy one has with regard to those issues. That is not to say that the use of tracking technology *could not* violate an employee's expectation of privacy—just that the employee's expectation should be different from that of a consumer.

B. Location Privacy Processes

Imagine a typical office worker in a large city. He gets up in the morning and stops on the way to work at a supermarket for a roll and coffee—he has been captured on tape by surveillance cameras, had his shopper's discount card scanned, and paid by credit card; multiple means of tracking his location are in play before his first sip of coffee. He gets on a toll road using a "FasTrak" system to bypass the tollbooth—yet another location noted and stored. A redundant one, it turns out, because his car is equipped with an *OnStar* telematics device, and his location is already being continuously monitored and stored in a computer database. He calls in to work—his cell phone's GPS chip notes his location. Because he's sipping coffee and talking on the phone, he runs a red light—a picture of his license plate is snapped and his location is tracked in yet one more way. It does not take a lot of thought to see that in the course of a single day, the list of potential ways in which an individual's location can be tracked and stored for ready processing quickly becomes very long. Although cell phones, credit cards, and red-light cameras appear to have little in common, each is a potential location tracking device, and each raises potential location privacy issues.

Location privacy has generally been analyzed in a technology-specific way.[30] What are the privacy implications of E911 for cell phone users, one typically asks, or the privacy implications of the use of telematics for drivers? It is useful, however, to look at location privacy issues more abstractly, apart from the individual technology that raises the issues. Each of the technologies in question—such as cell phones, telematics, shopping discount cards—raises a number of privacy issues beyond issues about their user's location. Discount cards and credit cards raise issues about the privacy of financial and personal information; telematics devices issues about the sharing and processing of information concerning one's driving habits. While it is a valid and important exercise to explore a given *technology* and catalog the potential privacy issues it raises, it is also important to view a given privacy *issue* in isolation, and to determine what the characteristics of a particular violation of an individual's privacy are when viewed apart from a given technology. Looking at privacy issues in this abstracted way offers a new perspective on the issues, facilitates the creation of analytic tools, and is an important step in crafting policy solutions.

To analyze location privacy issues, it is first necessary to identify the characteristics of privacy issues generally, and to see what about location issues make them different from other, more general, privacy issues.

1. The Nature of Privacy

Privacy has been defined in several ways.[31] Definitions have included:

- A right involving personal control over disclosure of information:
  - A person's right to information about herself, ranging from their address to health and financial records;
  - Confidentiality, a right to protect "secrets;"
  - Anonymity, a right to conduct transactions without identifying oneself.
- Certain rights pertaining to personal safety and security:
  - A right to bar intrusion into personal space, both in private and, as the *Nader* case demonstrates, in public as well;
  - A right to guard against the misuse or appropriation of personal information, as for example in the case of identity theft.
- Perhaps the broadest definition equates personal information with property, granting personal information the same property rights accorded physical property.

Analysis of privacy issues is difficult because of this murkiness of definition. Just what a right to privacy consists of is not clear, in part, because of the tenuous constitutional basis for such a right. While there is no explicit constitutional right to privacy, the Supreme Court has recognized the existence of such a right in the "shadows" of the First, Third, Fourth, Fifth, and Ninth Amendments.[32] There are conflicts between an absolute right to information privacy and First Amendment free speech protection,[33] and it has not been established that, even if one has a right to privacy vis-à-vis the government, that right extends to private interactions.[34]

Nonetheless, consumers have demonstrated that they place a financial value on the protection of personal information. Fifty-five percent of California residents pay telephone companies additional fees to have unlisted phone numbers, as do twenty-four percent of New Yorkers.[35] Privacy fears can affect consumer buying patterns. One survey reported that 92% of consumers are concerned, and 67% very concerned, about misuse of their personal information online.[36] Another survey showed that 48% of consumers who are "very concerned" about privacy do not shop online.[37] Congress has acted on this concern, on numerous occasions acting to protect personal information.[38] Interestingly, though, despite the stronger constitutional basis for protection against *government* violation of a right to privacy, Americans seem more concerned about potential abuses by *businesses* than potential governmental oppression.[39]

These conflicts, particularly disputes about First Amendment rights in the personal information gathered by a business about its customers[40] and about whether rights to privacy in the context of government activities extend to private transactions, must be taken into account by any framework that is drafted to deal with location privacy issues. These views of a right to privacy each allow for potential concerns about location issues: concerns about personal control over disclosure of one's location information,

concerns about personal safety and security, and issues about ownership rights in the information gathered. Location privacy issues are certainly *privacy* issues, but they are also *location* privacy issues, with characteristics that distinguish them from related privacy concerns.

2. What Makes Location Issues Different?

All information privacy issues in some way involve the gathering of personal information by a third party, some processing of that data, and some potential or actual use of that data. Like other information privacy issues, location privacy issues can be viewed as a series of processes. For location privacy, the three processes are: (1) location identification, (2) data processing, and (3) value-added use of the location information. Viewed together, these three processes offer a way to distinguish location privacy issues from other potential violations of an individual's privacy. Looking at each of them:

(1) *Location Identification*—All location technologies identify an individual and pinpoint her location. That location could be continuously tracked, such as the GPS signal transmitted by a telematics device in a car, or it could be captured in a one-shot transaction, such as the time-stamped photo produced by a red-light camera or the record created by a credit card or shoppers discount card transaction.

(2) *Data processing*—Once an individual's location has been identified, that location information must be stored in a way that would allow the information to be processed. The processing need not be substantial, although "data mining" can greatly increase the value of the processed data.

(3) *Value-added use*—There must either be an actual or potential "value-added" use for the location information that has been gathered—for example, E911 cell phone location technology is used to find callers in emergencies, or red-light cameras are used to track speeders. Again, there are often many value-added uses, and sometimes they are difficult for a user of the technology to anticipate.

The processes involved in location privacy issues, while similar to those involved in other, related, privacy issues are distinct enough that the presence of these three issues identifies a particular privacy issue as a location privacy issue.

TABLE 1.: IDENTIFYING LOCATION PRIVACY ISSUES

	Cell Phones	**Red-light Cameras**	**Compiling Personal Genetic Information**	**Web Browser Cookies**
Location Identification	Yes	Yes	No	No
Data Processing	Yes	Yes	Yes	Yes
Value-Added Use	Yes	Yes	Yes	Yes
Location Privacy Issue?	**Yes**	**Yes**	**No**	**No**

Table One looks at four important privacy issues, two of which are location-related, two of which are not. Because of E911 regulations, cellular telephones pinpoint a user's location, compile that information into a form that can be processed, and offer numerous potential value-added uses for that information—from rescue in the event of an accident to targeted, location-based advertisements. The gathering of personal genetic information, on the other hand, while allowing the compiling of information in a form that permits processing of the data and offering a number of sobering value-added uses, does not identify an individual and pinpoint her location. Therefore, while cell phones raise location privacy issues, the use of personal genetic information does not. Likewise, red-light cameras fit the categories of identification, processing and value-added use, while web browser cookies do not. The cookies track a user's activities in cyberspace, and can identify what *computer* a user employs, but the cookie makes no effort to pinpoint the *physical location* of that user. So, red-light cameras raise location privacy issues, and cookies do not.

3. The Significance of a Process-Based Approach

Each of the three process categories presents a distinct set of problems, and by viewing them in isolation, it becomes possible to assess the implications of each set of problems more accurately.

TABLE 2.: PROCESS-RELATED LOCATION PRIVACY ISSUES

	1. Location Identification	2. Data Processing	3. Value-Added Uses
Characteristics	All location technologies pinpoint the location of an individual.	This ability to process combine location information, discerning patterns, or combining location data with information gathered from other sources through "data mining"	The use of location information for purpose beyond simply allowing the user to identify where she is at a given point in time
Issues Raised	consumer choice, opt-in, opt-out, anonymity	consumer choice, opt-in, opt-out, use by advertisers, employers, use in court	security, advertising, location of user in emergencies, tracking of terrorists and criminals, sale to other data providers

Table Two shows that each phase of the location privacy process raises distinct issues, some of which are common to different privacy issues, some of which are unique to location privacy. For example, while many privacy issues involve questions of consumer choice and their ability to opt-in or opt-out of the use of their personal information, other issues such as location-based spamming are unique to location technologies. Viewing these issues in isolation facilitates the further analysis of them. It is also useful to explore the degree of active participation the user had in the deployment of the location-tracking device.

C. The Spectrum of User Choice

Once it is clear that an issue is location privacy related—it identifies an individual and pinpoints her location, that location information is stored in a way that would allow the information to be processed, and there are value-added uses of the information—it is helpful to next determine the degree to which the user has chosen to have his location information tracked and processed. While some tracking devices work with the full consent of the user, others could be employed without her choice, sometimes even without her knowledge. Although the degree of individual consent varies, there are three basic categories of user choice: (1) active use, in which the individual is a willing participant, (2) passive, which occurs without the individual's knowledge or permission, and (3) flexible, which covers devices whose use has the unintended consequence of tracking the user's location information.

TABLE 3.: THE USER CHOICE SPECTRUM

	Active Location Tracking Devices	**Passive Location Tracking Devices**	**Flexible Location Tracking Devices**
Element of Choice (as location device)?	YES	NO	SOME
One of the technology's purposes is location tracking	YES	YES	NO
Use of the technology is voluntary	YES	NO	YES
Examples	- cell phones - telematics	- security cameras	- credit cards - shoppers cards - driver's license

The key factor that differentiates active and passive location-tracking devices is consumer choice. Table Three shows the basic choice characteristics of active, passive and flexible devices. Whether of not a given technology is active, passive or flexible can be determined by answering two questions: (1) Is one of the primary purposes of the technology location tracking?; and (2) Is the technology being used voluntarily? Active technologies such as cell phones could be considered location-tracking devices whose purpose is to track the user's location and which are used voluntarily. Passive technologies like security cameras, while designed for tracking, are not employed voluntarily. Flexible technologies such as credit cards, however, while not necessarily designed for location tracking, are used voluntarily by consumers.

Table Four shows that at different points in the location privacy process, for example, the same location-tracking device can be passive, active or flexible.

TABLE 4.: USER CHOICE GRID

	Active Location Tracking	Passive Location Tracking	Flexible Location Tracking
Location Information →	A user can clearly opt to have their location noted, e.g. cell phone E911...	...without consenting to downstream uses of that data...	... particularly in the case of unintended tracking devices such as credit cards.
Data Processing →	A user can consent to have their location data processed, e.g. a user of a telematics device allowing the use of their data to provide directions to restaurants or shops...	... without consenting to having their data "mined" and combined with other databases of personal information...	... particularly in the case of unintended tracking devices such as credit cards.
Value-Added Uses →	A user can opt in to one value-added use....	... without granting consent for additional uses...	... particularly in the case of unintended tracking devices such as credit cards.

Examinations of location privacy issues have tended to focus on active devices. However, both passive and flexible devices raise the same location-tracking issues. And any location privacy policy that does not include passive and flexible devices will fail to adequately address broader location privacy issues. The next Part of this memo offers a factual overview of location-tracking devices across the user choice spectrum, looking at both the nature of these technologies and some of the issues raised by the use of these technologies.

III. TECHNOLOGIES

According to Moore's law, computing power doubles every eighteen months. Dan Farmer and Charles Mann recently described out the implications of this theory on the ability to monitor individuals:

> [B]y 2023, large organizations will be able to devote the equivalent of a contemporary PC to monitoring every single one of the 330 million people who will then be living in the United States.[41]

Because the potential location-tracking capability of future technologies is nearly limitless, it is essential both to understand the current state of location-tracking technology and to recognize how these technologies will develop. This Part describes the principal active, passive, and flexible technologies, and their characteristics and potential for growth. Although one tends to associate location privacy issues with wireless technologies, other land-based technologies such as surveillance cameras, even credit cards are part of the web of devices which track and individual's privacy.

The second section of this Part explores the issue of data mining. Understanding the implications of data mining is essential to an understanding of location privacy, since location privacy issues involve not only location identification, but also the data processing and value-added use of the location information which data mining provides.

