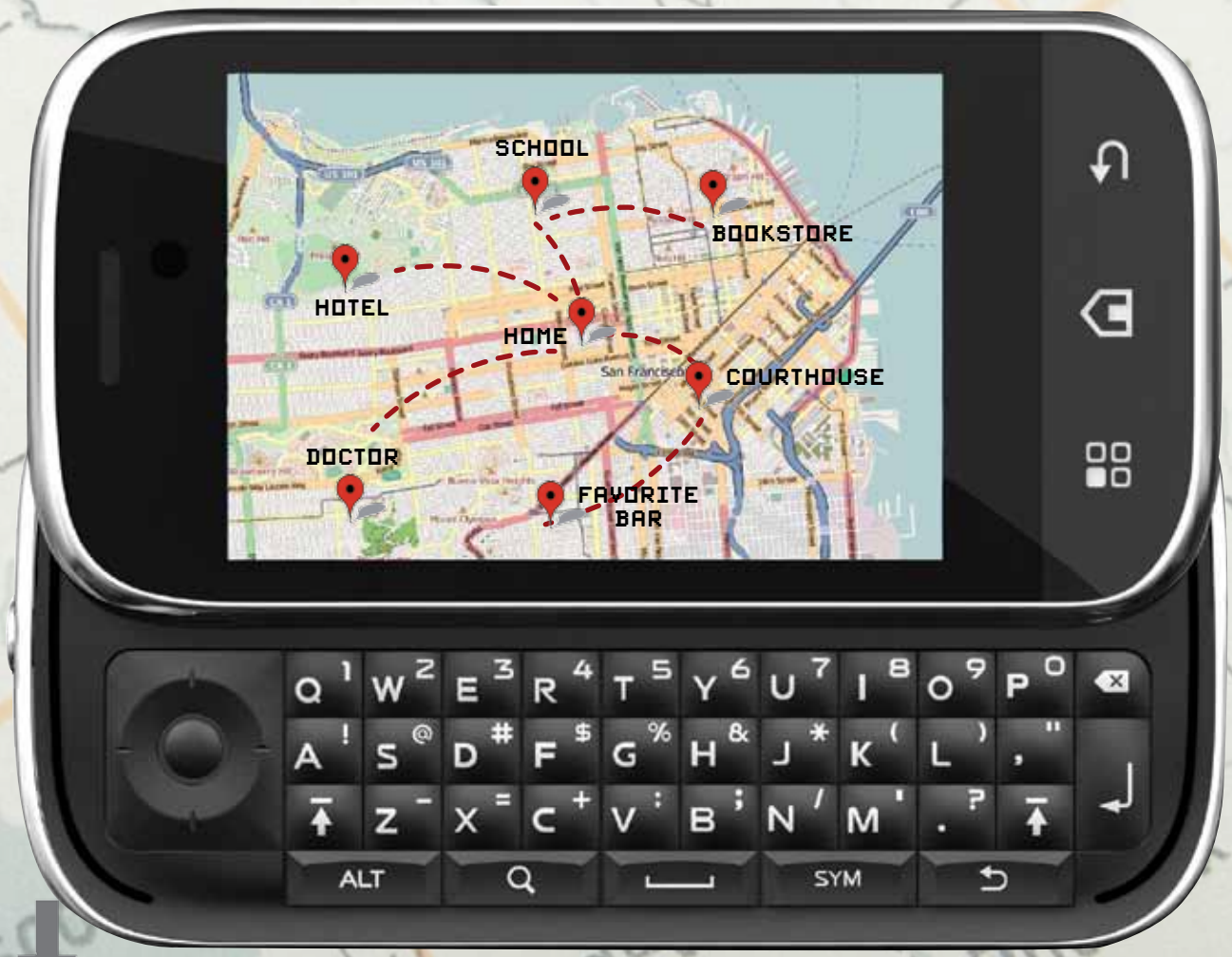


Location-Based Services: Time for a Privacy Check-In

A publication of the ACLU of Northern California
Available online at www.DotRights.org

Need to get directions when you are lost? Looking for a restaurant nearby? Want to know if your friends are in the neighborhood? Location-based services—applications and websites that provide services or information based on your current location—can put this information and more in the palm of your hand. But while it may be easy to find people or places, finding the privacy protections for all of the sensitive data collected by these location-based services can be far more difficult. Can location-based services protect your privacy? Do they? And what can we do to improve the situation?

Location-Based Services: Time for a Privacy Check-In is the third in a series of issue papers by the ACLU of Northern California that discuss new technology trends and their consequences. This paper examines the current state of legal and technical privacy protections for users of location-based services and explores opportunities for consumers, businesses, and policymakers to work together to update and enhance these protections.

Part I of this paper provides background information on location-based services. Part II examines the privacy concerns that arise from the use of location-based services and Part III surveys the current state of privacy protections for consumers of these services. Finally, Part IV identifies opportunities for consumers, businesses, and policymakers to reinforce privacy protections for location information so that individuals are not forced to pay for location-based services with control over their personal information.

For more information about location-based services and other emerging technology and online privacy issues, please visit the ACLU of Northern California's Demand Your dotRights campaign website at **www.dotRights.org.**

TABLE OF CONTENTS

CONTRIBUTING WRITERS: Nicole A. Ozer, Chris Conley, Hari O'Connell, Ellen Ginsburg, Tamar Gubins

Thank you to the staff of the ACLU Speech, Privacy, and Technology Project, the ACLU Washington Legislative Office, and Caitlin O'Neill and Alex Reicher for their assistance with this issue paper.

DESIGN AND LAYOUT: Gigi Pandian, ACLU of Northern California

MAP IMAGE ON FRONT COVER: Map data © OpenStreetMap contributors, CC-BY-SA

For more information about location-based services and other online privacy issues, please contact the Technology and Civil Liberties Program at the ACLU of Northern California and visit our online privacy website at www.dotRights.org.

The ACLU of Northern California wishes to thank the following funders for their support of this publication:

- Block v. eBay cy pres fund
- California Consumer Protection Foundation
- Consumer Privacy Cases cy pres fund
- Goodwin Procter LLP
- Howard Rice Nemerovski Canady Falk & Rabkin
- Rose Foundation for Communities and the Environment

INTRODUCTION

Location-based services (LBS)—applications that provide information to users based on their location—are a growing business. From social networking to navigation to banking, consumers are being offered a range of new location-based services. But every time a consumer uses one of these services, there is a risk that the company offering the service may be collecting and retaining detailed records of who she is, where she goes, and what she does. Once collected, outdated privacy laws and varying corporate practices can leave this sensitive information vulnerable to access by the government and third parties. What are the privacy implications of LBS, and how can businesses, policymakers, public interest groups, and consumers work together to update the laws and create stronger policies so that consumers can feel confident using these services?

LBS are rapidly expanding in both number and variety. They offer a wide range of services: navigation tools to help you reach your destination (e.g., MapQuest); local search to help you find nearby businesses or events (e.g., Yelp); friend-finders and social networking (e.g., Loopt and Google Buzz); applications that allow you to "check in" at certain locations (e.g., foursquare); and applications that can link your location to other activities (e.g., Twitter and Facebook). Many users currently access LBS through mobile phones, but location-aware devices such as laptop and desktop computers, iPads, and in-car navigation and assistance systems can also be used to access many of these services.

LBS offer tailored services that respond as you move from one place to another. But by using LBS, consumers may unknowingly allow companies to compile detailed profiles of their lives: the places they visit, the events they attend, the people they meet, and more. And if LBS assemble these consumer profiles, other parties—especially the government—may be eager to access this sensitive personal information. Americans should not be forced to choose between using new technology and keeping control of the private details of their lives. Instead, they have the right to expect that new technologies will improve their lives without invading their privacy.

Unfortunately, legal protections have not kept pace with technological change. Constitutional privacy protections have yet to account for the fact that LBS are capable of generating detailed records that may reveal intimate and personal facts about a person's life, facts that are rightly considered private. Existing privacy statutes were written decades ago, before LBS even existed. And many LBS privacy policies do more to protect company interests than to safeguard consumer privacy. As a result, the privacy protection for information collected, held, and shared by LBS providers is often inadequate or uncertain. As LBS become more popular and more central to the way Americans interact with technology and with each other, ensuring that there are strong and clear protections for the information they collect will be essential to building consumer trust, ensuring the long-term success of LBS, and protecting privacy.

