Research Report: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information

By Jennifer King and Chris Jay Hoofnagle[1]

April 18, 2008

Abstract

While law enforcement increasingly locates individuals by gaining access to wireless phone records, a supermajority of Californians supports judicial intervention and informing suspects before law enforcement acquires retrospective (historical) location data on individuals from wireless phone companies. A majority of Californians understands that wireless phones can track their location, and that there is broad support for location tracking in emergency situations. When compared with Professor Alan Westin's three privacy segments, "Fundamentalists," "Pragmatists," and the "Unconcerned," Californians are more likely to be privacy pragmatists or fundamentalists, and less likely to be unconcerned about privacy. Generally, Westin's segmentation was not predictive of Californians' attitudes towards law enforcement access to wireless location data.

[1] Respectively, Research Specialist and Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law.

We thank Kevin Bankston, Robert Morgester, and Orin Kerr for their assistance.

The Samuelson Law, Technology & Public Policy Clinic at UC Berkeley Law provides an opportunity for law students and graduate students to represent clients and conduct interdisciplinary research. Since January 2001, students participating in the Clinic have worked with leading lawyers in nonprofit organizations, government, private practice, and academia to represent clients on a broad range of legal matters including free speech, privacy copyright, and open source. http://www.samuelsonclinic.org/

Introduction

Location-aware communication devices and services provide individuals with new tools that make life more convenient. But this convenience comes with a price—these devices can enable individuals to be tracked at an unprecedented scale, both retrospectively and in real-time. The most ubiquitous device enabling this tracking is the wireless phone; the Wireless Association, an industry trade group, estimates that there are nearly 244 million wireless subscribers in the US as of 2007.[2] Wireless phones have more accurate tracking capabilities, in part because the Federal Communications Commission required that carriers be able to locate subscribers when they dial 911. This infrastructure enhanced by the "e911" mandate makes it possible to monitor location information for other purposes and store it so that it can be accessed later.

In addition to the implicit tracking provided by wireless phones, consumers are increasingly using devices that explicitly provide location-aware services. General Motor's OnStar[3] and ATX Group's[4] vehicle telematic systems provide location and safety information for drivers, and can be used to remotely track a vehicle, since telematic systems communicate location data back to the service provider.[5] On the other hand, many GPS devices do not communicate back to a central server or service, and thus allow individuals to enjoy the benefits of the technology without being tracked. For example, many handheld and aftermarket GPS devices for cars only receive information from location satellites, and thus do not provide an opportunity for remote tracking.

In other cases, individuals are actively providing location information that can later be accessed by law enforcement. Internet-based location services, such as Dodgeball,[6] and mobile applications such as Loopt,[7] and BuddyBeacon,[8] allow users to update these services by mobile phone with their location and share it with friends. Some mobile service providers offer GPS-based location services that will identify the

---

[2] CTIA, SEMI-ANNUAL WIRELESS INDUSTRY SURVEY (2007), available at: http://www.ctia.org/advocacy/research/index.cfm/AID/10316
[3] GM OnStar, available at: http://www.onstar.com/
[4] ATX Group, available at: http://www.atxg.com/
[5] Some of these systems can also enable remote "bugging" of a vehicle. *See Company v. United States (In re United States)*, 349 F.3d 1132 (9th Cir. 2003).
[6] Dodgeball, available at: http://www.dodgeball.com/
[7] Loopt, available at: https://www.loopt.com/loopt/sess/index.aspx
[8] BuddyBeacon, available at: http://www.helio.com/#services_gps

subscriber's location and provide maps and other local information, such as directions. Finally some services, like Yahoo's Zone Tags,[9] can infer location from a mobile phone and add location data to photos uploaded to Yahoo's photo sharing website, Flickr.com.

The location data generated by these devices is of growing interest to law enforcement. While location data can enable the rescue of kidnapped or missing people in emergency situations, it also can be used to pervasively track individuals in non-emergency situations, as well as provide a historical account of one's travels. The Washington *Post* reported in November 2007 that federal officials were "routinely asking courts to order cell phone companies to furnish real-time tracking data so they can pinpoint the whereabouts of drug traffickers, fugitives and other criminal suspects," often without demonstrating probable cause.[10] The availability of location data, and the ease with which law enforcement is able to obtain this data, raises concerns about the balance of power between the individual and government. In particular, obtaining location data from service providers gives law enforcement far more surveillance capability, both in breadth and depth, than agencies would have if conducting comparable surveillance themselves.

In order to understand both Californians' perception and attitudes towards these issues, we asked four questions of a representative sample of California residents. One question (Question 1) attempted to determine whether the public understood that wireless phones give law enforcement the ability to track individuals; one question (Question 2) assessed level of agreement regarding the intent of the e911 mandate, which required wireless carriers to build the infrastructure necessary for location information to be provided to police in emergency situations; one question (Question 3), asked of approximately half of the respondents, assessed whether Californians favored requiring notification to individuals when law enforcement requests historical location records; and one question (Question 4) asked of the other half of the respondents, assessed whether Californians favored requiring law enforcement to convince a judge that a crime has occurred before obtaining historical location records from a service provider. Results are

[9] Yahoo Zone Tags, available at: http://zonetag.research.yahoo.com/
[10] Ellen Nakashima, *Cellphone Tracking Powers on Request*, Washington Post, Nov. 23, 2007, available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444_pf.html.

discussed below in this paper; the questions and results are reproduced in the Appendixes.