A. Location-Tracking Technologies

1. Active Tracking Devices

Mobile wireless communications devices are a fast-growing business—by 2006, the worldwide market for location-based services is expected to be almost $40 Billion.[42] While wireless telephones are the most common active tracking technology currently in use, other potential uses of wireless communications are experiencing rapid growth. As I described above, active location-tracking technologies are location-tracking devices that the user employs voluntarily which can track the user's location . This section offers a brief look at three principal active tracking devices: mobile telephones, automobile-based telematics devices, and the rapidly growing field of "WiFi" Internet devices.

a) Mobile Telephones

Until recently, the principal privacy concern of cellular telephone subscribers was the fear of the interception and monitoring of conversations. While traditional landline calls can be traced in an emergency, cellular and PCS calls cannot, and concerns about the ability to locate cellular callers in emergencies have driven the creation of location-tracking capabilities for mobile telephones. Business or government could certainly use this system, designed for emergencies, for very different purposes. A principal fear of privacy groups is that once GPS and other tracking systems are common in mobile phones, the information gathered about individuals will be stored and possibly sold without their knowledge. Once personal information has been stored, it could possibly be used by police for law enforcement purposes, unearthed by a private investigator digging up dirt on a cheating spouse, or perhaps even become the consumer equivalent of the airlines' "black boxes," used to verify a driver's actions after an automobile accident.[43] Even if information is only retained and stored on an individual's handset, theft of that handset would yield invaluable information about that individual's activities.[44] This presents the possibility of two dystopian visions of a wireless future, one in which cell phone users are besieged by an endless barrage of carefully tailored, location-based Spam, and another in which the government keeps constant and indiscriminate track of its citizens.[45] Data mining, or the search for new knowledge derived from existing masses of data, raises further concerns.[46]

b) Telematics Devices

Telematics devices have been described as the marriage of two American obsessions—automobiles and wireless communications.[47] There are two principal uses of telematics devices: by consumers, to deal with safety and security concerns, and by businesses, to manage fleets of trucks or rental cars. The leading consumer telematics device is *OnStar*, a system designed by General Motors, installed on GM, Toyota and

Honda cars. Its principal competitor is ATX, used by Mercedes-Benz and Ford.[48] Unlike the use of location information in cellular phones, which is driven by the federal E911 initiative and resulting regulations, the production of these safety devices is market-driven.

Although cellular telephones were originally devices designed to be installed in automobiles, they have experienced their greatest growth after becoming freestanding communications devices. The strongest argument for the use of telematics devices in automobiles is as a safety device, a way to communicate with drivers in the event of accidents, or a way to provide direction information to lost and nervous travelers, maybe even a way to tell an injured person the fastest route to a hospital. But, it is difficult to sell consumers an expensive embedded technology for safety reasons alone when those same consumers already carry cell phones and PDAs. Selling consumers expensive embedded safety devices that they hope will never be used is just not a sustainable business model.[49] Manufacturers, who gain the opportunity to maintain a relationship with consumers after the vehicle is sold and potentially gather important information about how the vehicle is being used, have the major advantage from the use of the devices.[50] It is not clear that there is genuine consumer demand for these products—while the growth of most wireless devices has exceeded expectations, the growth of telematics devices has been much slower than imagined. But because of the general growth in the use of wireless communications, some form of wireless telematics is likely to catch on. Embedded wireless devices in automobiles could become voice-driven pieces of the wireless web of devices an individual uses, including cellular telephones and the Internet, and perhaps through the use of something like the Bluetooth technology described in the next section, telematics hook-ups could allow cars to become rolling "nodes," and part of the growing telematics market.[51]

Growth in business use of telematics for fleet management, on the other hand, has been steady. Commercial users were the first to employ telematics, initially as simple communications and tracking systems, currently as pieces of elaborate database applications.[52] These systems certainly can introduce efficiencies, for example linked when linked with a bar coding system location tracking can provide real-time monitoring of freight as it moves.[53] But they also offer companies the ability to monitor drivers, and raise privacy concerns about the point at which an employer's monitoring crosses the line and becomes invasive. These systems might also expose trucking companies to increased liability, since the failure to react to telematics data indicating driver recklessness could be considered recklessness on the part of the trucking company. In the case of a rental car company, such monitoring of vehicles raises even clearer privacy concerns.[54]

Currently, telematics exist in a regulatory no man's land. Since the wireless devices do not meet the current definitions of mobile telephones, they are not within the FCC's regulatory sphere. Although both the Automobile Association of America and the Cellular Telecommunications & Internet Association have asked the FCC to regulate the nascent industry, and the proposed Location Privacy Protection Act of 2001 mandated regulation of the industry, so far the commission has refused to regulate telematics.[55]

c) WiFi, Bluetooth, and Other Technologies

WiFi and Bluetooth are both wireless means of accessing the Internet. WiFi is a wireless networking standard that allows the creation of small, wireless networks. A WiFi network could be used, for example, to network a group of home computers or a small business, allowing file sharing and shared Internet access. A growing use of WiFi, however, is the creation of wireless public access points. These "hot spots" are springing up across the country, in coffee shops, hotels, stores, and airports. Some are free, community-based networks, others subscription systems.[56] Bluetooth uses similar technology for a different purpose. It is a cable-replacement technology with a thirty-foot range. Its limited range makes it similar to a cordless phone one might use within one's home. The ultimate purpose of Bluetooth is to provide interconnection between a wide variety of devices—mobile telephones, PDAs, laptops, even Internet-ready air conditioners or washing machines.[57] Both WiFi and Bluetooth present location privacy issues, since once wireless access to the Internet becomes readily available, once the access points a user employs become easy to identify, it becomes possible to use the Internet to track the location of mobile users.

2. Passive Tracking Devices

Discussions of location privacy have tended to focus on concerns associated with wireless location privacy technologies. Other devices, however, have the unintended consequence of tracking one's location information without his permission. Surveillance cameras, which can be coupled with facial recognition software to track the movements of individuals, or mounted at intersections to record the license numbers of speeders, can facilitate the creation of location databases that, through data mining, could offer violations of an individual's privacy every bit as severe as those presented by wireless devices. There are currently more than eleven million surveillance cameras in use in the United States, and one criminologist has estimated that the average person in London is filmed by more than 300 cameras per day.[58]

a) Biometrics

"Biometrics" is shorthand for a variety of automated methods of recognizing a person based on a physiological or behavioral characteristic. Any number of features could be measured: face, fingerprints, hand geometry, handwriting, iris, retina, vein, voice, even brain waves.[59] In the wake of the terrorist attacks of September 11, 2001, biometric technologies are becoming the basis for a range of identification and security applications, and biometric indicators embedded in "smart cards" may ultimately be part of a national identification system. When coupled with random surveillance of citizens, biometrics can drive a powerful system for the collection of location information. For example, each person who attended Super Bowl XXXV had his or her face scanned as he or she entered the sports arena. Algorithms measured their facial features and created a "face print," which was then compared with a database of known criminals and terrorists.[60] Although the purpose of this screening was the detection of terrorists, a valid goal in our uneasy society, the effect was the creation of a database that contained location information on thousands of people.[61] And unlike the information gathered by traditional surveillance cameras, which would remain fixed on individual videotapes and

have to be reviewed before an individual could be identified, the facial recognition software helped to create a database ready for combination with other data.

Despite their somewhat ominous name, we use "biometric identifiers" every day, recognizing someone by processing the sound of her voice or the color of her eyes. But the use of sophisticated technology raises questions about the amount and quality of data that can be gathered, and the type of processing that data can be put through. The use of biometrics raises the same basic questions as other technologies discussed in this memo: When does the use of technology facilitate an unreasonable invasion of personal privacy? As the ability to use technology to track and identify individuals increases, what expectation of privacy is it reasonable for one to have? One admittedly bizarre recent news report told of the adaptation of NASA brainwave technology to scan for passengers who might pose a threat.[62] Although "mind-reading" is not at this point technically feasible, it is in many ways the logical extension of the gathering and processing of biometric data.

b) Red-light Cameras and Other Technologies

Nearly any technology designed for tracking location and providing information in a readily processed form raises location privacy issues. For example, many localities have installed cameras at red lights to catch speeders. Advocates argue that red-light cameras are "a legal, necessary and effective safety measure . . . that . . . constitute[s] no new infringement of people's liberties because running red lights has always been against the law."[63] Those advocates' strongest argument is that, under the Fourth Amendment, one should not have a reasonable expectation of privacy when a red-light camera photographs his license plate because there is probable cause for a search, and because there is no expectation of privacy in a public place.[64] Others might argue that the very use of these cameras raise due process concerns. Regardless, even though it is reasonable for someone who runs a red light to expect to be caught, as with other location privacy issues, it is not reasonable for him to expect that his *location* could be stored, tracked, and processed after he has passed one of these cameras—the location information survives whether or not the driver proves guilty of the infraction.

In Massachusetts, this technology is being used to monitor traffic patterns. Every car that crosses the Calvin Coolidge Memorial Bridge near Boston has its license plate photographed by high-resolution cameras twice—once when it enters the bridge, once when it leaves. A computer uses character-recognition software to read the license plate at both ends of the bridge; and it uses the information to compile the average time it takes for a car to cross the bridge at different times of the day. While, because of concerns about privacy and potential liability the information is not stored, nothing would prevent the company administering the project from storing and reselling the data.[65]

3. Flexible Tracking Devices

"Flexible" is a term that covers devices used with an individual's permission that have the unintended consequence of tracking that user's location and stores it in a form capable of data processing. Credit cards and supermarket discount cards are obvious examples, but there are others. One private direct-debit toll system, for example, not only

collects data at toll booths, but also simultaneously reports data about individual vehicles gathered by radio transmitters hidden in traffic signs.[66] This example highlights perhaps the most important location privacy issue that these "flexible" devices raise. Despite their use with an individual's permission, once a secondary use exists, a use that *does* violate an individual's privacy without the user's knowledge, will providers refrain from making use of it?

* * *

The next section explores the issue of data mining. This is of particular importance because location privacy issues arise not only because of location identification, but also because of data processing and the value-added use of the location information which data mining provides. It will also explore the distinctions between government uses of this information, such as the massive data-mining operation called Total Information Awareness, and business uses of location technology, so-called "M-Commerce."

B. Data Mining and Location Data Policy

Data mining is the search for patterns and trends in existing masses of data.[67] Traditional information retrieval extracts information recorded in the individual fields of a database. A traditional search, then, is "explicit," since the results of a query are precisely the records that had always been attached to a particular entry in the database. Data mining is different; it is a search of bodies of data for patterns that most likely were not apparent before the search. A data-mining search, then, is "not explicit;" rather it is an attempt to create value-added end products from existing data.[68]

It is this distinction between the explicit, traditional data base searches that produce uninterpreted data, and the non-explicit, the use of computing power to link data in a way that creates new inferences, that raises privacy issues. Again, it is useful to think back to the expectation of privacy, and in particular to the view articulated in *Nader*—the stalker versus the watcher. The privacy question raised by data mining is this: Is there a point at which data that would not in itself receive privacy protection become protectable because the use of technology has altered the reasonable expectation of privacy.

Although *Kyllo* and *Katz* recognize the power of technology to alter one's expectation of privacy, the law currently appears to view data mining in a different light. The Supreme Court case that seems most on point is *Smith v. Maryland*.[69] In *Smith*, the Court held that the use of a pen register—a device that recorded the phone number called from a telephone without recording the content of the conversation—was not a "search" within the meaning of the Fourth Amendment, and did not require the use of a warrant. The court applied the *Katz* test: Did the individual exhibit an actual expectation of privacy and was that expectation reasonable?[70] An individual dialing a telephone is not considered to have any expectation of privacy regarding the telephone numbers she dials, since she knows that the numbers are being conveyed to the telephone company, and that the telephone company may well record those numbers for various reasons.[71] And, the

act of using her home telephone only evidenced an interest in keeping the content of the conversation private, not the number itself.[72] More importantly, the Court held that, even if the individual had an expectation of privacy, that expectation was not reasonable, because by exposing the number to the telephone company, he assumed the risk that the number would be turned over to the police.[73]

The importance of the decision lies in its refusal to recognize the power of data interconnection. A telephone number is public information, and as such is not protected. But the significance of the pen register is not that it records this unprotected number. The significance lies in the connection that the register creates between the caller and the number dialed. And it is that connection that the Court refused to recognize as worthy of protection.

While the value of data mining is apparent, there are two significant limits to its capabilities. First, while the principal value of data mining is its ability to reveal patterns and relationships between data, data mining cannot reveal the value or significance of the data to the user. Second, and perhaps more importantly, data mining sheds no light on issues of causation. While a computer-generated correlation can show that there is a relationship between location and behavior, it is incapable of revealing the reason behind that relationship.[74]

1. Government Use of Data Mining

Fundamentally, constitutional rights protect individuals from an overly intrusive government. However, once private companies have gathered personal information about an individual, there is no comprehensive federal law that prevents the government from using that data. And there is no protection from government use of otherwise publicly available information. The FBI and local police departments already routinely use tools such as credit reports for data analysis when tracking and investigating criminals.[75]

Due process plays no role in the gathering and processing of one's personal information. Technology is blind—pen registers only record numbers. Captured telephone numbers themselves have no inherent value. The value comes from the inferences that may be drawn from them, the connection between captured numbers and other databases—information that creates a link between the caller and the call.