Part I of this paper provides background information on LBS and the information that they collect and use. Part II examines the privacy concerns that arise from this collection. Part III surveys the current state of privacy protections for information held by LBS providers. Finally, Part IV identifies opportunities for consumers, businesses, and policymakers to work together to reinforce privacy protections for location information so that individuals are not forced to choose between using new LBS and keeping control of their personal information.

In several areas of this paper we have more questions than answers. It is our hope that this issue paper will help to support a robust conversation between companies, policymakers, public interest groups, and consumers about these important issues and encourage efforts to update and develop more robust legal and practical privacy protections for information held by location-based services.

PART I: UNDERSTANDING LOCATION-BASED SERVICES

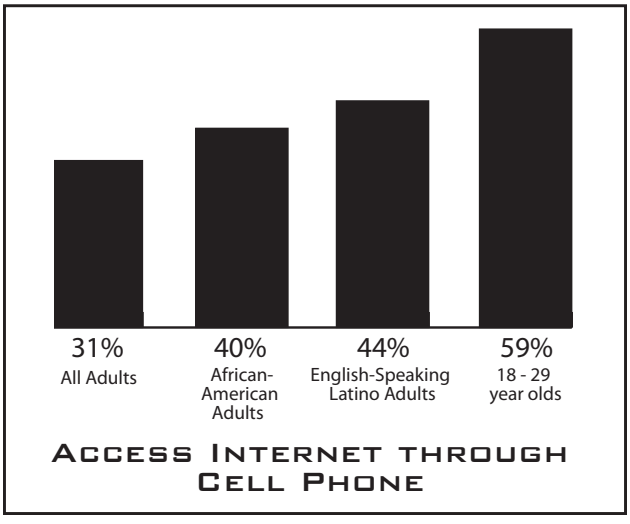
You do not have to own a smartphone to find yourself using LBS on a regular basis. If you have ever received a live traffic update from your navigation device or even searched for "pizza" on a search engine, you have probably used a location-based service. For purposes of this paper, a location-based service is any application or service that receives a consumer's location and provides that consumer with information or services tailored to that location.[1] LBS provide a wide range of services and run on a variety of platforms. Many of these LBS are able to collect and retain detailed records of the location of consumers and combine these records with other information to build profiles revealing the details of consumers' personal lives. As the actual and potential markets for LBS grow, so too does the need to address the implications for consumer privacy.

LBS provide a wide range of services and run on many different devices. Most consumers with a smartphone have access to a variety of LBS: navigation tools such as MapQuest or Google Maps provide driving directions and real-time traffic information, social networking applications like Loopt notify consumers when their friends are nearby, and foursquare and Gowalla let consumers "check in" at specific locations. But consumers may also use LBS when they use a search engine on their personal computer (some search engines generate advertisements and display results based on approximate location),[2] or when an in-car navigation system provides live traffic updates. LBS are also used for myriad other purposes such as campus safety,[3] education,[4] financial management,[5] and dating.[6] Some LBS such as "Future Checkin" and Booyah's "InCrowd" are even built on top of other LBS.[7] It is likely that even more varieties of LBS are on the horizon.

LBS may collect and use vast amounts of information about consumers for a wide range of purposes. By definition, every LBS determines the consumer's location (using one or more of several methods; see sidebar) to provide its service. This location information may be used once for a single purpose, or it may be stored or combined with other information to produce a history of the consumer's activities or a more detailed profile for advertising or other purposes.[8] Search engines may combine location information with search terms entered or results selected. Navigation tools could determine driving speed to inform their traffic estimates. Social networking services may collect and retain location data along with photos, status updates and comments, and information about friends, interests, gender and sexual orientation, and more.[9] For example, when it announced its new Places LBS, Facebook stated that it wants to help build "our collective memory" by enabling users to share details with future generations about "where your parents had their first kiss, here are the photos, this is what their friends said about it."[10]

The popularity of LBS is rapidly growing due in part to the increased use of location-enabled devices like smartphones and iPads. As of May 2010, approximately 49 million people in the United States owned smartphones.[11] Mobile devices, including smartphones, are particularly popular with younger consumers and people of color. According to a 2010 study, roughly 90 percent of Americans between the ages of 18 and 29 own mobile phones (compared to 82 percent of all American adults), and 65 percent of such owners use their device to access the Internet. Similarly, 87 percent of African-Americans and English-speaking Latino/as own cell phones, with 51 percent of African-American phone owners and 46 percent of Latino/a phone owners accessing the Internet through their phone.[12]

Increasing ownership of smartphones is already beginning to translate into growth in the LBS market. A February 2010 study found that there were almost 6,000 location-aware applications for the iPhone, as well as 900 for the nascent Android marketplace and 300 for the Blackberry.[13] Recent research found that one in four U.S. adults have used LBS, and that two-thirds of all iPhone users access LBS at least once a week.[14] And leading LBS are seeing explosive growth: foursquare doubled its user base to more than two million registered users over just a three-month period ending in July 2010,[15] and in May 2010 Yelp's iPhone application accounted for 27 percent of the total searches on the service and led to almost one million requests for point-to-point directions to a local business.[16] As location-enabled devices become the norm, the potential market for LBS is likely to continue to expand.



ACCESS INTERNET THROUGH CELL PHONE

But the proliferation of location-enabled devices and LBS providers also means that an ever-growing number of companies possess detailed and sensitive records about users. If consumers are going to be able to use these services with confidence, their personal information must be properly protected.

How do location-based services determine your location?

- **Cell tower-based identification:** Cell phones can determine their own location based on nearby cell-relay towers and provide this information to LBS running on the phone. Currently this information is accurate to within 100 meters—the length of a football field or city block—and is becoming more accurate as more cell towers are deployed.[17]

- **Global Positioning System (GPS):** GPS-enabled devices receive signals from a network of satellites and use these to triangulate the device's location. GPS location information is accurate to within 20 meters—which can place the device at a specific location, like a church or doctor's office.[18]

- **WiFi Triangulation:** Some devices and services determine location by surveying signals of nearby wireless networks, and comparing those signals to a list of known wireless access points.[19] WiFi Triangulation is accurate to within 200 meters.

- **Internet Protocol (IP) Address Approximation:** Any website or Internet-based service can approximate a device's location based on its IP address, which roughly maps to geographic location. The precision of IP approximation varies; generic addresses may only identify a given metro area,[20] while certain IP addresses can identify a specific university campus or other location.

- **User-Provided Information:** LBS can also simply ask the user to manually supply their current location.[21] The accuracy and precision of this method is up to the service and user.

PART II: THE IMPORTANCE OF PRIVACY FOR LOCATION-BASED SERVICES

Privacy is both an individual and a social good. As individuals, privacy gives us the autonomy to address sensitive issues without fear of exposure, the ability to explore facets of our personality and individuality, and the power to form close bonds with some by excluding others. Privacy allows a healthy society to experiment and grow, and safeguards the balance between individual liberties and government powers. As such, privacy is a fundamental building block of a robust democracy. But this privacy, autonomy, and control over personal information, so essential to American society, may be at risk as consumers increasingly place their personal information into the hands of LBS developers.

The tools necessary for pervasive, detailed tracking are already in your pocket or purse. The information collected and held by LBS can expose highly personal information: where a consumer goes, whom she sees, and what she does. Failing to protect this information threatens not only the right to privacy but also the freedoms of expression and association. The threat is already being realized. Unless privacy protections for the information collected by LBS are reinforced, the potential growth of LBS may be stifled.

LOCATION-BASED SERVICES POSE SIGNIFICANT PRIVACY RISKS

Location information collected from consumers, knowingly and unknowingly, can reveal far more than just a consumer's latitude and longitude. Knowing where a consumer is can mean knowing what he is doing: attending a religious service or a support meeting, visiting a doctor's office, shopping for an engagement ring, playing hooky from work, or spending an evening at the corner bar. It might reveal that he is interviewing for a new job or "out" him as a participant at a gun rally or a peace protest. It can mean knowing with whom he spends time, and how often. When location data is aggregated it can reveal his regular habits and routines—and when he deviates from them.[22] Depending upon the information and who learns it, the ramifications could range from annoying to embarrassing to downright dangerous.[23] Robberies have been linked to location status updates[24] and GPS technology already has been involved in a significant number of stalking cases.[25]

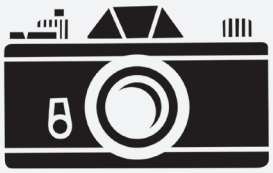
> *"The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church-goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."*
>
> *—United States v. Maynard (2010)*[26]

Many LBS collect vast amounts of location information that may be stored indefinitely.[27] LBS may collect information about a user's location even when she is not actively using the LBS, either by passively monitoring her device's location or by receiving information shared by friends or colleagues.[28] Many LBS retain location information indefinitely unless the user manually deletes her records, and some do not even permit this option.[29] Thus, LBS have the potential to compile a robust history of a person's location.