The Technology

The e911 mandate, passed in 1998, required that all cell phones be able to provide their physical location in order for emergency responders to accurately locate users in distress. To accomplish this, mobile providers triangulate a phone's position based upon the location of the communication towers with which the phone is communicating. Because phones require interaction with a network to send and receive data, location information is available whenever the phone is powered on (not just when calls are in progress). If a phone includes a GPS transmitter, then GPS can be used to determine location in conjunction with tower triangulation. The effectiveness and accuracy of each method varies, depending upon the number of nearby cell towers, or physical impediments, like mountains, trees, or tall buildings, that can block GPS reception.

The e911 system has offered successes in aiding both emergency responders and law enforcement. At the same time, the system is far from accurate,[11] and in September 2007 the FCC released new benchmarks for carriers requiring compliance by 2012.[12]

The Law of Access to Phone Location Data

The federal government has taken an aggressive stance on law enforcement access to wireless location data.[13] Although the US Department of Justice's legal rationale for accessing records has shifted over time, it generally has argued that both retrospective (past, historical records) and prospective location information can be obtained on a "relevance" standard, relying upon 18 USC § 2703(d). Under that standard, the "governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe … the records or other information sought, are relevant and material to an ongoing criminal investigation" before a magistrate judge to obtain the order. This falls short of a warrant standard, which would require law enforcement to

[11] Lesley Cauley, *Growing wireless use highlights limitations of 911*, USA Today, Apr. 22, 2007, available at http://www.usatoday.com/tech/wireless/2007-04-22-e911-systems_N.htm
[12] Brad Reed, *FCC Details E911 Accuracy Requirements*, PC World, Sept. 13, 2007, available at http://www.pcworld.com/article/id,137169-c,cellphones/article.html
[13] See generally, Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. Rev ___ (forthcoming 2007) (describing and analyzing recent cases where federal law enforcement have sought location information).

show that there is probable cause to believe that a crime has been committed or is about to be committed, and that the phone data sought would related to the alleged crime. No notice to the subscriber is required, and under 18 USC § 2705, the government can obtain an order preventing the carrier from notifying the subscriber of the request upon showing serious adverse results from giving notice, such as jeopardizing an investigation.

California law enforcement treats prospective and retrospective location data differently. It uses the federal "relevance" standard for access to retrospective data. But prospective data requires a higher, warrant standard. California applies this standard, because the State's Attorney General treats wireless phones as "tracking devices."[14]

Table 1: Wireless Phone Location Data: Law Enforcement Access Standards

	Prospective or Current Location	Retrospective (historical) Location
Federal Law Enforcement	"Relevance" standard under 18 USC § 2703 (d). No notice to subscriber.	
California Law Enforcement	Requires search warrant because cellphone is a wireless tracking device.	Same as federal.

Technology Choice and Privacy

Individuals' choice of products also has a profound effect on privacy. Wireless phones that rely upon GPS for location information can collect more precise data on individuals, while non-GPS phones that rely upon the triangulation of network towers provide a more general indication of location.

The law also creates incoherent divides between technologies. For instance, California law[15] provides strong protections against law enforcement access to automobile "black boxes," devices that monitor driving habits, and in some cases, the location of the vehicle.[16] Most cars now come equipped with these black boxes, known as "event data recorders," and they can be used in accident reconstruction and law enforcement investigations. As these devices become more sophisticated and incorporate more features and increased storage capacity, law enforcement will seek access to them in order to determine a vehicle's past location.

---

[14] Email from Robert M. Morgester, Deputy Attorney General, Special Crimes Unit, State of California, Feb. 1, 2008 (on file with authors).
[15] Cal. Veh. Code § 9951 (2007).
[16] Patrick Mueller, *Every Time You Brake, Every Turn You Make - I'll Be Watching You: Protecting Driver Privacy in Event Data Recorder Information*, 2006 Wis. L. Rev. 135 (2006).

The California statute protecting black boxes is written broadly enough to cover GPS devices in vehicles; however, the protection only applies if the manufacturer installed the device.[17] Under the statute, law enforcement must obtain a court order before accessing the information. But, if the exact same device was installed aftermarket by an electronics store, different, weaker rules apply.