Technology may well be blind—but it is not fool proof. Systems designed to identify and track individuals make mistakes. One digit misread, and the wrong license plate goes into the database. Facial recognition software misreads a feature, and evidence that you were somewhere you have never been enters your profile. The Congressional Research Service has estimated that under a government data-mining scheme, a conservative estimate of ratio of false terrorist suspects to actual terrorist suspects found by the system to be 200 to 1.[76]

a) The USA PATRIOT Act

One of the most profound responses to the September 11th terrorist attacks was the passage of the USA PATRIOT Act.[77] The act amended over fifteen statutes, and was introduced without a House, Senate, or conference report, and with little debate.[78]

Although many of the Act's sections raise a large number of privacy concerns, some particular sections raise concerns about information privacy:[79]

- Section 210 expands the information available to law enforcement officials about subscribers to electronic communications services. The section allows for government access to information including temporarily assigned Internet addresses, and could possibly be used as justification for disclosure of gathered and processed location information.
- Sections 214 and 216 of the Act authorizes government agents to capture information from "trap and trace" devices and pen registers for information other than telephone calls—such as captured location information. Before the enactment of the Act, such use was limited to facilities used by foreign agents.
- Court orders authorizing these warrants are executed on a national level.
- Section 217 makes "cybercrime" a federal terrorist offense and allows the government to intercept electronic communications of intruders to electronic systems without a warrant.

b) Total Information Awareness

Total Information Awareness ("TIA") is a government data-mining project designed and managed by John Poindexter, one of the architects of the Iran-Contra affair.[80] TIA is a division of the Defense Research Projects Agency ("DARPA"), which has three components: the machine translation of languages; data search and pattern recognition; and advanced decision support. Its goal is to identify terrorists and prevent terrorist attacks by creating the tools that would allow analysts to "data-mine an indefinitely expandable universe of databases."[81] While some have questioned whether it is even possible for TIA to meet its ambitious technological goals,[82] certainly the scope of this data-mining enterprise raises major privacy questions. First, it authorizes the creation by the government of vast dossiers on innocent citizens, and second, risks mis-identifying large numbers of innocent individuals as potential terrorists.[83]

The government has already gathered large amounts of information about citizens. The Social Security Number, created in 1943 as account numbers for the "old age insurance" established by the Roosevelt administrations slowly became a de facto national identification number.[84] Government databases track individuals' labor, medical, education, and financial information.[85] TIA's goal is to merge these existing databases with retail, educational, travel, telephone, biometric, and even DNA information to create a vast database that will profile every American citizen and every foreigner with U.S. contacts.[86] While the stated goal of TIA is to "detect, classify and identify foreign terrorists" to "defeat terrorist acts,"[87] as with any data-mining regime,

absent controls TIA profiles can be used for whatever purpose the government might devise. And in light of the abuses of the 1960s and 1970s, when civil rights and anti-war groups were a focus of the FBI's counterintelligence program, this broad expansion of government power must give one pause.[88]

2. Business Use of Location Data and Data Mining

Marketers have latched onto the freedom inherent in the concept of wireless communication devices.[89] Wireless users are free—using phones free of cords that bind them to a particular location, free of the need to communicate from a particular location. But that freedom from a *particular* location has a cost—the possibility that one must give up the ability to communicate from *any* location without disclosing that location to the wireless provider, allowing processing of that location information and further downstream uses.

Mobile commerce, called "M-Commerce," describes transactions conducted via wireless devices that allow customers to "buy anything, anywhere."[90] Others call these transactions by a name that more accurately describes the value of the information gathered—"L-Commerce" or location-based commerce.[91] M-Commerce is predicated on the use of location information for the creation of content whose value comes from knowledge of where a user physically is, such as traffic or weather information.[92] With the rapidly increasing popularity of customized Web portals based on a user's interests and preferences, such as my Yahoo or my AOL, the sale of customized information based on a user's location is a logical next step. But, even if one accepts the value of these specific business uses of location information, the numerous downstream uses of that information that must raise concerns.

DoubleClick is an online advertising company that places third-party advertisements on thousands of web sites. When a consumer accesses the web site of one of DoubleClick's clients, the advertising company places a "cookie," an electronic tag that follows users around the web, on the user's hard drive. DoubleClick uses the information it gathers to create detailed, but anonymous, Internet profiles.[93] The company's revenue comes from its ability to use those profiles to "help marketers deliver the right message, to the right person, at the right time, while allowing Web publishers to maximize their revenue and build their business in the process."[94] In 1999, DoubleClick announced its acquisition of Abacus Direct, a direct mail company that compiles a large database of personally identifiable information, and its intention to merge its vast anonymous database with that of Abacus Direct. A huge uproar ensued, followed by investigations by the FTC and states attorneys general.[95] Ultimately, DoubleClick entered into an agreement with ten states to maintain the anonymity of its information, give consumers access to compiled profiles, and give consumers the ability to opt-out of its Internet tracking service.[96]

The DoubleClick/Abacus controversy highlights some of the potential problems with the business use of data mining to process location information. Virgin Mobile, a wireless provider in the U.K. admitted in October 2001 that it had been tracking the location of its users without their knowledge and storing that information in a database.[97]

Such information, like DoubleClick's information, could easily be combined with databases of consumer preferences, or with medical or financial information for marketing purposes. Location information could add an important piece to such a data profile, and policy-makers must be aware of the implications of its use.

IV. THE LEGAL AND REGULATORY ENVIRONMENT

Regulators and lawmakers have reacted to growth of these location-tracking technologies in a number of ways. Not surprisingly, cellular telephones, the most heavily regulated of the location-tracking technologies, have attracted the most attention from policy-makers. This Part focuses on law and regulatory environment in which mobile phones and other location-tracking devices operate. It also looks at the as-yet-un-passed Location Privacy Protection Act, which, notably, proposed a technology-neutral approach to location privacy issues.

A. Enhanced 911 Initiative

While the idea of access to emergency services through a single, universal telephone code was first introduced in Great Britain in 1937, it took until the late 1960s for the idea to be implemented in the United States.[98] The use of emergency 911 service grew rapidly, until today almost 90% of American landline phones have access to it.[99] The terrorist attacks of September 11, during which people buried under piles of rubble called rescuers from cellular telephones that were unable to provide information about the caller's location, highlighted the need for location-based, or enhanced, 911 service for U.S. cellular telephones.[100] Most traditional, landline 911 callers are identified through a two-step process. Calls are made to an emergency center called a Public Safety Answering Point ("PSAP"), where the caller's telephone number is identified through Automatic Numbering Identification ("ANI"), and the caller's location is pinpointed through Automatic Location Identification ("ALI"). In the case of a landline call, ALI typically involves comparing a caller's phone number with a database of telephone numbers and addresses.[101]

To create universal mobile 911 service, emergency calls from wireless phones need to emulate the two key characteristics of their landline equivalents. First, wireless 911 service will have to be uniform and universal. No matter where a caller is, and no matter what handset she uses, she must be able to reach a PSAP. Second, the PSAP must be able to pinpoint the wireless caller's location, whether or not she is able to communicate it to them. This is arguably even more important for mobile callers than landline callers, since a stranded motorist or a person trapped in the ruins of a collapsed building may have no idea where she is when she calls, while a landline caller who is able to speak will often know the address of his phone's location.

The Wireless Communications and Public Safety Act of 1999[102] was a substantial step toward universal 911 service. In 1999, the FCC began to implement the act by adopting rules creating a special method for processing 911 calls. All handsets manufactured after February 3, 2000 must allow 911 calls to be routed to any available

provider rather than to the customer's preferred service provider. And, as of August 29, 2000, all service providers are required to route calls to a PSAP regardless of whether the call was originated by one of their subscribers.

The second goal, identification of the caller's location, has been more difficult to achieve. Mobile phones, unlike landline equivalents, by definition have no fixed location. Finding the location of a caller requires a changing the technology of existing phones. In 1996, the FCC established a two-part plan to enable wireless carriers to provide location information for 911 callers. Phase I involved the creation of the wireless equivalent of ANI, and required wireless carriers to locate the base station or cell site though which a 911 call was made. Phase II creates the wireless equivalent of ALI, and requires wireless companies to pinpoint the location of callers.[103]

Phase I required carriers to supply PSAPs with the telephone number of the originators of all emergency calls by April 1, 1998, or within six months of a request by the designated PSAP, whichever comes later. Phase I regulations also required mobile services to provide the location of the tower from which a call originated.[104] This information could help emergency workers narrow the possible location of a call's origin, since the coverage of a cellular tower ranges from a few floors of an office building to ten square miles.[105]

Phase II is more ambitious, and would bring a wireless service's caller-location capabilities in line with those of landline local exchange companies. It requires wireless companies to identify the location of a caller to within a few hundred feet. When the regulation was originally implemented, the dominant technology was network-based, and necessitated the use of triangulation to locate callers. The decreased costs of Global Positioning Satellite-based ("GPS") systems, however, have made handset-based location technology a feasible and more precise alternative in many situations.[106] Companies have begun to roll out systems that either employ one of these techniques or rely on a hybrid of them, with full deployment mandated by 2005.[107] However, this deployment has consistently been far slower than planned. As FCC Commissioners Kathleen Abernathy and Jonathan Adelstein recently said in Congressional hearings:

> In hindsight, wireless carriers and their vendors may not have fully appreciated the difficulties in deploying such a new, but important, technology. All parties have been frustrated by unforeseen obstacles . . . .[108]

The FCC has granted every major wireless carrier's waiver request, and no wireless carrier is currently capable of accurately locating callers in the way that Phase II requires.[109]

B. Wireless Communications and Public Safety Act of 1999

The Wireless Communications and Public Safety Act was the enabling legislation for the E911 initiative. As its preface states, the purpose of the act was:

> To promote and enhance public safety through the use of 9-1-1 as the universal emergency assistance number, further deployment of wireless 9-1-1 service, support of States in upgrading 9-1-1 capabilities and related functions, encouragement of construction and operation of seamless, ubiquitous, and reliable networks for personal wireless services, and for other purposes.[110]

The Act had broad support, and passed both the Senate and the House unanimously. Most of its provisions related to the establishment of E911 service, and established the parameters within which the FCC was to operate in creating this service. It granted wireless service providers similar protection from liability in emergencies to that enjoyed by landline telephone companies and mandated the creation of universal wireless emergency service. But the Act also took steps to protect consumer information by modifying 47 U.S.C. § 222 to explicitly address fears that wireless customers, by facing government-imposed mandatory location tracking devices, would not be signing away rights to their personal location information:

> [W]ithout the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to call location information concerning the user of a commercial mobile service . . . .[111]

1. Section 222 and the Protection of Consumer Privacy

Section 222 is entitled "Privacy of Consumer Information," and offers several broad protections for the privacy of users, not only of wireless telephones, but also of other telecommunications devices:

- In general, all telecommunication carriers have a duty to protect the confidentiality of the proprietary information of its customers;
- Any information a carrier receives from another carrier must be kept confidential and may not be used for marketing purposes;
- Unless a customer approves, or unless the law requires disclosure, a telecommunications company may not use, disclose, or permit access to "individually identifiable customer proprietary network information" except in the provision of its telecommunications services;
- The authorized uses of this information are:
    - Providing services, including telemarketing information authorized by the customer,
    - Sale of subscriber list information to any person for the purpose of publishing directories,
    - Provision of location information for emergency services.

Despite Congress' clear intent to protect consumer information, the Court of Appeals for the Tenth Circuit decided in *U.S. West v. FCC* that the privacy protections had unconstitutionally constrained the First Amendment rights of telecom companies, and the court invalidated the provisions of the act which granted consumers default protection of their personal information.[112]

2. US West v. FCC—*Section 222 and the First Amendment*

In *U.S. West v. FCC*, the Tenth Circuit found that Section 222's default protection of consumer information violated the First Amendment's freedom of speech protections.[113] Even though the court's interpretation is not binding on other circuits, the logic of the court in *U.S. West* has had a profound effect on how personal information used in business transactions is viewed. The court obviously rejected a view of consumer privacy that considers an individual's personal information as property controlled by that individual; rather the court considered private information to be a kind of "speech," and the use of a consumer's information by third parties in commercial transactions commercial speech protected by the First Amendment.