Further, LBS may combine location information with other data to profile a consumer's activities and connections in even greater detail. LBS may collect information about consumers—such as real name and identity, interests, or friends and co-workers—from the consumer herself, or even acquire this information from third parties.[30] They may link the user's location to other activities such as financial transactions.[31] The combination of location data and other information increases the possible harm if this information were abused.

The risk of disclosure is heightened by the fact that the proliferation of LBS places sensitive information in the hands of many parties, any one of whom could reveal that data. When many different companies hold copies of valuable information about consumers, the privacy protection afforded to consumers is only as strong as the weakest link. Unfortunately, in a climate lacking both clear legal protections and strong privacy safeguards provided by LBS themselves, consumers are starting to recognize and experience privacy failures.

GEOTAGGING



An increasing number of devices like smart phones, video cameras and digital cameras are using location information to "geotag" your photos and videos. If you have ever used the camera function on an iPhone and clicked "OK" when told that "'Camera' Would Like to Use Your Current Location," you have geotagged a photo or video. The device determines your current location (often using its built-in GPS) and then attaches this information as hidden "metadata" that may be carried with the image wherever it goes. Recent research shows that many photos and videos associated with websites and services such as Flickr, YouTube, Craigslist, and Twitter are geotagged.[32]

Although geotag information may be used for creative purposes, such as maps of all tagged photos and videos uploaded to Flickr[33] and YouTube,[34] it may also compromise privacy. For example, many Craigslist users have chosen to anonymize their identity and conceal their exact address—and then compromised these protections by linking a geotagged photo to an item they post for sale. Even Adam Savage, host of the popular science television show "MythBusters," unknowingly revealed his home address when he used TwitPics to post a picture of his car and the message "Now it's off to work."[35]

Some companies are taking steps to safeguard consumer privacy. Flickr is now blocking access to geotag data on images taken with smartphones unless a user opts in to that function, and Facebook strips any geotags off of the more than 100 million photos that are uploaded to the site every day.[36]

Since location data is collected in the background, it is easy to forget that posting a photo or video on a website may reveal more than meets the eye. More needs to be done to make it clear to consumers when images are being geotagged. One step in the right direction would be to make it easier to turn off the geotagging function and to ensure that sensitive location information is protected when photos and videos are uploaded to other services.

WARNING SIGNS HIGHLIGHT THE NEED FOR CHANGE

Law enforcement agents are already aggressively seeking massive amounts of information about consumer location, at times under questionable circumstances that highlight the potential for abuse of this information. For example:

- In 2009, a Sprint representative provided a rare glimpse into the scope of government demands for location data when he revealed that the company's automated system of handling law enforcement requests for location information had been used more than ***8 million times*** over a 13-month period.[37]
- In 2010, FBI agents investigating a series of bank robberies demanded the records of every cell phone that was near each bank when it was robbed.[38]
- In 2010, Michigan police officers sought information about every cell phone near the site of a planned labor protest.[39]
- An Alabama sheriff demanded that a telecommunications company track his daughter's location without a warrant when she didn't come home from a date, claiming that she had been kidnapped.[40]
- In 2008, the FBI sought and received location-tracking information not just for a robbery suspect, but for 180 other innocent people—all without a warrant.[41]

These examples are likely just the tip of the iceberg. As noted above, much of this location tracking is happening in secret, and the parties involved typically do not have much incentive to draw attention to the activities. Law enforcement officials may want to avoid disclosing their investigatory techniques, and telecommunications carriers may want to avoid any potential backlash from their customers. Without transparency and oversight, LBS are likely to become targets for similar broad-ranging government demands as they become more popular.

Consumers are starting to worry about location privacy. A recent study found that 55 percent of those already using LBS are concerned about loss of privacy.[42] Many fear for their personal safety and want to make sure that their current location or home address is protected from those who may want to harm them. Others are troubled about receiving unwanted advertisements based on their location.[43] Many consumers believe that these and other risks associated with location-sharing technologies generally outweigh the benefits.[44] Consumers are right to be nervous about location privacy. Location-based services may facilitate social interaction and provide users with helpful information about their surroundings, but they also present real risks to privacy. Unfortunately, those risks are exacerbated by outdated laws that do not adequately protect the privacy of information held by LBS.

55 percent of those already using LBS are concerned about loss of privacy.

PART III: LEGAL PRIVACY PROTECTIONS AND LOCATION-BASED SERVICES

While LBS are growing more sophisticated, enabling the collection of increasingly detailed information about consumers' physical locations and other aspects of their personal lives, privacy laws are mired in the past and fail to provide the necessary legal protections for this sensitive information.

Court decisions over the past 40 years leave it unclear whether the Constitution requires law enforcement officers to obtain a judicially-approved search warrant before accessing the various types of information that may be collected by LBS. Likewise, the decades-old patchwork of statutory electronic privacy laws often creates more questions than answers about the privacy protections for this information. Privacy policies, which are effectively contracts between a consumer and an LBS provider, often fail to provide additional protection. For now, consumers, LBS providers, and the government alike are acting in a legal domain filled with gray areas.

Ultimately, this lack of legal clarity benefits no one. Consumers are unsure how using LBS affects their privacy. Providers are confused whether they may, must, or must not disclose consumer information in various circumstances, and may be hampered in attracting consumers who have privacy concerns. Even law enforcement officials are encumbered when confusion leads providers to resist legitimate requests for information.

The following sections examine the three basic categories of legal protection for location information: constitutional protections, statutory protections, and privacy policies. Each currently falls short of fully protecting the interests of consumers and businesses. Courts, policymakers, and companies all need to use the tools at their disposal to clarify and extend these legal protections and ensure the privacy of information collected by LBS.

CONSTITUTIONAL PROTECTIONS: LOCATION-BASED SERVICES AND THE THIRD-PARTY DOCTRINE

Privacy is an essential civil liberty protected both by the United States Constitution and several state constitutions, including the California State Constitution.[45] However, because location-based technology is so new and the judicial process moves slowly, courts have yet to address the specific issue of how constitutional protections apply to the type of information held by LBS. Until the courts provide a clear statement of the constitutional protections for information held by LBS, law enforcement agents and other third parties may continue to try to take advantage of loopholes and gray areas in the existing legal doctrine to demand a great deal of information from LBS.

The Fourth Amendment prohibits "unreasonable searches and seizures."[46] If an individual has a "reasonable expectation of privacy," the government generally must obtain a warrant and show probable cause prior to any search or seizure.[47] This test balances the privacy rights of the individual with the legitimate aims of law enforcement and other government actors. To make sure that the government is not improperly intruding on a person's privacy, the Constitution requires the government to prove to a judge that it has a good reason to think that the information it seeks will turn up evidence of a crime.

A court's decision of whether to apply Fourth Amendment protection to information held by LBS may turn on one or both of two questions: First, do consumers have a reasonable expectation of privacy related to the type of information collected by the LBS? Second, does the fact that the information is collected and held by a LBS affect its privacy protection? Depending on the circumstances and the court's interpretation of the law, the answer to either question could determine whether information held by a location-based service is protected by the Constitution.

Courts continue to grapple with the issue of whether an individual has a reasonable expectation of privacy in his or her location. The Supreme Court has not addressed location privacy since the 1980s, when the tracking technologies available were much cruder. In cases from that era, the Court held that the government must obtain a warrant before using technology to infer facts about "location[s] not open to visual surveillance," but that no warrant was necessary to track someone in purely public locations.[48] However, tracking technology has come a long way since the '80s. Modern technologies make it possible to track an individual in great detail over a prolonged period of time, 24 hours a day. Lower courts have come to conflicting conclusions about whether the more comprehensive and invasive nature of this tracking triggers the Fourth Amendment's warrant requirement even when individuals are in public spaces.[49]

The constitutional analysis is further muddied by the potential application of the "third-party doctrine." This doctrine, which was established in a pair of pre-Internet Supreme Court cases, suggests that there is no reasonable expectation of privacy, and thus no Fourth Amendment privacy protection, in information relinquished to a third-party business.[50] Despite this doctrine, courts have long extended the protection of the Fourth Amendment to the contents of documents or communications even when they are in the possession of third parties, such as files on a personal computer completely under the control of another[51] or on a networked computer accessible by third parties.[52] More recently, courts have begun to consider the application of the Fourth Amendment and the third-party doctrine to online services such as web-based email, producing conflicting results.[53] However, courts have not yet considered the third-party doctrine or related questions in cases directly involving LBS.