The court came to its decision by applying the analysis used by the Supreme Court in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York.*[114] The *Central Hudson* test is the analysis a court performs to determine whether a restriction on commercial speech violates the First Amendment. Under the test, as a threshold matter a court asks first whether the commercial speech concerns lawful activity and is not misleading.[115] Next, the court determines that the government can restrict the speech in question if it proves that: (1) it has a substantial state interest in regulating the speech, (2) the regulation directly and materially advances that interest, and (3) the regulation is no more extensive than necessary to serve the interest.[116]

In the context of consumer privacy, the key decision of the *U.S. West* court came in the way it resolved the question of whether there was a substantial state interest in regulating the commercial speech of telecommunications providers. First, the *U.S. West* court sidestepped the issue of a constitutional right to privacy by asserting that there are numerous types of privacy interests, and that the privacy interest at issue in this case was distinct from the rights involved in a constitutional right to privacy, claiming that constitutional privacy covers only personal rights deemed "fundamental" or "implicit in the concept of ordered liberty."[117] Because of the recognition by the Supreme Court of a constitutional right to privacy, the court could not declare that the state does not have a substantial interest in promoting privacy per se. Rather, according to the *U.S. West* court, "privacy is not an absolute good because it imposes real costs on society."[118] The only privacy interests the state can assert are those that are substantial, and even then only when the state has properly balanced the benefits and harms of the privacy interest involved. In the context of a speech restriction, the court claimed that the government can only restrict the dissemination of information the disclosure of which "would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity."[119]

Once the court set out an extremely limited view of personal information, it was not difficult to satisfy the other prongs of the test. The court went on to state that, if the privacy interest at stake is indeed substantial, then the restrictions must also be narrowly tailored. To narrowly tailor its restrictions, an administrative agency must first weigh costs and benefits to assess whether the burden on speech is too severe.

At issue is whether Congress may enact "opt-in" rules at all, or whether such restrictions are necessarily too broad. Under an opt-in rule, such as Section 222, consumers must proactively agree that their personal information can be used. If a consumer takes no action, then his information cannot be used. An "opt-out" rule, on the other hand, requires that a consumer agree his information will *not* be used. Unless a consumer agrees that his information cannot be used, or opts out, the consumer's personal information is up for grabs. According to *U.S. West*, Congress was not permitted to enact an opt-in regime such as that of Section 222 without first considering an opt-out scheme, under which consumers would be required to inform telephone companies in advance that they did *not* want their personal information shared with third parties.

Although the case principally discussed the constitutionality of Section 222, it did not invalidate the law, rather it criticized the FCC's interpretation of the law's standard as an opt-in rule.[120] In the wake of *U.S. West*, the FCC reinterpreted Section 222's clear opt-in regime, deciding instead that it must be structured as an opt-out rule, since such a rule was the most "narrowly tailored" way to implement Congress' intent.[121] Under current FCC regulations, consumers are required to inform companies that they do not want their personal information used, despite than the law's clear statement that consumers must opt-in, telling telecommunication companies if they desired to have their personal information used for marketing.

Even in an opt-in regime, it is not clear that consumers would have any recourse if telecommunications companies ignored consumer choice.[122] In *Conboy v. AT&T Corp.*, AT&T gave information about a couple's unlisted telephone number to their credit card affiliate, which was attempting to collect a debt owed by their daughter-in-law.[123] AT&T was granted summary judgment because the couple could not demonstrate any damages, despite the obvious violations of the Act's provisions and thirty-to-fifty calls made to them by the credit card company. The logic of *Conboy* is similar to that of *U.S. West*—if the state has no interest in protecting individual privacy, then a violation of that privacy does not cause harm unless it is accompanied by an egregious financial harm.

3. How Does U.S. West *Apply to Location Information?*

There are any number of problems with the court's logic in *U.S. West*, and certainly the failure to consider the possibility that *consumers*, not businesses, might be the parties whose constitutional rights are implicated here must be high among them. There are numerous instances in which Congress regulates the ability of a business to "speak" about information that an individual might provide to it. Copyright is one obvious example, where the government's interest in promoting arts and sciences gives it the right to prohibit one business from selling intellectual property created by another;

trademark, which is justified by the law of unfair competition rather than the Constitution's Copyright Clause, is another.[124] But even if one accepts the court's tenuous First Amendment logic in the case of consumer information generally, it is nearly impossible to extend that fractured logic to regulation over location information. In *U.S. West*, the court refused to recognize that the consumer was "speaking" at all—apparently the court's logic only allowed it to recognize the disclosure of a consumer's information as "speech" when the information was being disclosed by a third party. Location information, on the other hand, is clearly not "speech" on the part of a consumer, rather it is purely information gathered by the cellular phone provider.

The *U.S. West* court articulated only one state interest in protecting the consumer information of telecommunications consumers—privacy. There is, however, another articulated state interest in the case of location information—public safety. Section 222 clearly sets out the state's reason for gathering location information:

> To provide call location information concerning the user of a commercial mobile service...
>
> (A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
>
> (B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or
>
> (C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.[125]

This clearly articulated state purpose would seem to justify an opt-in regime for location information. The state has a clear interest in seeing that consumers do not avoid use of a potentially life-saving technology because of fears of abuse of their private information. An opt-in rule seems the clear way to avoid this. The FCC's recent ruling setting opt-out as a standard for consumer information, however, failed to take note of this distinction.

C. Location Privacy Protection Act of 2001

In 2001, before the September 11th terrorist attacks, Senator John Edwards introduced a location privacy bill in the Senate.[126] It was referred to the Committee on Commerce, Science, and Transportation, but no action was taken on the bill in the 107th Congress, and it was not re-introduced in the 108th. It is interesting, though, to note the emphasis of the proposed legislation. The bill states as a finding:

> There is a substantial Federal interest in safeguarding the privacy right of customers of location-based services or applications to control the collection, use, retention of, disclosure of, and access to their location information.[127]

The bill presents six findings in all, a clear response to the *U.S. West* court's claim that Congress must offer a compelling state interest before protecting a privacy interest. The bill goes on to require the FCC to hold a rulemaking proceeding on location privacy. The key provisions of the act:

- Providers of location-based services are required to give customers clear and conspicuous notice about proposed uses of their personal location data;
- Consumers must give express authorization (opt-in rule) before their data can be used;
- Third parties would be restricted from disclosing location information without prior authorization.

1. Technology Neutrality and the Regulation of Telematics and Other Wireless Devices

Unlike the Wireless Act, the proposed Location Privacy Act sets a standard that is technology neutral.[128] The act explicitly extends FCC jurisdiction to *all* providers of mobile services, including telematics companies. As Senator Edwards said when he introduced the bill:

> [A]lthough under the law customers must give their permission before wireless carriers can use or disclose their location information, the [current] law does not require carriers to clearly notify consumers about how their location information will be used if they do give permission. Consumers also have no control over what happens to their information once third parties gain access to it. These parties are free to share it with anyone they please. And, shockingly, there are no laws that protect the privacy of users of new technologies like telematics . . . and global positioning systems.
>
> . . . .
>
> The law needs to be strengthened, and we have the opportunity to do so while these location-based technologies are in their infancy.[129]

2. The FCC's Rejection of Location Privacy Regulation

Like much privacy-related legislation, the Location Privacy Act died in committee after the September 11th attacks. Before Sen. Edwards introduced his legislation, the Cellular Telecommunications & Internet Association ("CTIA") had proposed a similar set of location privacy regulations to the FCC. The industry organization was hoping that the agency could bring clarity to the tangle of location

privacy. The commission enacted the general opt-out requirement for consumer proprietary information on July 16, 2002, and four day later, it refused to consider location privacy rules. The commission declared that, even though the proposal came from the industry's largest trade association, it did not want to inadvertently "constrain the still-developing market for location-based services,"[130] and decided that it would be better to "vigorously enforce the laws as written, without further clarification of the statutory provisions by rule."[131]

Commissioner Michael Copp wrote a dissent in which he highlighted the current confusion surrounding Section 222(f).[132] Some, he noted, interpret the statute as permitting the *collection* of location data without a consumer's permission, while others read the statute as requiring an opt-in before the data is even gathered. He argued that it was not too early to clarify the uncertainty concerning the meaning of Section 222(f), precisely because of the nascent state of the market, since industry would be forced to retool later a far more expense.[133] The CTIA criticized the commission's decision as well, calling it a "fumble."[134]

D. The Data-Mining Moratorium Act of 2003

Senator Russell Feingold introduced a bill designed to impose a moratorium on governmental data-mining activities.[135] The Act prohibits any employee of the Department of Defense or Department of Homeland Security from engaging in data mining for TIA or any similar data-mining project. Some of the findings are particularly significant when one considers the skepticism with which privacy advocates view governmental data mining:

> (2) There has been no demonstration that data-mining (sic) by a government, including data-mining such as that which is to occur under the Total Information Awareness program, is an effective tool for preventing terrorism.
>
> (3) Data-mining under the Total Information Awareness program or a similar program would provide the Federal Government with access to extensive files of private as well as public information on an individual.
>
> (4) There are significant concerns regarding the extent to which privacy rights of individuals would be adversely affected by data-mining carried out by their government.[136]

The Act enacts a moratorium to give Congress time to analyze the impact of data-mining techniques on the privacy rights of individuals. The bill has been referred to the Senate Judiciary Committee.

E. Tort Law Approach

A California State Senator proposed one solution to information privacy issues—the creation of a new invasion of privacy tort.[137] The primary effect of the creation of such a tort would be to give individuals a basis for suits against companies that had

abused their personal information. The law, which was deleted from the bill as it was finally enacted, read:

> There shall be a cause of action for the unlawful disclosure of any personal information gathered by a commercial or governmental entity for a commercial or governmental purpose which that entity subsequently releases to a third party without the express permission of the person to who the information relates. It shall be presumed in any proceeding authorized by this section that the person to whom the information released relates has sustained damages thereby.[138]

Courts have recognized four traditional torts of invasion of privacy: (1) intrusion upon personal physical solitude, (2) public disclosure of private facts, (3) publicity which places a person in a false light, and (4) misappropriation of a person's likeness for another's benefit.[139] *Conboy* highlights the problem with the traditional torts in the context of information privacy—an identifiable injury.[140] In the case of location privacy, this problem becomes even more acute. As was noted earlier, location information is gathered in a public space that is observable by any passing member of the public, a place over which it is difficult to assert a claim of privacy. *Nader* demonstrates, however, that an invasion of privacy can happen in places other that the traditional "private sphere."[141] Revisions to tort law such as those attempted in California might well offer individuals a way to defend privacy rights against infringement by private parties through civil law suits. But a more pervasive regime, such as the FTC fair information practices[142] or the protections offered by the European Union's data directive[143] offer the possibility of the development of a *culture* of privacy protection—since the prevention of data abuse is far preferable to consumers than the collection of damages after some particularly heinous data abuse.

F. FTC Fair Information Practices

The fundamentals of information privacy protection advanced by the Federal Trade Commission ("FTC") offer a summary of principals to consider when analyzing privacy issues. Although the FTC has not used these criteria specifically in the context of location privacy issues, they provide a useful analytic framework. The FTC's five principals are (1) notice, (2) choice, (3) access, (4) security, and (5) enforcement.[144]

1. Notice—The FTC has called notice "the most fundamental of the fair information practice principles.[145] Data collectors must disclose their information practices before collecting personal information from consumers, including: (1) identification of the entity collecting the data, (2) the uses to which the data will be put, and (3) the nature of the data collected and the means by which it is collected. Personal information is information data that is used to identify, contact or locate a person.[146] Notice requires more than the mere mailing of a privacy statement, rather it requires a proactive effort to ensure that consumers are aware of the ways in which their data will be used.

2. Choice—Choice means that consumers must be given options about how information collected from them may be used beyond what is necessary to complete a

particular transaction. Under this principle, consumers must give their consent before data collectors can make secondary "downstream" use of their data. This is in keeping with consumer expectations—a recent FTC study shows that 88% of consumers who use the Internet expect opt-in privacy policies in which they are asked before their personal information is passed on to a third party.[147]

3. Access—Refers to an individual's ability to access data about herself by viewing a data collector's files and having the ability to contest the accuracy of the data. Access is the only real way to guarantee the quality of the data that has been gathered and introduce a measure of accountability into the data collection process.

4. Security—A data collector has an obligation to protect data against unauthorized access, use or disclosure. Finding the balance between access and security can be difficult, since making a database readily available to authorized users exposes it to access by unauthorized ones.

5. Enforcement—Enforcement can mean different things in different cases. In some cases, it can mean self-regulation, in others, government regulation, and in still others, it can mean civil law suits or criminal prosecutions.

V. INTERNATIONAL BEST PRACTICES

Although this memo focuses on U.S. location privacy issues, it is also useful to look at various international standards for privacy protection. Privacy protection in the United States has tended to focus on protection of the individual from an intrusive government, while in other countries, such as those of the European Union, the emphasis is on protection of personal information from third-party users. The U.S. has taken a more *laissez faire* approach to markets, and regulation is often avoided unless there is a market failure, and government intervention is considered likely to improve matters.

A. Models for Privacy and Data Protection

Privacy International has identified four major models for privacy protection.[148] In various countries, different combinations of these models are used to offer privacy protection:

1. Comprehensive Laws

Many countries have a general law that governs the collection, use, and dissemination of personal information by both the government and private sector. The prime example is the European Union Data Protection Directive ("E.U. Data Directive").[149]

2. Sectoral Laws

The United States offers a second model. The U.S. has rejected the concept of general data protection rules. Instead, there are specific sectoral laws governing, for

example, videocassette rentals and financial or medical privacy. An obvious drawback to this approach is that privacy protection tends to be spotty. As Privacy International notes, " [t]he lack of legal protections for individual's privacy on the Internet in the United States is a striking example" of the failure of this sectoral approach.[150]

3. Self-Regulation

Another U.S. approach to data protection is to encourage companies and industry groups to adopt various forms of self-regulation by adopting codes of self-regulation and engaging in self-policing. Adequacy and lack of enforcement are two major problems with this approach.

4. Technology

Technological self-help is yet another way to provide varying degrees of protection. Techniques include encryption, anonymous remailers, proxy servers and various digital payment methods.

B. E.U. Database Directive and Location Information

The European Union Data Protection Directive, which became effective in 1998, regulates *businesses*, setting restrictions across industries on the type of data companies can gather, and dictates that data can be collected only for legitimate business purposes.[151] A principal piece of U.S. privacy legislation, on the other hand, the Privacy Act of 1974, limits the ability of the *government* to collect, maintain and release information about its citizens.[152] The market, rather than the government, is the place where privacy protections in the U.S. tend to begin.

The E.U. Data Directive offers a different level of privacy protection than comparable U.S. laws. Individuals must be informed before any of their personal information can be transferred to a third party, and they must be given a chance to object.[153] Location information is treated no differently than any other kind of data. The European Parliament enacted something similar to the protections offered in the U.S. Section 222(f), declaring that, while public telephone networks should ensure that emergency location information about mobile subscribers are made available to appropriate authorities, any other use of such information must comply with the Directive's constraints on the processing of personal data.[154] The European Union's Directive for the Protection of Data and Privacy in the E-Communications Sector ("E.U. Data and Privacy Directive") establishes a clear opt-in requirement for the use of personal data in electronic communications consistent with the general directive.[155]

C. Location Privacy in Emerging Democracies

Joe Bailey has noted that in Communist Russia, the concept of privacy was quite different than that which arose in Western societies:

> The Bolshevik revolution commenced an experiment in reconfiguring the private/public distinction in which the "New Soviet Man" attempted a radical transformation of individuality itself in everyday life. The background was Marx himself, who saw no positive value in privacy and anticipated the total subordination of the private to the public. Bolshevism relied on the fervency of individual belief and motivation, but, paradoxically, did not recognize a private sphere that could not be revealed, displayed, and confessed under an ever-present public gaze.[156]

Certainly, communist societies were different from Western analogues. If the individual was dominant in the West, under Communism the collective was most important. The English word "privacy" has no direct equivalent in Russian.[157] Mark Neocleous points out the historical closeness of the terms "secrecy" and "privacy." He quotes Samuel Johnson, who defined privacy as the "state of being secret; secrecy," and secrecy as "privacy; state of being hidden."[158] If privacy, then, is a kind of "private secrecy," perhaps this kind of individual privacy is necessary for the growth of democracy. "State secrecy," on the other hand, is the sort of "public secrecy" which can give rise to totalitarianism. Yet, as these countries move toward a market economy, they have made a "Western" view of privacy, along with the primacy it places on the individual over the collective, a policy priority.

Interestingly, although data protection is not a priority in the United States, it is explicitly spelled out in the constitutions of most post-Communist countries. This is in keeping with the protection spelled out in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of the rights and freedoms of others.[159]

The European Commission of Human Rights and the European Court of Human Rights have consistently recognized an expansive right of privacy:

> In the opinion of the Commission... the right to respect for privacy does not end [with the right to live protected from publicity]. It comprises also, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality.[160]

It is interesting to note that the scattershot protection of individual information offered in the United States has formed the model for none of these countries. Instead, Eastern Europe has looked to the broader protections offered by the E.U. Data Directive. This drive by these nascent democracies for conformity with pan-European laws is driven not only by a desire to promote international electronic commerce but also by a desire to

remedy past privacy abuses. If institutional secrecy is a legacy issue faced by these countries, perhaps they are looking to a different concept for the answer, a regime grounded in a solid guarantee of individual privacy.

While all of the former Warsaw Bloc countries have included some protections for individual privacy in their constitutions and laws, and each has attempted to work within the broader European framework, each country has also taken a different approach to solving the problem.

VI. ANALYSIS

The earlier parts offered a framework for identifying location issues, and examined relevant technologies. This Part looks at how to assess a location privacy issue, using the expectation of privacy and the analytical tools discussed in Part I as a guide and, through a series of case studies, looks at how this location privacy framework can help one conduct cost-benefit analyses of potential location privacy problems.

A. The Location Framework and Cost-Benefit Analysis

For wireless location services, the negative impact of privacy concerns must be balanced against a genuine social good—enhanced safety and security. With the advent of E911 service, the time it takes to rescue a wounded, stranded motorist could be reduced from hours to minutes. The ability to locate callers in distress can literally be the difference between life and death,[161] and in the wake of the attack on the World Trade Center, when desperate callers trapped in the building's rubble attempted to call rescuers,[162] the demand for E911 services is high.

How does one assess the benefit to society of this service and weigh the countervailing costs of lost privacy? In a paper for the American Enterprise Institute–Brookings Joint Center for Regulatory Studies, Robert Hahn and Anne Layne-Farrar propose a framework for analyzing the costs and benefits of privacy regulation.[163] They assert that economic arguments concerning privacy can be reduced to arguments about the existence and alienability of property rights in personal information.[164] At one end of the spectrum are privacy advocates who assume that one can possess property rights in their personal information. At the other, is the idea that the collector of information may use any data he can collect, since individuals do not have any property rights in information that can be gathered about them. By valuing those property rights, and comparing them to an assessment of the cost of privacy regulation to business, they claim, one can assess the relative costs and benefits.

In *U.S. West*, the court claimed that there was no absolute right to privacy. Rather, according to the court, there are two sources for the protection of privacy rights: absolute constitutional rights in privacy, like those set out in *Griswold* and *Roe v. Wade*; and those privacy rights which should be protected because the costs of depriving an individual of them exceeds the benefits of not enforcing them.[165]

There are serious gaps, however, in the ability to quantify both sides of a cost-benefit analysis ("CBA") of wireless location privacy. Information is incomplete, and consumers are often unaware of the implications of the use of their personal information, in particular the possible "downstream" use of their information. For example, cellular telephone customers face the use of their personal information by non-regulated businesses affiliated with their wireless carrier. These companies, who sometimes have no or minimal privacy protections in place, can "add value" to personal information by combining the information contained in multiple databases, creating detailed profiles of potential buyers.

The transaction costs involved in an attempted regulation of location-based information are potentially huge. Some argue that the costs of an aggressive regulatory scheme would necessarily be borne by taxpayers, because of the infrastructure necessary to enforce it.[166] Rapid technological change and the undefined nature of the market make any attempt at regulation at best a shot at a moving target. Self-regulation by wireless businesses provides one possible solution to the problem of how to balance privacy and business concerns, since any wireless marketing program must be premised on a certain level of trust between business and consumer. Wireless companies presumably have an incentive to protect the privacy of users out of fear of bad publicity or because of an expected backlash from injured consumers.[167] Groups such as the Cellular Telecommunications Industry Association and the Wireless Advertising Association have emphasized the importance of a self-regulatory structure "with teeth" that would protect consumers and yet give advertisers wide latitude to use location information.[168] And cellular manufacturers have shown some sensitivity to privacy concerns. For example, even though government regulations do not require the feature, new phones equipped with GPS allow users to turn off the tracking functions.[169] And some of the most aggressive proposals for pro-privacy regulations have been proposed to the FCC by the CTIA.[170]

But, the example of the Internet shows some of the problems with a self-regulatory model. The FTC initially encouraged websites to police themselves, and hoped that industry organizations such as TRUSTe and BBBOnline would provide an efficient enforcement mechanism for privacy violations on the Internet. Unfortunately, those programs' privacy principles were adopted by only 8% of the web's most heavily used sites. In the face of non-existent self-enforcement, the FTC was forced to reverse itself and push for the enactment of regulation in the face of the failure of self-regulation.[171]

There are two kinds of information at play in location-based transaction. The first is information as *commodity*—the actual bits of data gathered about individual consumers. The second is information *about* the transaction—who has the data, what will they do with it, how will that use affect consumers? While personal data is the commodity involved in the transaction, it is the lack of the second type of information, the transactional information, which causes a market failure. This information cost clouds any attempt to weigh the costs and benefits of location-based services. Hahn & Layne-Farrar take the view that the government should have little role in regulating information privacy, nonetheless proposing an interesting role for an agency such as the

FCC or FTC. "The government," they say, "should attempt to make it easier for the public to obtain information on online privacy."[172] In their view, though, a web site detailing information about how to opt-out is the extent of tolerable government regulation, even though the impact of privacy abuses on consumers in nearly impossible to quantify.

Discussions of costs and benefits have tended to revolve around easily quantified costs. And certainly, it is tempting to focus on readily quantifiable costs, such as infrastructure and compliance costs. But for a cost-benefit analysis to be useful, it must factor in intangible costs as well. Each of the FTC fair information practices represents costs for businesses. For example, Hahn and Layne-Farrar try to quantify some of the costs to business of compliance with some fair information practices:[173]

- *Cost of Providing Notice*—e.g., the estimated cost to financial institutions to design, print and mail privacy notices to customers under Gramm-Leach-Bliley: $2 billion to $5 billion.
- *Cost of Providing Choice*—e.g., estimated ten-year compliance cost to the health care industry for allowing the use of individual information with individual consent: $11.8 billion.
- *Cost of Providing Access*—e.g., estimated cost of correcting errors in consumer credit reports: $100 million.

It is tempting to stop with such figures and decry the costs to business of potentially disruptive privacy regimes. But consumers also incur costs from the absence of privacy protections. Jerry Kang has proposed a formula for choosing between opt-in and opt-out, which takes into account the costs either regime exact on an individual consumer.[174] The cost of a regime, opt-in or opt-out, equals the cost of "sticking" (accepting the rule despite its inefficiencies, particularly high transaction costs) plus the cost of "flipping" (contracting around the default rule). Kang argues that an opt-out rule is more costly for consumers for two reasons: (1) it is costly to determine whether one's personal information has been shared, and who might currently have access to that information; and (2) individuals who want to "flip" may not have the bargaining power to do so. Factoring consumer costs into the equation complicates efforts at cost-benefit analysis.

B. Comparing Alternate Uses of a Location Technology

Table Five sets out some of the potential benefits and costs of a technology such as wireless telephones or telematics devices.