Ultimately, the only thing that is clear about constitutional protections for location-based service information is the lack of clarity.

Whether the government must get a warrant to obtain data collected by LBS may be particularly difficult to resolve given the variety and complexity of LBS. Should the privacy protection of location information be affected by the manner in which it is generated?[54] Does "social sharing" of location information affect its constitutional protection? Does information that is automatically transmitted to a location-based service without the device owner's knowledge or informed consent fall under the third-party doctrine?[55] Is location information used for advertising purposes constitutionally different from location information used solely to provide directions from Point A to Point B? Does the fact that the user can choose whether to retain or delete records matter? Does the specific language of a location-based service's privacy policy have any impact?[56] The number and complexity of these questions, and the slow pace of the legal process, suggest that courts may struggle with the constitutional protections for information held by LBS for many years.

Finally, courts may be faced with yet another question: whether and how state constitutional protections apply to LBS information. State constitutions offer privacy protections that often differ dramatically from that offered by the Fourth Amendment as interpreted by federal courts. For example, the California Supreme Court has explicitly rejected the third-party doctrine as a limitation on the right to privacy in the state constitution.[57] Thus, the privacy protections for location information could differ depending on the state where a consumer lives or where a location-based service stores its data.

Ultimately, the only thing that is clear about constitutional protections for LBS information is the lack of clarity. In the absence of clear constitutional protection, consumers may need to rely on other avenues, such as statutory protections, to safeguard the privacy of their LBS information.

STATUTORY PROTECTIONS: LOCATION-BASED SERVICES AND STATUTORY LAW

Federal and state legislation can provide additional sources of privacy protection above and beyond the protections provided by the Constitution as interpreted by the courts. Such statutory law can be particularly important in providing greater certainty in a situation, as with LBS, where technology has advanced and constitutional protections have not yet been firmly established. Unfortunately, statutory law that should apply to LBS is woefully outdated and also does not provide adequate clarity.

The primary federal law that should—but does not—provide clear statutory protection for LBS information is the Electronic Communications Privacy Act (ECPA).[58] Congress was concerned that information in the control of third parties "may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties" and designed ECPA to provide statutory protection for electronic communications and records (in transit or in storage) to supplement the protections offered by the Constitution.[59]

Unfortunately, ECPA was enacted in 1986, back when available technologies included a two-pound cell phone and the World Wide Web did not even exist. ECPA did not anticipate many of the technologies that we use today and the sensitive personal information that would be collected and stored by these services. While ECPA was forward-thinking legislation in 1986, technological advances have outpaced its protections. In the last 24 years, these new technologies have become a ubiquitous part of American life. As such, concerns about consumer privacy are not only again relevant, but in many ways, even more critical today.

It is particularly difficult to apply an outdated law such as ECPA to the rapidly evolving world of LBS. Does a particular location-based service constitute an "electronic communication service"[61] or a "remote computing service"[62] as defined by ECPA, each of which carries different protections? Is all location data collected by LBS "content," which receives the highest level of protection?[63] Does the fact that cell phones automatically transmit information make them "tracking devices" subject to a standard of probable cause?[64] These questions and more challenge judges and lawyers who attempt to apply ECPA's outdated language to modern technologies such as LBS. Lacking modern laws for modern technology, judges are constantly forced to fit square pegs into round holes.

> *"With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. ... For the person or business whose records are involved, the privacy or proprietary interest in that information should not change."*
>
> *—Senate Judiciary Committee (1986)[60]*

In addition to providing questionable privacy protections, ECPA also lacks a mechanism to provide transparency or recordkeeping around demands for LBS information. Unlike a traditional search of a house or physical space, demands for electronic records from a third party can be carried out easily without the subject's knowledge and are often issued under seal or subject to a gag order.[65] Sealed surveillance applications are not made public so only the court and the government knows about them. Because the government has no motivation to move to unseal the orders or reveal how often these demands are made, they may never become public. While a suspect who is eventually charged with a crime may become aware of surveillance through the discovery process, innocent people may never find out that they too were subject to surreptitious tracking.[66]

Moreover, while the federal Wiretap Act requires prosecutors and courts to provide Congress with information detailing the nature and scope of intercepted communications,[67] reporting about demands for electronic information is not required under ECPA. Without the aggregate data of demands that such a report would provide, and in ignorance of individual orders issued under seal, lawmakers and the public are largely unaware about the extent of law enforcement demands for electronic information.

As with government access to information, technology has also outstripped statutory protections in the commercial context. Telecommunication carriers are generally prohibited from disclosing "customer proprietary network information" (CPNI), which includes some information relating to the location of a customer.[68] Unfortunately, these CPNI rules—which some considered groundbreaking protections when enacted—no longer provide sufficient protection for today's location-based technology because they do not include location technologies independent of telecommunication carriers, like many LBS.[69]

Lacking clear-cut protection for LBS information from federal or state constitutions, consumers should be able to turn to legislative efforts to bridge the gap and safeguard their rights. ECPA, a statute enacted over two decades ago and not substantially updated since that time, and other statutory laws are clearly inadequate to that task. Lawmakers need to recognize the confusion that the current system creates and act decisively to provide consumers with the protection they deserve.

CORPORATE PRACTICES AND PRIVACY POLICIES

An additional area of potential protection for consumers lies with the companies that provide LBS. These companies have the opportunity to establish practices that protect individual privacy and to codify those practices in a clear privacy policy. Unfortunately, the reality is that most "privacy" policies and corporate practices do little to protect consumer privacy, instead often reserving broad latitude for the company at the potential expense of the consumer.

According to a recent study, only 66 percent of LBS have any privacy policy at all,[70] and some of those that do exist fail to specify what information is collected or how long it is retained.[71] Other privacy policies permit companies to collect vast amounts of information about consumers, keep that information for an extended period of time, and use it in any way that the company can imagine. Consumers are often given limited and difficult-to-use privacy controls.[72] Finally, consumers may receive no assurance that the company will protect information from inappropriate demands for information from third parties.

Research shows that consumers feel more comfortable sharing personal information with companies that have clear privacy policies.[73] Companies looking to succeed in the emerging and competitive market for LBS should take note of consumer desires for strong privacy practices.

PART IV: REINFORCING PRIVACY PROTECTIONS FOR LOCATION-BASED SERVICES

As LBS continue to develop, it is critical to establish mechanisms—legal, technological, and social—to protect the privacy of consumers. Courts and policymakers need to recognize the realities of modern technology and satisfy consumers' continued expectations of privacy. Companies should invest in privacy-friendly technologies and practices that put consumers in control of their own location information. They should also support legal reform to update the outdated constitutional and statutory understandings of location privacy. Consumers also have a role to play: by using their collective voice, they can demand stronger protections and meaningful controls from companies and policymakers. Together, we can pave the way for expanded use of LBS by ensuring that legal, technological, and social mechanisms adequately safeguard consumer privacy.

LEGAL REFORM: PRIVACY LAWS DON'T AUTO-UPDATE

Technology has developed at an astounding rate in the past two decades, but the law has not kept pace. The law needs to evolve to match today's new online and mobile world and properly safeguard the privacy rights of individuals. Consumers need a clear set of rules that will provide clarity for companies and law enforcement while safeguarding the privacy of consumers who use LBS.

CONSTITUTIONAL PRIVACY PROTECTIONS SHOULD APPLY TO LOCATION-BASED SERVICES

Courts need to clearly establish that location information and other records held by LBS are protected by federal and state constitutions from warrantless demands for disclosure. Doing so will ensure that privacy, one of the fundamental building blocks of our democracy, is not slowly eroded by advancing technology and social changes. Instead, extending the protection of the Fourth Amendment to LBS will allow consumers to enjoy the benefits of these new services without being forced to sacrifice their constitutionally protected freedoms in exchange.

EXISTING STATUTORY PRIVACY PROTECTIONS NEED A TECHNOLOGICAL UPGRADE

Lawmakers need to reform ECPA and other privacy rules to address the technologies that are part of our daily lives and provide updated statutory protection for online privacy. LBS and telecommunications carriers should both be required to protect location privacy, and location information and other sensitive information collected by either carriers or LBS should only be accessible to law enforcement with a warrant supported by probable cause. This will restore not only fairness and the privacy Americans are due but also clarity. Consumers and businesses should not be required to puzzle out confusing legal distinctions between an "electronic communication service" and a "remote computing service" or between "content" and "transactional information" in order to determine if and when this information must be disclosed to a police officer.