TABLE 5.: COSTS AND BENEFITS OF ACTIVE LOCATION DEVICES

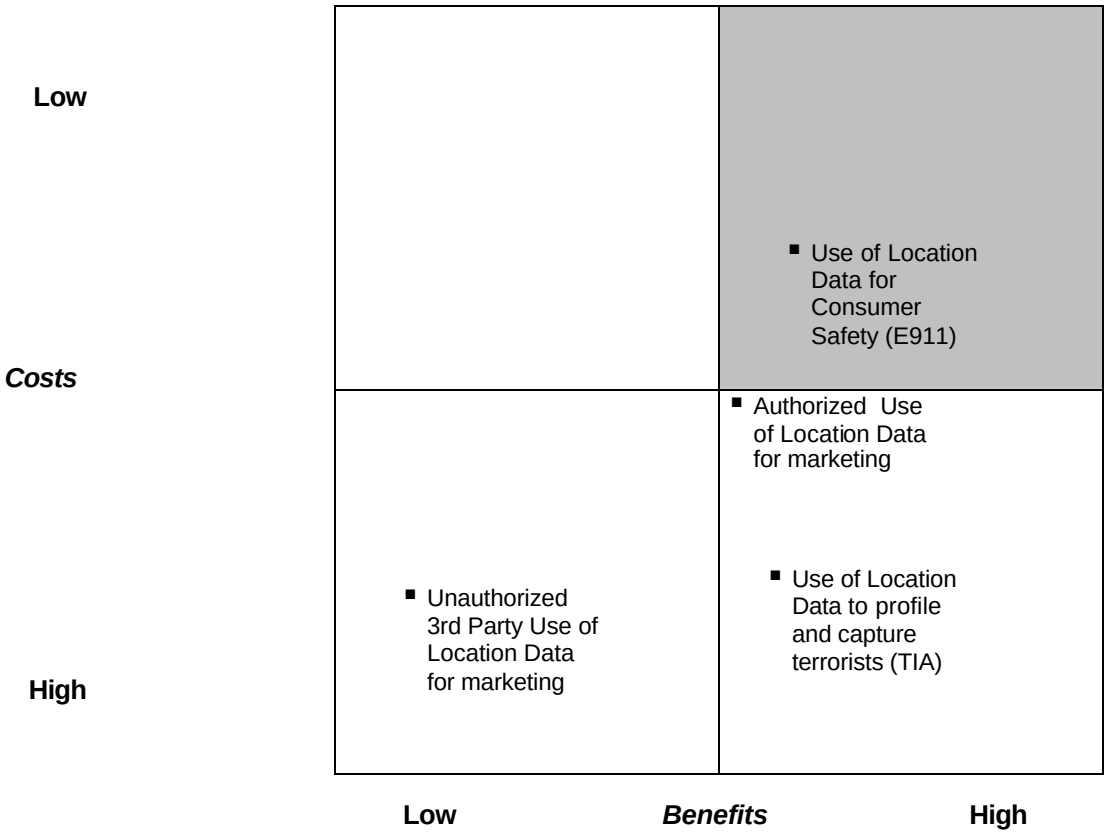
	Consumers	Business
Costs	▪ Tracking device ▪ Loss of property right in personal information ▪ Access by law-enforcement to ordinarily unobtainable information ▪ Loss of anonymity ▪ Government intrusion into personal life ▪ Possible profiling by "downstream" users ▪ Cost of obtaining information about possible downstream users ▪ Cost of profiles based on incorrect or incomplete information ▪ Possible impact on ability to get work, credit or housing ▪ Identity theft	▪ Cost of providing choice: Opt-in, not opt-out ▪ Cost of providing notice: Written permission ▪ Cost of providing access: Carriers may be required to share their information with consumers, possible need to track "downstream" uses of a consumer's information ▪ Complexity; cost of inadvertent noncompliance ▪ Cost of installing location technology ▪ Cost of complying with government regulations ▪ Cost of playing a "policing" role
Benefits	▪ Life-saving rescue technology ▪ Personalized auto directions, even when caller doesn't know her location ▪ Personalized advertisements	▪ Ability to market based on a detailed profile of a consumer, combing location with other information ▪ Create new and different products ▪ Reach consumers who are physically in a position to make an immediate purchase

Obviously, this list is long and not easy to quantify. And yet, when one looks at a *particular* use of a given technology, the balance between costs and benefits for *that* use changes.

If one were to set this out in a grid with four quadrants, a given technology's placement in a particular quadrant would dictate whether or not the implementation of that technology was beneficial to consumers. For example, looking at Chart One, in the upper right quadrant are those technologies that are high-benefit and low-cost. Such technologies should be implemented. As we will see when looking at active, passive, and flexible technologies, few uses end up in that quadrant. Rather, many attractive uses end up in the lower right quadrant, high-benefit, and high-cost. Such technologies must be viewed skeptically, and ways to lower costs, which are often measurements of deprived liberties, should be sought and implemented. The lower left quadrant, high-cost, low-

benefit technologies, should be avoided. Few, if any, technologies are in the upper left quadrant, low-cost, low-benefit, but because of their minimal utility, such technologies should be avoided as well.

CHART 1.: CONSUMER COSTS AND BENEFITS OF ACTIVE LOCATION DEVICES

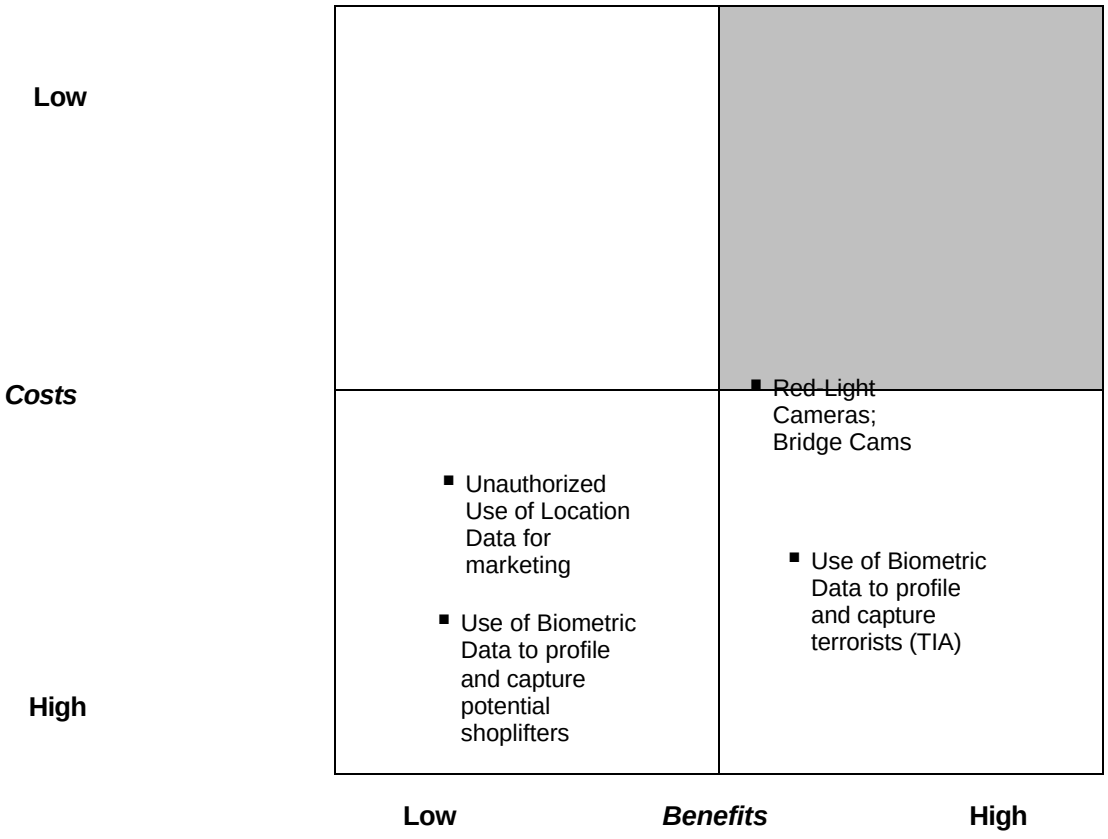


The three uses of location data set out in Chart One show how the same use of a technology (GPS tracking and processing) has a different combination of costs and benefits to consumers depending upon the ultimate use.

- *Location Data for Consumer Safety*—It is difficult to argue that this does not belong in the top right quadrant. Chart One places this low in the quadrant only because of the high initial costs of deploying such a system. The life-saving benefits of this technology clearly outweigh the costs—even transaction costs and costs associated with lost privacy and loss of anonymity.
- *Unauthorized Third-Party Use of Location Data for Marketing*—"Location spam" sits in the opposite quadrant from life-saving technology. The costs to consumers are high—the cost of flipping, the lost time and effectiveness of their wireless devices—while the benefits are low.

- *Authorized Use of Location Data for Marketing*—Location information can also be used for targeted messages sent with the authorization of the user. Even with consumer buy-in, the potential for abuse is high, and in an opt-out regime, the potential for sale of one's information to third parties without his knowledge is particularly high.
- *Use of Location Data to Profile and Capture Terrorists*—The benefits of tracking and capturing terrorists are high, but so are the costs. Consumers face the risk of eroding personal liberties, and the personal costs that come from false profiling and the potential for deportation or arrest based on incorrect information.

CHART 2.: CONSUMER COSTS AND BENEFITS OF PASSIVE LOCATION DEVICES



By definition, passive location tracking involves the tracking and storage of information about a consumer without her knowledge, and so the cost of such a technology is necessarily increased.

- *Red-Light Cameras*—The safety benefits associated with red-light cameras are clear: fewer accidents and greater enforcement of traffic laws. And yet, because of the lack of due process associated with their use and the potential for unauthorized downstream use of the information gathered, the technology

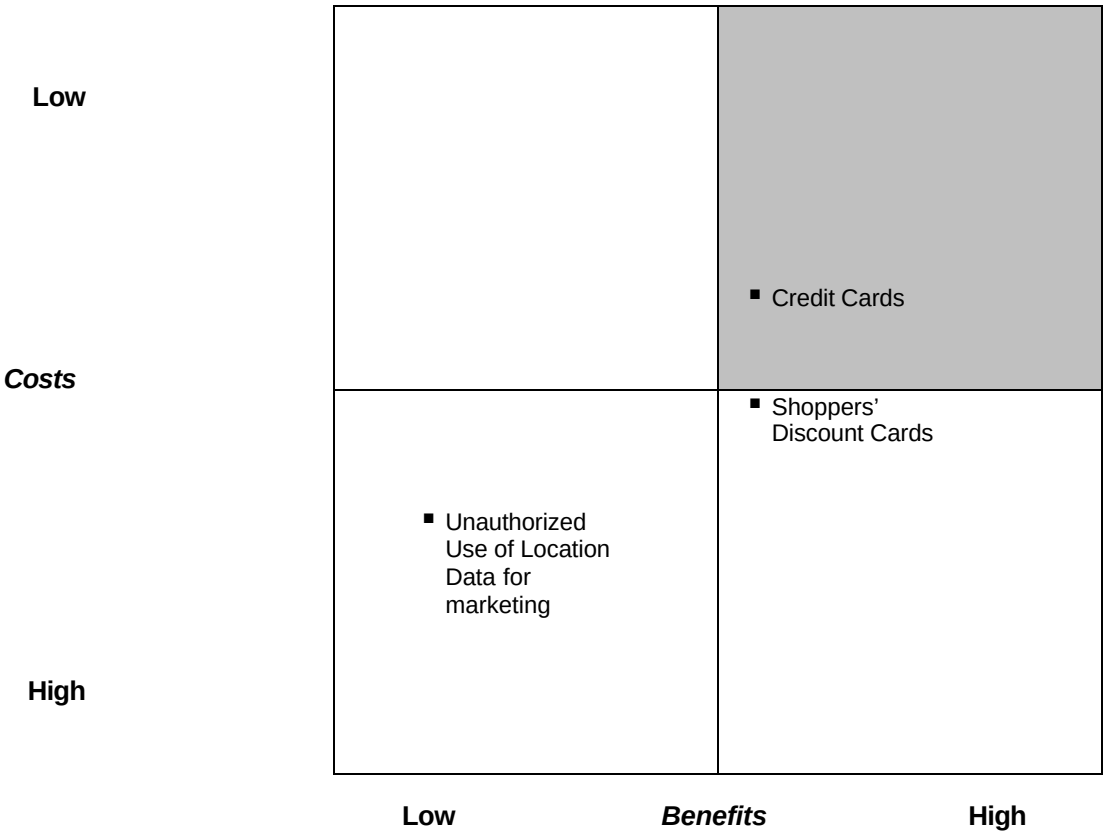
is on the edge of being too costly in terms of privacy violations to be an effective location technology.

- *Unauthorized Use of Location Data for Marketing*—Although there are currently not a large number of marketing uses for these biometric technologies, it is possible to imagine a species of "location spam" that is based on the use of these passive devices. In the film *Minority Report*, Tom Cruise is greeted by "smart" billboards that make their sales pitches based on a reading of his biometric signals. The costs of such technologies for individual consumers in terms of violation of individual privacy would be high enough to call into question the value of such a system.

- *Use of Biometric Data to Profile and Capture Terrorists*—The benefits and costs here are similar to those detailed above.

- *Use of Biometric Data to Profile and Capture Potential Shoplifters*—But these technologies could be used for more that profiling and capturing terrorists. Borders purchased and planned to install cameras equipped with facial recognition software to track and locate known shoplifters, but did not implement the plan because of consumer outcry.[175] The theme which has surfaced again and again in this memo surfaces yet once more—if a location-tracking technology exists, it will be used, and used in ways that were quite possibly unintended by the designers of the system.

CHART 3.: CONSUMER COSTS AND BENEFITS OF FLEXIBLE LOCATION DEVICES



- *Credit Cards*—Location tracking is an unintended consequence of an electronic commerce system. Unlike a hidden camera equipped with facial recognition software, which captures location information with neither knowledge nor consent, credit cards create records of voluntary transactions. While credit cards certainly raise a number of privacy issues, in terms of their ability to track a consumer, the benefits associated with them are not outweighed by excessive costs.

- *Shoppers' Discount Cards*—Interestingly, one recent survey showed that shoppers who buy their groceries at supermarkets that use discount cards on average pay *more* than consumers who shop at stores that do not.[176] Like credit cards, the use of these cards is voluntary, and it is not reasonable for a user to expect his location to be tracked. However, because the benefits of the use of these cards are only moderate, they sit somewhere near the center of the grid.

- *Unauthorized Use of Location Data for Marketing*—It is the potential abuse of credit card and shoppers' card data that must give one pause, and ultimately calls into question their value. Like any other location-tracking technology, the information gathered by these devices is subject to abuse.

VII. RECOMMENDATIONS

What *is* the reasonable expectation of privacy one can expect in regard to information about her location? What *are* the trade-offs one must make between privacy and safety? These are not easy questions to answer. But an approach such as that taken in *U.S. West* could lead to disastrous results. The *U.S. West* court was right to underscore the importance of cost-benefit analysis. But for such an analysis to be meaningful, it must weight the cost of the deprivation of privacy rights. In approaching the formulation of location privacy policy, policy-makers must proceed cautiously, always remembering the distinction between the casual watcher, who is fee to observe, and the stalker, who is not. Technology can gradually transform us into a nation of victims, constantly pursued by legions of electronic stalkers, and "expectation of privacy" can, sadly, become a quaint expression from a dimly remembered past.

Location Privacy Policy Recommendations:

- *Location privacy practices should be technology-neutral, and based on future, rather than current, capabilities of technologies*—Moore's law highlights a key problem with making recommendation on the basis of current technology: The capabilities of a given technology changes rapidly, almost daily.[177] As storage and processing capabilities increase, so does the severity of potential privacy abuses. Technology neutrality provides a way to assess the impact of a location privacy *practice* rather than a particular location privacy *technology*. One clear lesson of this memo is that technologies will be used to their full capabilities, even if such use violates an individual's right to privacy, unless regulatory or other restrictions restrict such uses.

- *Support creation of an opt-in regime for location information*—Cost benefit analyses of location privacy technologies and practices must factor in the cost of lost privacy rights. As we have seen,[178] the transaction costs associated with an opt-out regime are high, and it is difficult, if not impossible, for consumers to monitor abuses of their personal location information.

- *Support the re-introduction of the Location Privacy Information Act*—Senator Edwards' act[179] offered logical and effective location privacy protection, and its re-introduction should be advocated.

- *Support the enactment of reasonable restrictions on the Government's use of data-mining technologies*—The potential for "false leads" from government data-mining efforts offers the possibility of serious invasion of individual's privacy to a degree not warranted by the level of threat, and the potential privacy violations from elaborate government dossiers is not known.

- *Urge the FCC to reconsider its refusal to enact location privacy regulations*—The FCC has the capability of enacting regulations that could enable the nascent location-based technology business to incorporate appropriate privacy protections, and industry groups seem to support such an enactment.[180]

- *Support the enactment of similar measures on the State level*—Even if federal location privacies are not passes, enactment of similar measures on the state level could also have a positive impact on location privacy.

APPENDIX—ABOUT THE ELECTRONIC PRIVACY INFORMATION CENTER

The Electronic Privacy Information Center ("EPIC") is a public interest research center that was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has been an advocate for pro-privacy issues, with its fellows testifying before Congress, bringing privacy litigation, filing amicus briefs and appearing before Federal agencies. EPIC also publishes a comprehensive selection of books and reports on computer security, cryptography, the First Amendment and free speech, open government and privacy.

EPIC has identified location privacy as an important issue precisely because of the lack of available material detailing approaches to the problem. This memo will help EPIC craft a position on the issue, as well as provide a framework policy-makers can use to approach the issue.

ENDNOTES

[1] In the Chevy ad, actor James Garner recites a paean to location privacy that is designed to sound like a classic poem one has heard somewhere before but just can't place. The poem, however, was written specifically for the ad campaign by copywriter Patrick O'Leary. *See Plum Productions' Eric Saarinen Mimics Old Masters for Chevy Tahoe Branding Campaign*, DIGITAL PRODUCER , Nov. 21, 2002, *at* http://www.digitalproducer.com/2002/11_nov/news/11_18/plum21.htm.
[2] Katz v. United States, 389 U.S. 347, 351 (1967).
[3] Practicing Law Institute, *Mobile Telephony*, 684 PLI/PAT 383, 389-90 (2001).
[4] *See* discussion of E911 *infra* IV.A.
[5] *See* Brad Smith, *Driving Telematics Beyond Safety, Security*, WIRELESS WK., Jan. 01, 2003, at 28.
[6] *See infra* Part III.A.2.a)
[7] *See infra* Part III.A.3.
[8] *See infra* Part III.A.2.
[9] *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967).
[10] *See, e.g.*, Aaron Fulch & Christine Soares, iBrief, *MEDIA & COMMUNICATIONS: Enhanced 911 Technology and Privacy Concerns*, 2001 DUKE L. & TECH. REV. 38 (2001); Paul K. Hentzen, Comment, *The Trouble with Telematics*, 69 UMKC L. REV. 845 (2001); Aaron Renenger, Note, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L.J. 549 (2002) (discussing location privacy in the context of GPS devices); *but see* Location Privacy Protection Act of 2001, S. 1164, 107th Cong. (1999) (calling for a technology neutral approach to location privacy issues).
[11] *Katz* , 389 U.S. at 348 n.1 (citing 18 U.S.C. § 1804 (2000)).
[12] *Id.* at 349.
[13] *Id.* at 350-53.
[14] *Id.* at 351.
[15] Kyllo v. United States, 533 U.S. 27, 34 (2001) (paraphrasing the *Katz* test).
[16] *Id.* at 24.
[17] *Id.* at 34.
[18] *See* quote from *Kyllo* at text accompanying *supra* note 17; Katz v. United States, 389 U.S. 347, 358 (1967) ("[Constitutional] considerations do not vanish when the search in question is transferred from a home . . . to a telephone booth.").
[19] As the Court says:

> In the case of a search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimal expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.

Kyllo, 533 U.S. at 34 (emphasis in original).
[20] *See* Nader v. GMC, 25 N.Y.2d 560 (1969).
[21] *Id.* at 564.
[22] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890).
[23] *Nader*, 25 N.Y.2d at 567 (emphasis omitted).
[24] *Id.* at 570-71.
[25] This tort of "intrusion into seclusion," offers at best an inexact analogy to the issues that arise in the case of location tracking technologies. *See* Renenger, *supra* note 10, at 558. This is in part because the information has been gathered in a public space that is observable by any passing member of the public, a place over which it is difficult to assert a claim of privacy. *See id.* However, *Nader* demonstrates that an expectation of privacy can arise in places other that the traditional "private sphere."
[26] See *infra* Part II.B.
[27] Michelle Delio, *Rent-a-Car Motto: Speed Bills*, WIRED NEWS, Jul. 12, 2001, *at* http://www.wired.com/news/privacy/0,1848,45163,00.html.
[28] *See id.*

[29] *See* discussion of Total Information Awareness, *infra* Part III.B.1.b).
[30] *See supra* note 10.
[31] *See* ROBERT W. HAHN & ANNE LAYNE-FARRAR, THE BENEFITS AND COSTS OF ONLINE PRIVACY LEGISLATION 2-5, AEI-Brookings Joint Center for Regulatory Studies, *available at* http://papers.ssrn.com/abstract_id=292649 (Oct. 2000).
[32] *See* Griswold v. Connecticut, 381 U.S. 479, 484-86 (1965)([S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees . . .); *see also* Roe v. Wade, 410 U.S. 113, 152-56 (1973); *cf.* FRED CATE, PRIVACY IN THE INFORMATION AGE 66 (1997) ([T]he U.S. Constitution . . . offers little support for information privacy . . . .").
[33] *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1294 (2000) (arguing that property rights in personal information are "inconsistent with much of our First Amendment jurisprudence").
[34] *See* CATE, *supra* note 32, at 66; HAHN & LAYNE-FARRAR, *supra* note 31 at 4-5.
[35] ELI M. NOAM, PRIVACY AND SELF-REGULATION, U.S. DEPT OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE DIGITAL AGE (1997).
[36] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 2 (2000) *available at* http://www.fcc.gov/reports/privacy2000/privacy2000.pdf [hereinafter PRIVACY ONLINE]
[37] FORRESTER RESEARCH, THE PRIVACY BEST PRACTICE (1999).
[38] *See, e.g.*, The Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (codified at 47 U.S.C. § 222 (2000))(protects the privacy of wireless customers); The Cable TV Privacy Act of 1984, 47 U.S.C. § 551 (2000), (protects the privacy of cable subscriber records); The Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. 2510) (protects the privacy of electronic mail); The Video Piracy Protection Act of 1988, 18 U.S.C. 2710 (2000) (protects the privacy of the rental records for videos); The Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936 (establishing safeguards for the delivery of medical information); *but see* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.
[39] *See,e.g.*, Sarah Marcisz, *Digital Advances Bring Privacy Concerns*, WASH. TIMES, Feb. 10, 2003, at A2; *see also* discussion of Total Information Awareness, *infra* Part III.B.1.b).
[40] For an extreme statement of the view that businesses have a First Amendment right to information gathered about their customers, including the right to sell that information for profit, see *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999). *See also* discussion *infra* Part IV.B.2.
[41] Dan Farmer & Charles C. Mann, *Surveillance Nation*, TECH. REV., Apr. 2003, at 38.
[42] Fabio S. Leite & Jorge M. Pereira, *Developing Location-Based Services*, INTERMEDIA, Feb. 2002.
[43] *See* Privacy Foundation, E911: Big Brother's Tracking System, Tipsheet, at https://www.privacyfoundation.org (last modified Dec 04, 2000).
[44] *See id.*
[45] *See* Fulch & Soares, *supra* note 10, at ¶9(describing these two visions as "Big Ad" and "Big Brother").
[46] *See* Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105, 106 (2000).
[47] *See* Smith, *supra* note 5.
[48] *See id.*
[49] *See* ALDO MORRI, WHITE PAPER: TELEMATICS PARADIGM SHIFT: INDUSTRY STRATEGIES MAKE BUSINESS MODEL REALITIES SINK IN 1-2, Strategis Group, *at* http://www.eyeforauto.com/reports/TelematicsParadigmShift1.pdf (last visited Mar. 15, 2003).
[50] *See* Anthony Harrington, *Mixed Signal on Telematics*, FIN. DIRECTOR, Nov. 1, 2001, at 14.
[51] *See* MORRI, *supra* note 49, at 10,11.
[52] Claire Starry, *The Emerging In-Vehicle Intelligent Transportation Systems Market* , BUSINESS ECON., Apr. 1, 2001, at 49.
[53] *See id.*
[54] *See* discussion *supra* text accompanying notes 27-28.

[55] *See* Smith, *supra* note 5; *In the Matter of Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, Order*, July 24, 2002. [hereinafter *Fair Practices Order*]
[56] *See* Michelle Kessler, *Growing Wi-Fi Services Cast Wide Net*, U.S.A. TODAY, Nov. 13, 2002, *available at* http://usatoday.com/money/industries/technology/2002-11-13-wi-fi-technology_x.html.
[57] *See* Kim Gilmour, *No Strings Attached: Wireless Access is Going to Change Our Lives*, INTERNET MAG., Mar. 1, 2002, at 62.
[58] Farmer & Mann, *supra* note 41, at 34, 36.
[59] *See* The Biometric Consortium's Home Page, *at* http://www.biometrics.org/html/introduction.html (last visited Mar. 27, 2003)
[60] JOHN D, WOODWARD, JR., SUPER BOWL SURVEILLANCE: FACING UP TO BIOMETRICS 1 (2001) *available at* http://www.rand.org/publications/IP/IP209/IP209.pdf.
[61] *See* discussion of the negative implications for technological tracking of terrorists at text accompanying note 76.
[62] *The Washington Times* reported:

> Officials of the National Aeronautics and Space Administration have told Northwest Airlines security specialists that the agency is developing brain-monitoring devices in cooperation with a commercial firm, which it did not identify. Space technology would be adapted to receive and analyze brain-wave and heartbeat patterns, then feed that data into computerized programs "to detect passengers who potentially might pose a threat," according to briefing documents....