LAWS SHOULD REQUIRE REPORTING OF DEMANDS FOR LOCATION-BASED SERVICE INFORMATION

Legal reform is needed to ensure that consumers and lawmakers have enough information about demands for LBS data to make informed decisions. As Supreme Court Justice Louis Brandeis once said, "sunlight is said to be the best of disinfectants."[74] Unfortunately, policymakers and consumers are currently in the dark as to the scope of government demands for location information and information held by LBS. While there are reporting requirements for other types of surveillance, such as wiretaps on phones, there is no similar requirement that encompasses LBS.[75] In addition, few companies are willing to voluntarily disclose how often they comply, or are asked to comply, with law enforcement requests for location information.[76]

To fully understand the extent to which government officials demand, receive, and utilize information collected by LBS, consumers and lawmakers need to know the following:

- the number and type of demands (e.g., "informal request," subpoena, search warrant) issued, and by what agency or office;
- the scope of demands, including the type of records sought, the quantity and timeframe of information sought, and the number of consumers whose records were sought;
- the responses to demands, including the number of demands that were legally challenged and the results of such challenges; and the number of demands that were sealed, the affected number of consumers that were not notified, and the length of time the seal was in place;
- the number of arrests, trials, and convictions resulting from disclosure; and
- the costs involved to the public of demands, including reimbursements made to LBS services, costs incurred while negotiating or litigating demands, and manpower and any other resources associated with demands.

While much of this information could be obtained from either reporting by government agencies or businesses, ideally both the government and LBS providers would report on demands and disclosure. Government reporting would provide a clear picture of the scope of demands made by law enforcement and other agencies and allow policymakers and taxpayers to evaluate the costs and benefits of issuing demands to LBS providers. Meanwhile, reporting by individual companies would provide transparency to consumers about the risks to personal data of using a particular location-based service. The two sets of data could also serve as a check on the other, encouraging both parties to fully record and report any government requests or demands for information.

BUSINESS PRACTICES: COMPANIES CAN LEAD THE WAY

Businesses have an important role to play in helping to safeguard the privacy of their consumers and building trust in location-based services.[77] LBS providers should provide strong privacy protection for their own users through robust privacy practices and the use of privacy-enhancing technologies such as anonymization and encryption. They can also improve the environment for LBS by pushing policymakers to enact stronger privacy laws and regulations that protect LBS information from disclosure to the government without a warrant.

LOCATION-BASED SERVICE PROVIDERS SHOULD ESTABLISH AND FOLLOW ROBUST PRIVACY PRACTICES

Businesses have the opportunity to proactively address consumer concern and help to avoid negative press, government investigations, and costly lawsuits by establishing and following robust privacy practices.[78] They can begin by committing to the core principles of the Fair Information Practice Principles[79] and making conscious, privacy-aware decisions about what user information they will collect, how this information will be used and retained, and how they will handle third-party requests or demands for this information.[80] Once they have made privacy-aware decisions about their own practices, they need to communicate these safeguards to users by producing and following a clear and robust privacy policy.

LBS providers should think carefully about what information to collect and for how long to retain and use it to avoid privacy disasters, security breaches, and time-consuming demands for information from the government or third parties down the line.[81] Only companies that develop robust privacy policies that anticipate potential conflict and lay out procedures to safeguard user privacy to the greatest extent possible will meet user expectations during these difficult situations; those that do not may find themselves alienating both existing and potential users.

Some companies have already recognized the value of establishing strong privacy practices backed by a clear privacy policy. For example, WHERE promises consumers that it does not "collect, maintain or track your location history" or "enable or allow location tracking in any form."[82] Mologogo deletes the GPS data that it collects after one month.[83] Loopt maintains only a user's most recent location and the location associated with content geotagged by the user.[84] Other companies should follow these examples and build user trust and avoid costly demands or disclosures by establishing and following strong privacy practices.

The more "locks" a provider puts in the consumer's control, the less likely it is that third parties will be asking providers for the keys.

LOCATION-BASED SERVICE PROVIDERS SHOULD PROTECT USER INFORMATION WITH ALL AVAILABLE TECHNICAL TOOLS

Companies can also improve trust in LBS by using technological tools that protect user privacy. LBS should provide controls that allow users to view, edit, and delete their own information, including choosing which (if any) other users or services can access their information. LBS should also routinely delete data and use effective anonymization and blurring procedures that do more than remove obvious identity markers.[85] Companies should also create a solid data security plan, including access controls to prevent unauthorized access to data and encryption of data. By designing a service with technical measures to protect consumers, LBS can both protect privacy and boost consumer confidence.

Some companies are already utilizing approaches such as these to help protect user privacy. Google Latitude, for example, clearly states that "Google stores only the most recent automatic update or location selection you manually entered on our servers. If you hide in Latitude, we don't store your location."[86] Locaccino, a friend-finder LBS, allows users to define time- and location-based rules, such as allowing coworkers to access the user's location only during business hours.[87] FireEagle allows users to determine the granularity of the location information they reveal.[88]

Providing technical measures that protect and secure consumer information may carry both practical and legal significance. Practically, the measures suggested above and others that may emerge reduce the likelihood of breach or unnecessary disclosure. In addition, these mechanisms may strengthen the legal positions of both consumers and providers by making it clear that the consumer, and not the provider, is the party with access to and control over any location information and that the consumer has a reasonable expectation of privacy in this information. The more "locks" a provider puts in the consumer's control, the less likely it is that third parties will be asking providers for the keys.[89]

LBS PROVIDERS SHOULD PUSH FOR UPDATED PRIVACY LAW

Finally, LBS providers should actively engage with policymakers and push for updates to ECPA and other legal reforms that clarify and strengthen the legal protections for consumers. Outdated privacy laws can be very costly to companies. LBS may find themselves paying legal fees to maneuver through confusing laws, facing expensive class action lawsuits and fines if they err in their activities, and seeing customers and business partners disappear in a firestorm of bad press when they act "legally" but in a manner contrary to the expectation of users.[90] It is good both for the public and for business to have strong and clearly defined protections for the information that LBS collect, use, and retain.

CONSUMER ACTION: DEMAND YOUR DOTRIGHTS!

If privacy laws and practices are to be brought into the modern era, consumers also must play a critical role in providing the political and commercial will to make it happen. As a united force, Internet and mobile consumers have the political power to force policymakers to update privacy laws and regulations and the financial power to force companies to build privacy protections into product design and business models. Consumers are currently paying a very high price for many online and mobile services: control of their personal information. It is time to demand our dotRights and ensure that protections for privacy are part of the foundation of location-based services, not an afterthought.

CONCLUSION

Location-based services offer many advantages to consumers. But outdated privacy laws and inadequate privacy policies mean that consumers will not be able to trust that their sensitive location information will remain private. The time is now for policymakers, businesses, and consumers to work together to ensure that consumers can use location-based services and still maintain control of their sensitive personal information.

ENDNOTES

1 "Location-based services," as defined for this paper, is not meant to encompass location-based advertising, the practice of delivering advertisements to a mobile or Internet user based on the location of the user. However, many of the issues raised in this paper may also apply to location-based advertising services.

2 Google AdWords, for example, may target advertisements based on physical location as determined by Internet Protocol (IP) address. How Does AdWords Know Where to Show My Keyword-Targeted Ads?, http://adwords.google.com/support/aw/bin/answer.py?hl=en&answer=6401 (last visited Aug. 6, 2010).

3 *See*, *e.g.*, Montclair State University App Registration Alerts, Guardian, Mobile Blackboard & Transit, http://oit.montclair.edu/documentationpdf/YourMSUAppInstructionManual.pdf (last visited Aug. 6, 2010).

4 *See*, *e.g.*, Welcome to the MIT STEP's Handheld Augmented Reality Simulations Site, http://education.mit.edu/drupal/ar (last visited Aug. 6, 2010).

5 *See*, *e.g.*, Tie Your Money, http://www.tieyourmoney.com/ (last visited Aug. 6, 2010).

6 *See*, *e.g.*, meetMoi, http://www.meetmoi.com/welcome (last visited Aug. 6, 2010) ("We update your location in real-time and send alerts to your phone when singles are near you."). *See also* J.G. Mason, *Geo-location Meets the Dating Game: Urban Signals Smartphone App,* GADGETELL, Jan. 25, 2010, http://www.gadgetell.com/tech/comment/geo-location-meets-the-dating-game-urban-signals-smartphone-app/.