Frank J. Murray, *NASA Plans to Read Terrorist's Minds at Airports*, THE WASHINGTON TIMES, Aug. 17, 2002.
[63] Mary Lehman, Comment, *Are Red-light Cameras Snapping Privacy Rights?*, 33 U. TOL. L. REV. 815, 815 (2002).
[64] *Id.* at 816.
[65] *See* Farmer & Mann, *supra* note 58, at 36.
[66] *See* Tim Moran, *Going with the Flow: Telematics-Equipped Vehicles Feed Real-Time Information to Highway System*, AUTOMOTIVE NEWS, Sept. 23, 2002, at 24T.
[67] *See* Fulda, *supra* note 46 at 106; GINA MARIE STEVENS, PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS 3 (Congressional Research Service, 2003).
[68] *See* Fulda, *supra* note 46 at 106-07 for the distinction between explicit and non-explicit data processing.
[69] Smith v. Maryland, 442 U.S. 735 (1979).
[70] *Smith*, 442 U.S. at 739.
[71] *Id.* at 741-46.
[72] *Id.*
[73] *Id.*
[74] *See* JEFFREY W. SEIFERT, DATA MINING: AN OVERVIEW 3 (Congressional Research Service, 2003)
[75] *See* STEVENS, *supra* note 67 at 4.
[76] AMY BELASCO, TOTAL INFORMATION AWARENESS PROGRAMS: FUNDING, COMPOSITION, AND OVERSIGHT ISSUES 15 (Congressional Research Service, 2003).
[77] *See* United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT), Pub. L. No. 107-56, Stat. (2001).
[78] EPIC USA PATRIOT Act Page, *at* http://www.epic.org/terrorism/usapatriot/ (last visited Mar. 20, 2003).
[79] *See* CHARLES DOYLE, THE USA PATRIOT ACT: A LEGAL ANALYSIS 5 (Congressional Research Service 2002); MARCIA S. SMITH ET AL., THE INTERNET AND THE USA PATRIOT ACT: POTENTIAL IMPLICATIONS FOR ELECTRONIC PRIVACY, SECURITY, COMMERCE, AND GOVERNMENT 2-8 (Congressional Research Service 2002).
[80] Total Information Awareness, http://www.darpa.mil/iao/TIASystems.htm (last visited Mar. 27, 2003).
[81] *Id.*
[82] *See* Erick Schohnfield, *Total Information Delusion*, BUSINESS 2.0 (Feb. 3, 2003), *at* http://www.business2.com/articles/web/print/0,1650,46876,00.html.

[83] *See* text accompanying *supra* note 76.
[84] *See* CHARLOTTE TWIGHT, WATCHING YOU: SYSTEMATIC FEDERAL SURVEILLANCE OF ORDINARY AMERICANS 5 (Cato Institute Briefing Papers, No. 69 2001).
[85] *Id.*
[86] *See* Farmer & Mann, *supra* note 41, at 39.
[87] *Id.*
[88] *See* BELASCO, *supra* note 76, at 11.
[89] *See, e.g.*, PETER G. W. KEEN & RON MACKINTOSH, THE FREEDOM ECONOMY: GAINING THE M-COMMERCE EDGE IN THE ERA OF THE WIRELESS INTERNET (2001).
[90] *See* Andy Dornan, *Can M-Commerce Find a Place in Your Network?*, NETWORK MAG., Nov. 1, 2001, at 38.
[91] *See* Andrew Rimkus, *Location Commerce & Privacy*, M-COMMERCE REV. (a supplement to WIRELESS REV.), Oct. 1, 2000.
[92] *See id.* ("It's clear that the origin of the wireless call or transaction is fast-becoming an asset that providers want.").
[93] *See* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 866-69 (2002).
[94] DoubleClick Inc. Form 10-K for the Fiscal Year Ending Dec. 31, 2000 (filed Mar. 12, 2001).
[95] *See* Spencer, *supra* note 93.
[96] *See* Robert O'Harrow Jr., *Web Ad Firm to Limit Use of Profiles*, WASH. POST, Aug. 27, 2002, at E01.
[97] Tim Kridel, A Sense of Where You Are, ¶ 1 (Nov. 12, 2001), at http://www.theneteconomy.com.
[98] *See* Peter P. Ten Eyck, Note, *Dial 911 and Report a Congressional Empty Promise: The Wireless Communications and Public Safety Act of 1999*, 54 FED. COMM. L.J. 53, 55-56 (2001).
[99] *Id.* at 56 n.15. The figure is not 100% because of the difficulty of some rural telephone systems to establish emergency call centers. *Id.*
[100] *But see* Ben Charny, *Could E911 Have Helped in Disaster?*, C/NET NEWS.COM (Sept. 12, 2001), *at* http://news.com.com/2100-1033-272923.html (arguing that Enhanced 911 would not have done much in a situation such as the World Trade Center collapse, since it would have required technology capable of locating a caller within 1 yard).
[101] *See* United States Cell. Corp. v. FCC, 254 F.3d 78, 80 (D.C. Cir. 2001).
[102] Pub. L. No. 106-81, 113 Stat. 1286.
[103] *See E911 FACT SHEET*, *at* http://www.fcc.gov/911/enhanced/factsheet_requirements_012001 (last visited Mar. 12, 2003) [hereinafter FACT SHEET].
[104] *See id.*
[105] Betsy Harter, *Location Services Stood Up*, M-BUSINESS DAILY ¶ 4 (Oct. 25, 2001), *at* http://www.mbizcentral.com.
[106] *See* FACT SHEET, *supra* note 103.
[107] Joshua Israelson, *On the Edge of Geolocation*, EDN, Mar. 7, 2002, at 35, 35; FACT SHEET, *supra* note 103.
[108] *Hearing on Wireless E911: Hearings Before the Subcomm. on Communications of the Senate Commerce, Science, and Transportation Committee*, 108th Cong. (2003) (statement of Kathleen Q. Abernathy & Jonathan S. Adelstein, Commissioners of the FCC).
[109] *See Press Release, FCC Acts on Wireless Carrier and Public Safety Requests Regarding Enhanced Wireless 911 Services*, Federal Communications Commission, *at* http://www.fcc.gov/Bureaus/Wireless/News_Releases/2001/nrwl0127.html (Oct. 5, 2001).
[110] Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286.
[111] 47 U.S.C. § 222(f) (2000).
[112] 182 F.3d 1224 (10th Cir. 1999) *cert. denied sub nom.* Competition Policy Inst. v. U.S. West, Inc., 530 U.S. 1213 (2000).
[113] *Id.*
[114] 447 U.S. 557, 562-63 (1980).
[115] *Central Hudson*, 447 U.S. at 566; *U.S. West*, 182 F.3d at 1233.

[116] *Central Hudson*, 447 U.S. at 564-65; *U.S. West*, 182 F.3d at 1233.
[117] *U.S. West*, 182 F.3d at 1234 n6 (*citing* Roe v. Wade, 410 U.S. 113, 152-53 (1973)).
[118] *Id.* at 1235.
[119] *Id.*
[120] 47 C.F.R. § 64.2007(b) (1998).
[121] *See In the Matter of Implementation of the Telecommunications Act of 1996*, 17 F.C.C.R. 14860 (2002).
[122] *See* Renenger, *supra* note 10, at 561-62.
[123] 84 F. Supp. 2d 492 (S.D.N.Y. 2000).
[124] *See* U.S. CONST. art. I., sec. 8. cl. 8; The Trademark Cases, 100 U.S. 82 (1879).
[125] 47 U.S.C. § 222(d)(4) (2000).
[126] Location Privacy Protection Act of 2001, S. 1164, 107th Cong. (1999).
[127] *Id.* at § 2(2).
[128] *Id.* at §§ 3(b)(1)(E), 3(b)(4)(c).
[129] CONG. REC. S7497-98 (daily ed. July 11, 2001) (statement of Senator John Edwards).
[130] *Fair Practices Order*, *supra* note 55, at ¶6.
[131] *Id.*, at ¶1.
[132] *In the Matter of Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, Statement of Commissioner Michael J. Copps, Dissenting* , July 24, 2002, at 2. [hereinafter *Copps Dissent*]
[133] *Id.*
[134] *FCC Turns Down CTIA Petition on Wireless Location Privacy Rules*, FCC REP., Aug. 9, 2002 (quoting CTIA President Thomas Wheeler).
[135] The Data-Mining Moratorium Act of 2003, S. 188, 108th Cong. (2003).
[136] *Id.* at § 2.
[137] *See* discussion of Peace's proposed tort in Renenger, *supra* note 10, at 564.
[138] S. 129, 1999-2000 Leg., Reg. Sess. (Cal. 1999) (as amended Aug. 26, 1999).
[139] *See* Renenger, *supra* note 10 at 558. The traditional privacy torts were created as a reaction to Warren & Brandeis' articulation of a right to privacy. *See* Warren & Brandeis, *supra* note 22.
[140] *See* discussion of *Conboy v. AT&T*, 84 F. Supp. 2d 492 (S.D.N.Y. 2000), *supra* text accompanying note 123.
[141] *See supra* note 25.
[142] *See* discussion *infra* Part IV.F.
[143] *See* discussion *infra* Part V.B.
[144] *See* PRIVACY ONLINE, *supra* note 36.
[145] *Id.* at 14.
[146] *See* HAHN & LAYNE-FARRAR, *supra* note 31, at 5.
[147] PRIVACY ONLINE, *supra* note 36, at 16.
[148] EPIC & PRIVACY INTERNATIONAL, PRIVACY AND HUMAN RIGHTS 2002, 3-5. [hereinafter PRIVACY & HR]
[149] Council Directive 95/46/EC, 1995 O.J. (L 281). [hereinafter E.U. Data Directive]
[150] PRIVACY & HR, *supra* note 148, at 4.
[151] *See id.* at 30-33(evaluating the European Directive).
[152] *See id.* at 33 n.148(discussing the Privacy Act of 1974, 5 U.S.C. § 552A (1974)).
[153] E.U. Database Directive, *supra* note 149 at Art. 14(b).
[154] *Telecommunications: Parliament Amends Universal Service Directive*, EUR. REP., June 16, 2001, at Section No. 2601.
[155] Council Directive 2002/58, 2002 O.J. (L 201) 37.
[156] Joe Bailey, *From Public to Private: The Development of the Concept of the "Private,"* SOCIAL RES., Spring 2002, 15, 26
[157] Mikhail Ivanov, *Privacy is Not Everything*, RUSSIAN LIFE, Jan./Feb. 2000, at 64.
[158] Mark Neocleous, *Privacy, Secrecy, Idiocy*, SOCIAL RES., Spring 2002, at 85, 103, *quoting* SAMUEL JOHNSON, A DICTIONARY OF THE ENGLISH LANGUAGE.

[159] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (1950).
[160] X v. Iceland, 5 Eur. Comm'n H.R. 86.87 (1976).
[161] Matthew M. Werdegar, Note, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 STAN. L. & POL'Y REV. 103, 103 (1998)(describing the case of Karen Nelson, who died in a South Dakota snow bank when rescue workers were unable to pinpoint the location of her cell phone call).
[162] *See* Fulch & Soares, *supra* note 10
[163] HAHN & LAYNE-FARRAR, *supra* note 31.
[164] *Id*. at 8.
[165] U.S. West v. FCC, 182 F.3d 1224 (10th Cir. 1999); *see also supra* note 32; *supra* Part IV.B.2.
[166] *See* PETER P. SWIRE, MARKETS, SELF-REGULATION, AND GOVERNMENT ENFORCEMENT IN THE PROTECTION OF PERSONAL INFORMATION (1997); Ellen Traupman, Comment, *Who Knows Where You Are? Privacy and Wireless Services*, 10 COMMLAW CONSPECTUS 133, 152 (2001); at 152; Scott Foster, *Online Profiling is on the Rise: How Long Until the United States and the European Union Lose Patience with Self-Regulation?*, 41 SANTA CLARA L. REV. 255, 266-67 (2000).
[167] *See* Traupman, *supra* note 166, at 152.
[168] *See* Fulch & Soares, *supra* note 10 at ¶13.
[169] *Id*. at ¶8.
[170] *See infra* Part IV.C.2.
[171] *See* Traupman, *supra* note 166, at 152 n.162, 152 n.165.
[172] HAHN & LAYNE-FARRAR, *supra* note 31, at 69.
[173] *See id*. at 78-80 (table 4 details the various types of economic impact on industry); Part IV.F (detailing the FTC's fair information practices).
[174] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1249-59 (1998).
[175] *Borders Books Kills Face-Scanning Plan Amid Criticism*, COMP. WORLD, Aug. 27, 2001 *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,63359,00.html.
[176] *CRANKY CONSUMER, The Discount Grocery Cards That Don't Save You Money*, WALL ST. J., Jan. 21, 2003.
[177] *See* text accompanying *supra* note 58.
[178] *See* text accompanying *supra* notes 174-174.
[179] *See supra* Part IV.C.
[180] *See supra* Part IV.C.2.