7 *See* M.G. Siegler, *Check-In on Foursquare Without Taking Your Phone Out of Your Pocket*, TECHCRUNCH, Aug. 2, 2010, http://techcrunch.com/2010/08/02/future-checkin/, *and* Dean Takahashi, *Booyah Builds a New Location App for Facebook Places in Three Weeks (Video)*, GAMESBEAT, Aug. 18, 2010, http://games.venturebeat.com/2010/08/18/booyah-builds-a-new-location-app-for-facebook-places-in-three-weeks-video/.

8 In many cases, this additional information comes from the consumer or her device directly, but some LBS also acquire information from third parties to supplement their own firsthand information. *See, e.g.*, Yelp Privacy Policy Statement, http://www.yelp.com/static?p=privacy (effective Apr. 21, 2010) (stating that, with user permission, some third-party sites "may also provide us with information from your accounts there to enhance and personalize your use of this Site. For example, you can allow Facebook to tell us who your Facebook friends are so you can follow their activity on Yelp.").

9 For example, the social networking LBS Loopt collects "profile information" which may include "event times and locations, interests and hobbies, age, gender, sexual orientation, relationship status, and favorite places for breakfast, drinks, dancing, outdoor activities," and other information. Loopt Privacy Notice, https://app.loopt.com/loopt/privacyNotice.aspx (last visited Aug. 6, 2010). Likewise, Tweetsii creates user profiles that may include "personal interests and search criteria, gender, education, occupation, and physical location coordinates." Tweetsii Privacy Policy, http://www.tweetsii.com/info/privacy.html (effective Mar. 1, 2010).

10 Live Blog: Facebook Location Announcement (Statement of Chris Cox, Vice President of Product, Facebook), http://www.readwriteweb.com/archives/live_blog_facebook_location_announcement.php.

11 Press Release, comScore Reports February 2010 U.S. Mobile Subscriber Market Share, July 8, 2010, http://www.comscore.com/Press_Events/Press_Releases/2010/7/comScore_Reports_May_2010_U.S._Mobile_Subscriber_Market_Share ("49.1 million people in the U.S. owned smartphones during the three months ending in May").

12 PEW INTERNET & AMERICAN LIFE PROJECT, Mobile Access 2010, July 2010, *available at* http://pewinternet.org/Reports/2010/Mobile-Access-2010.aspx. In comparison, only 80 percent of White non-Hispanic adults own a cell phone, and only 33 percent of these owners have accessed the Internet through their phone.

13 Skyhook Wireless, *Location Aware App Report,* Feb. 2010, http://www.locationrevolution.com/stats/skyhookfebreport.pdf.

14 Mobile Marketing Ass'n, *U.S. Consumers Significantly More Likely to Respond to Location-Based Mobile Ads than Other Mobile Ad Types,* Apr. 21, 2010, http://mmaglobal.com/news/us-consumers-significantly-more-likely-respond-location-based-mobile-ads-other-mobile-ad-types.

15 Leena Rao, *Boom! Foursquare Crosses 2 Million Users*, TechCrunch, July 10, 2010, http://techcrunch.com/2010/07/10/foursquare-crosses-2-million-users/.

16 Michael Arrington, *Yelp Stats Show iPhone App Usage Staggeringly Deeper than Website*, TechCrunch, June 3, 2010, http://techcrunch.com/2010/06/03/yelp-stats-show-iphone-app-usage-staggeringly-deeper-than-website/.

17 This is a two-way communication, i.e., the cell towers are aware when a given device is nearby, and can and do record that information. *See*, e.g., Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year*, Wired, Dec. 1, 2009, http://www.wired.com/threatlevel/2009/12/gps-data/.

18 The satellites themselves do not receive the device's location; instead, the device determines its own location based on satellite signals and can share this with the cell service provider or LBS. *The Collection and Use of Location Information for Commercial Purposes: Hearings Before the Energy and Subcomm. on Communications, Technology and the Internet, and Subcomm. on Commerce, Trade, and Consumer Protection of the H. Commerce Comm*., 106th Congress, Feb. 24, 2010 (testimony of Lorrie Cranor), *available at* http://energycommerce.house.gov/Press_111/20100224/Cranor.Testimony.2010.02.24.pdf.

19 A number of companies maintain these databases, including Google, whose Street View trucks have reportedly been scanning network names as they map and photograph city streets across the world. *See id.*; Andrew Orlowski, *Google Street View Logs WiFi Networks, Mac Addresses*, The Register, Apr. 22, 2010, http://www.theregister.co.uk/2010/04/22/google_streetview_logs_wlans/.

20 *See* ACLU v. Gonzales, 478 F. Supp. 2d 775, 807 (E.D. Pa. 2007) (reviewing testimony from a Quova executive regarding the effectiveness of its technology); Quova, Press Release, Quova's Geolocation Data Helps Continental Airlines Improve Web Banner CTR (Mar. 24, 2009) ("Quova provides IP address location data down to a metro area (25 to 50 miles).").

21 For example, foursquare users manually "check-in" to locations using the service rather than provide their location using an automated method. foursquare, http://foursquare.com. Facebook allows users to manually check in as well, but corroborates their information with location information derived by other means. Places, http://www.facebook.com/places/.

22 As the D.C. Circuit Court stated in a recent opinion, "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble... . A person who know all of another's travels can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." United States v. Maynard, No. 08-3080, 2010 U.S. App. LEXIS 16417, at *39-40 (D.C. Cir. Aug. 6, 2010).

23 *See*, *e.g.*, Nicholas Deleon, *Discontent Grows With Facebook Places' Ability To Tag Without Users' Express Permission*, TechCrunch, Aug. 23, 2010, http://www.crunchgear.com/2010/08/23/discontent-grows-with-facebook-places-ability-to-tag-without-users-express-permission/.

24 *See* twittown, *Another Robbery Linked to Facebook*, Mar. 26, 2010, http://twittown.com/social-networks/facebook/facebook-blog/another-robbery-linked-facebook.

25 More than one in four stalking victims interviewed in a recent study reported some form of cyberstalking was used. Of these, GPS technology was involved in 10 percent of the electronic monitoring of stalking victims. U.S. Dep't. of Justice Special Report, *Stalking Victimization in the United States* at 5 (Jan. 13, 2009), *available at* http://www.ovw.usdoj.gov/docs/stalking-victimization.pdf.

26 No. 08-3080, 2010 U.S. App. LEXIS 16417, at *40 (D.C. Cir. Aug. 6, 2010).

27 Many LBS that allow users to check-in retain histories of these locations indefinitely. In addition, even if the user manually deletes a previous check-in, it is not clear whether all associated records of her location are also deleted. *See* Location-Based Services: A Privacy Comparison, http://dotrights.org/lbs-privacy-comparison.

28 For example, Facebook Places allows a user's friends to check her in to a Place. Facebook Places, http://www.facebook.com/places/.

29 *See* Location-Based Services: A Privacy Comparison, supra note 27.

30 *See* notes 6–8 and accompanying text.

31 *See, e.g.*, Kevin C. Tofel, *Track Money Habits by Location With TIE Your Money on Android*, JkOnTheRun, Aug. 31, 2009, http://jkontherun.com/2009/08/31/track-money-habits-by-location-with-tie-your-money-on-android/.

32 Gerald Friedland and Robin Sommer, *Cybercasing the Joint: On the Privacy Implications of Geo-Tagging,* International Computer Science Institute, at 3 (Aug. 2010), *available at* http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf. The study estimated that 4.3 percent of photos uploaded to Flickr and 3 percent of videos uploaded to YouTube included geotagging, and that 1.3 percent of ads posted to the San Francisco Bay Area "For Sale" section of Craigslist linked to at least one geotagged photo. Note that photos uploaded directly to Craigslist have all geotags removed, but photos that are uploaded to another site and linked to a Craigslist post may not. Similarly, Twitter itself did not allow photos at the time of the study, but a second service called TwitPics allowed Twitter users to post links to photos with geotags intact.

33 Explore Everyone's Photos on a Map, Flickr, http://www.flickr.com/map/ (last visited Aug. 13, 2010).

34 *See YouTube Videos in Google Maps*, Google Lat Long Blog, Apr. 14, 2008, http://google-latlong.blogspot.com/2008/04/youtube-videos-in-google-maps.html.

35 Kate Murphy, *Web Photos That Reveal Secrets, Like Where You Live,* N.Y. Times, Aug. 12, 2010, at B6, available at http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html.

36 *Id*.

37 Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year*, Wired, Dec. 1, 2009, http://www.wired.com/threatlevel/2009/12/gps-data/.

38 Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET News, Feb. 11, 2010, http://news.cnet.com/8301-13578_3-10451518-38.html.

39 *See* Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, Feb. 19, 2010, available at http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html.

40 *See id*; Comments of Al Gidari, Where I'm Calling From, On the Media (NPR radio broadcast May 8, 2009), available at http://www.onthemedia.org/transcripts/2009/05/08/05.

41 Christian Nolan*, Can Your Cell Phone Put You in a Cell Block?* Conn. Law Tribune, July 7, 2010, available at http://www.law.com/jsp/article.jsp?id=1202463302148; Brief of Amici Curiae in Support of Motion To Suppress, United States v. Soto, Case No. 09-cr-200 (D. Conn. June 18, 2010), *available at* http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf. While the details remain unclear because the government surveillance demands are under seal, it appears that the government engaged in dragnet surveillance, seeking and obtaining location information for a large number of innocent people to identify who was involved in the crime.

42 Press Release, Webroot Survey Finds Geolocation Apps Prevalent Amongst Mobile Device Users, But 55 Percent Concerned About Loss of Privacy, July 13, 2010, http://pr.webroot.com/threat-research/cons/social-networks-mobile-security-071310.html.

43 Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls* 15 (updated February 2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

44 *Id*.

45 The modern legal understanding of privacy evolved in large part from Justice Brandeis's lengthy dissent in *Olmstead v. United States*. 277 U.S. 438 (1928) (Brandeis, J., dissenting). According to Brandeis:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

46 U.S. Const. amend. IV.

47 Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring). There are some exceptions where a warrant is not required for a search or seizure, including searches conducted at the country's border, seizures when contraband is in "plain view," or searches conducted under "exigent circumstances" such as when an officer believes lives are in imminent danger, a criminal suspect is about to escape, or evidence of a crime is about to be destroyed.

48 *Compare* United States v. Karo, 468 U.S. 705, 714-15 (1984) (holding that the warrantless use of a "beeper" to track the location of an object inside a home violates the Fourth Amendment) *with* United States v. Knotts, 460 U.S. 276 (1983) (holding warrantless tracking by means of a beeper in public locations is not a Fourth Amendment violation if it reveals no information that could not be obtained by visual surveillance).

The question of what is "open to visual surveillance" was recently considered by the D.C. Circuit Court, which held that month-long, round-the-clock GPS surveillance by law enforcement violated a suspect's reasonable expectation of privacy because "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil." United States v. Maynard, No. 08-3080, 2010 U.S. App. LEXIS 16417, at *35 (D.C. Cir. Aug. 6, 2010), *available at* http://pacer.cadc.uscourts.gov/common/opinions/201008/08-3030-1259298.pdf.

49 *Compare* Maynard, 2010 U.S. App. LEXIS 16417 (finding month-long surveillance can violate reasonable expectations of privacy even if individual event surveillance would not, because the aggregate surveillance is more intrusive) with United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010) (finding no Fourth Amendment violation in using mobile-tracking devices intermittently over a four-month period because they only revealed information that could be obtained by visual surveillance).

50 *See* United States v. Miller, 425 U.S. 435 (1976) (holding that banking records are not protected by the Fourth Amendment); Smith v. Maryland, 442 U.S. 735 (1979) (finding that records of dialed phone numbers fall outside of Fourth Amendment protection).

51 *See*, e.g., United States v. Barth, 26 F.Supp.2d 929 (W.D. Tex. 1998).

52 *See* United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007); United States v. Simons, 206 F.3d 392 (4th Cir. 2000).

53 *Compare* Warshak v. United States, 490 F.3d 455 (6th Cir. 2007) (Fourth Amendment does apply to email held by a third-party web email provider), vacated on other grounds, 532 F.3d 521 (6th Cir. 2008) (en banc), with Rehberg v. Paulk, 598 F.3d 1268 (11th Cir. 2010) (Fourth Amendment does not apply to email held by a third-party web email provider), vacated, No. 09-11897 (July 16, 2010) (Rehberg II) (holding instead that Fourth Amendment protection for email is not clearly established and actual issue of Fourth Amendment protection need not be reached in context of qualified immunity), *available at* http://www.ca11.uscourts.gov/opinions/ops/200911897reh.pdf. *See generally* Rehberg II, No. 09-11897, at 22–28 (discussing the lack of clarity of Fourth Amendment protection for email stored with a web email provider).

54 "The Justice Department draws a distinction between cell-tower data and GPS information, according to a spokeswoman, and will often get warrants for the latter." Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, Feb. 19, 2010, http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html.

55 *See* In re Application for Pen Register and Trap/Trace Device With Cell Site Location Auth., 396 F. Supp. 2d 747, 756-57 (S.D. Tex. 2005) (stating that CSLI is sent by the phone "entirely independent of the user's input, control, or knowledge"); *see also* In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 534 F. Supp. 2d 585, 615 (W.D. Pa. 2008).

56 For example, Google's privacy policy is clear that it collects location information when you use Google Maps for mobile, but what is less clear is whether Google collects any location information when you use Google Maps on your desktop computer. The company's privacy policy simply states that it collects information about your "web request." Google, Privacy Policy, http://www.google.com/privacypolicy.html. Similarly, foursquare's privacy policy says that it collects "use information" but does not explicitly say it collects location data. foursquare, Privacy Policy, http://foursquare.com/legal/privacy (effective Aug. 17, 2010).

57 *See, e.g.*, People v. Chapman, 679 P.2d 62, 71 (Cal. 1984) (affirming a right to privacy in unlisted telephone directory information even though the information was "shared" with the third-party telephone company); People v. Blair, 602 P.2d 738, 745-48 (Cal. 1979) (finding a reasonable expectation of privacy in hotel phone records and credit-card charge records); Burrows v. Superior Court, 529 P.2d 590, 594-95 (Cal. 1974) (finding a privacy right in bank records).

58 Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2712. The term "ECPA" is used in this paper to describe both Title I of the Electronic Communications Privacy Act, which protects wire, oral, and electronic communications in transit, and Title II, referred to as the Stored Communications Act, which protects communications held in electronic storage.

59 S. Rep. No. 99-541, at 3 (1986). A longer excerpt reads:

> The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third-party computer operator, the information may be subject to no constitutional privacy protection. . . . Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties.

60 *Id*.

61 18 U.S.C. § 2510(15) (2008).

62 *Id*. § 2711(2).

63 A warrant is generally required to access the contents of unopened email for the first 180 days. Only a subpoena may be required after 180 days or after it is opened. *Id*. § 2703.

64 Fed. R. Crim. P. 41(d)(1) (establishing a probable cause standard in order to issue a warrant to install a tracking device).

65 *ECPA Reform and the Revolution in Location-Based Technologies and Services, Hearing Before the Subcomm. On the Constitution, Civil Rights, and Civil Liberties of the H. H. Comm. on the Judiciary,* June 24, 2010 (statement of U.S. Magistrate Judge Stephen W. Smith), at 9-10. These orders could be issued publicly with any law enforcement sensitive information redacted so the public at least would be privy to the legal standards applied by the courts.

66 *Id*.

67 18 U.S.C. § 2519 (2008).

68 47 U.S.C. § 222 (2008).

69 *The Collection and Use of Location Information for Commercial Purposes: Hearings Before the Energy and Subcomm. on Communications, Technology and the Internet, and Subcomm. on Commerce, Trade, and Consumer Protection of the H. Commerce Comm.,* 106th Congress, Feb. 24, 2010 (testimony of John B. Morris, Jr.), *available at* http://energycommerce.house.gov/Press_111/20100224/Morris.Testimony.2010.02.24.pdf.

70 Tsai et al., *supra* note 43, at 8.

71 For example, the privacy policy for the ride-sharing LBS Carticipate is a mere 107 words long and notes that "limited information may be recorded in our logs" without providing any suggestion as to what that information might be or how long those logs are retained. Carticipate, Privacy Policy, http://www.carticipate.com/privacy (last visited Aug. 6, 2010).

72 Tsai et al., *supra* note 43, at 12 (finding that "location-sharing technologies offer limited flexibility in their privacy controls…. [T]here are no commercially available systems that offer anywhere near as powerful a control set as one could imagine").

73 Better Business Bureau, Security and Privacy—Made Simpler (Mar. 2006), http://bbb.org/us/storage/16/documents/SecurityPrivacyMadeSimpler.pdf.

74 Louis D. Brandeis, Other People's Money and How the Bankers Use It 92 (2d ed. 1932) *available at* http://www.law.louisville.edu/library/collections/brandeis/node/191.

75 The Administrative Office of the U.S. Courts must submit an annual Wiretap Report to Congress concerning intercepted communications under the Wiretap Act. 18 U.S.C. § 2519. The Foreign Intelligence Surveillance Act requires the Attorney General to submit a semi-annual report on electronic surveillance conducted under that statute. 50 U.S.C. § 1808. And the Attorney General reports to Congress on the number of pen register and trap-and-trace orders. 18 U.S.C. § 3126. (Pen registers record outgoing digits one dials when using a telephone, but not spoken conversation, while a trap-and-trace device records incoming data. Originally the Pen Register Act allowed the government access only to numbers dialed on a telephone line, but the USA-PATRIOT Act expanded the definition. 18 U.S.C. § 3121(c).) There is no similar requirement to report on the invasive practices of obtaining electronic information via search warrant, subpoena, and other means.

76 Many companies will not say how many demands for information are received, and those that do often do so inadvertently. When a Sprint manager discussed the automated portal for law enforcement and 8 million requests for information (see *supra* note 18 and accompanying text), he did so at a closed conference and his remarks were only made widely public by an attendee. After the conference a Sprint spokesperson insisted that the number of individual customers affected was much smaller than 8 million, but refused to disclose exactly how many customers' data was shared. Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year*, Wired, Dec. 1, 2009, http://www.wired.com/threatlevel/2009/12/gps-data/.

77 *See generally* ACLU of Northern California, *Privacy Practices* in Privacy and Free Speech: It's Good for Business, *available at* http://dotrights.org/business/primer/. See also Yvonne Jones, *Rants and Raves*, Wired, Sept. 2009, at 20, available at http://www.wired.com/culture/culturereviews/magazine/17-09/rants ("Facebook's changes to its privacy settings killed my affection for the company … it's revoking one of the things I valued most about it and in the process ensuring that I trust it less.").

78 *See* Privacy and Free Speech: It's Good for Business, *supra* note 77.

79 Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Aug. 6, 2010).

80 *See generally* Privacy and Free Speech: It's Good for Business, *supra* note 77.

81 *See id.*

82 WHERE Privacy Policy, http://www.where.com/privacy-policy/ (last visited Aug. 6, 2010).

83 Mologogo Terms of Service, http://www.mologogo.com/terms.jsp (last visited Aug. 6, 2010).

84 Loopt Privacy Notice, https://app.loopt.com/loopt/privacyNotice.aspx (last visited Aug. 6, 2010).

85 This can be particularly difficult in the context of location information, since simply linking specific locations with a specific user may be enough to identify that user. *See* Mike Elgan, *Location-Tracking Software: Will the Revolution Be Killed by Fear?* Datamation, July 21, 2010, http://itmanagement.earthweb.com/mowi/article.php/3894291/Location-Tracking-Software-Will-the-Revolution-be-Killed-by-Fear.htm. *See also, e.g.*, AOL, *in* Privacy and Free Speech: It's Good for Business, *supra* note 77, at http://dotrights.org/business/primer/node/37 (describing a 2006 incident in which AOL made public "anonymized" search results which were not, in fact, properly anonymized, accidentally releasing identifiable search records of hundreds of thousands of consumers), *and* Arvin Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *available at* http://userweb.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (describing how the researchers "de-anonymized" Netflix-consumer movie reviews that had been released by Netflix).

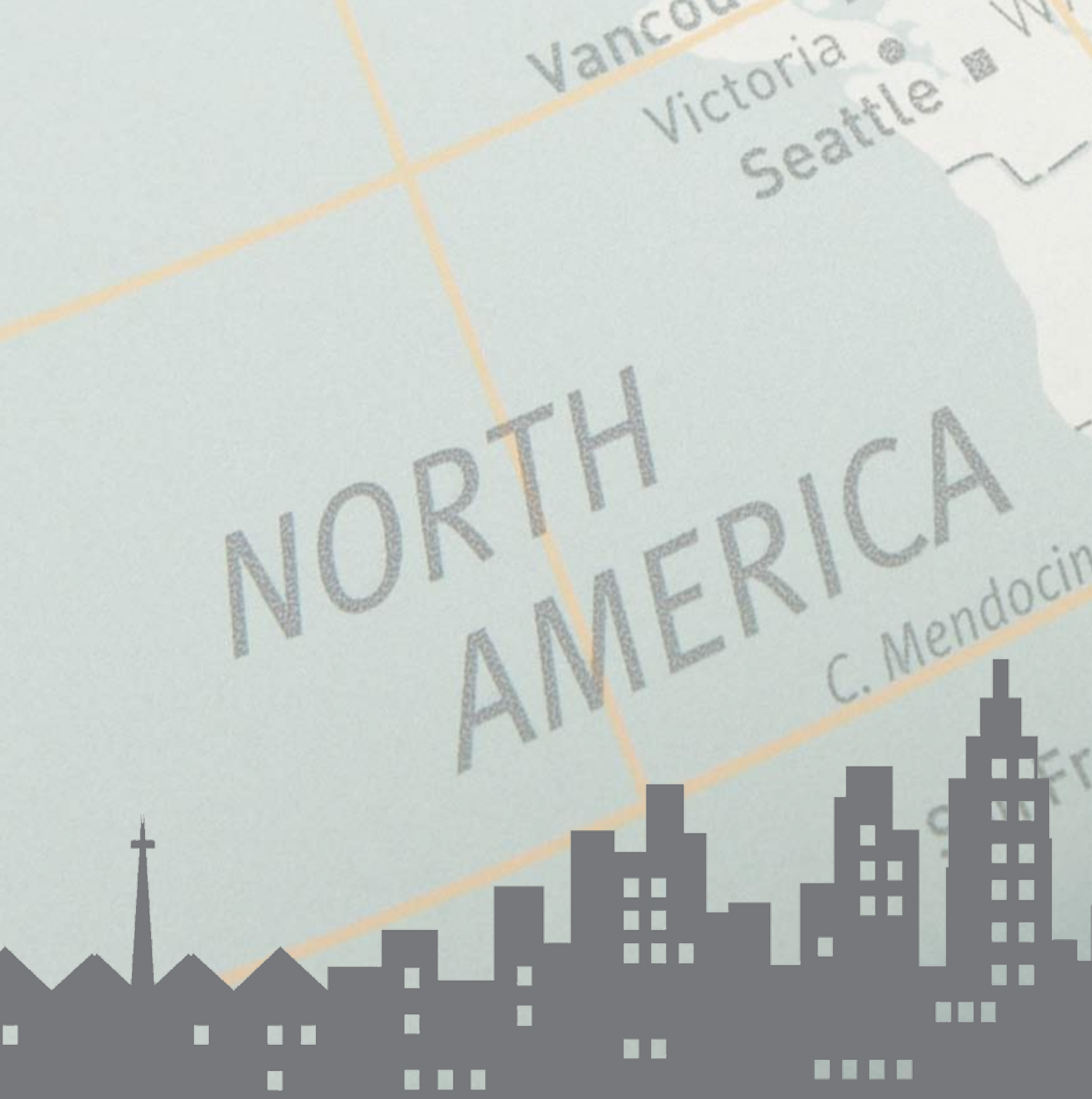
86 Google Latitude: Privacy, https://sites.google.com/a/pressatgoogle.com/latitude/privacy (last visited July 28, 2010).

87 Locaccino, http://www.locaccino.org/ (last visited Aug. 6, 2010).

88 Fire Eagle, http://fireeagle.yahoo.net/ (last visited Aug. 6, 2010).

89 *See* Peter Wayner, *You Know About Backups. Now, Do It Online,* N.Y. Times, Oct. 22, 2008, *available at* http://www.nytimes.com/2008/10/23/technology/personaltech/23basics1.html ("Intronis, for instance, has never received a subpoena for stored data and couldn't provide the information even if it did. 'We don't consider ourselves as having access to customer's data. It's not even a thought,' said Mr. Webster.").

90 *See generally* Privacy and Free Speech: It's Good for Business, *supra* note 77.



DEMAND YOUR dotRIGHTS

ACLU
AMERICAN CIVIL LIBERTIES UNION of NORTHERN CALIFORNIA

A Publication of the ACLU of Northern California

November 2010

www.dotrights.org
www.aclunc.org/tech