Methods

Our survey questions were asked as part of the 2007 Golden Bear Omnibus Survey, a telephone-based survey of a representative sample of California residents conducted by the Survey Research Center of University of California, Berkeley. The Samuelson Law, Technology & Public Policy Clinic funded the privacy portion of the Golden Bear survey from general operating funds; no outside organization sponsored the survey. The dual frame sample used random digit dialing of both cell phones and residential landline telephones, with one respondent per landline household selected.[18] English and Spanish speakers over the age of 18 were eligible. 1,186 respondents completed the telephone interview, conducted from April 30th to September 2nd, 2007, for a response rate of 15.9%. However, in order to include more questions in the survey than could be administered to all respondents in a reasonable period of time, the sample was divided into six randomized parts or units. All respondents were asked certain basic demographic and background questions, but most questions were administered only to 5/6th of the complete sample. This reduced the number of respondents who answered our questions to 991. Weights were applied to compensate for probabilities of selection and to match certain demographic distributions.[19] This weighting ensures that the results reflect a representative sample of Californians by age, education, ethnicity, and gender, and compensates for differences in probabilities of selection based on use of landline versus mobile phone.

---

[17] A covered device includes any manufacturer-installed equipment that records: "how fast and in which direction the motor vehicle is traveling" or "a history of where the motor vehicle travels." Cal. Veh. Code § 9951 (a)(1)-(2) (2007).

[18] For details on the construction of the sample, please see http://sda.berkeley.edu/src/GBO/2007/Doc/hcbka01.htm

[19] For a detailed overview of sampling methods, please see: http://sda.berkeley.edu/src/GBO/2007/Doc/hcbka02.htm

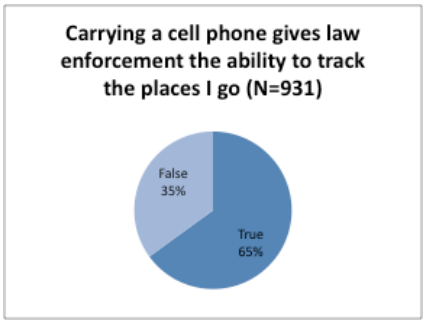
Responses to four questions provided the basis of analysis for this paper; two questions were asked of all respondents, and two were randomly administered to 48.8% (Question 3) and 51.2% (Question 4) of the respondent pool. All questions and the results are reproduced the Appendixes.

Our Research Standards

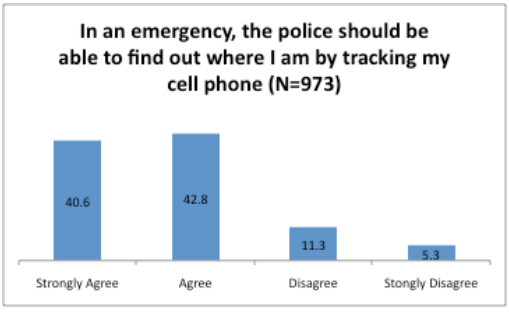
We hold ourselves to high standards in conducting public polls. We encourage the reader to compare our methods to the best practices articulated in *20 Questions A Journalist Should Ask About Poll Results*, published by the National Council on Public Polls.[20] Furthermore, we go beyond these standards by, first, guaranteeing that we publish all the questions asked and responses received; and second, sharing our results so that others can inspect them (*see* Appendixes). The Survey Research Office will post the raw data file associated with the Golden Bear Omnibus Survey online later this year.

Results and Discussion

When we asked Californians to answer true or false to the following true statement: "Carrying a cell phone gives law enforcement the ability to track the places I go," 65% of respondents answered true, while 35% of respondents answered false. This shows that while a majority of respondents are aware that law enforcement can track their location by cell phone, a sizeable minority are not aware that this is possible.

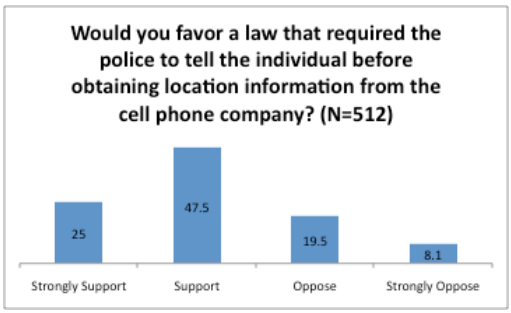


A substantial majority, 83% of respondents, agreed or strongly agreed with Question 2: "In an emergency, the police should be able to find out where I am by tracking my cell phone." This shows support for the principle behind the e911 mandate, when used in emergency situations. Only 17% disagreed or strongly disagreed with this question.



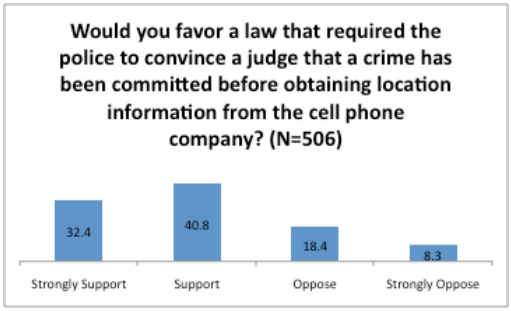
[20] Available at http://www.ncpp.org/?q=node/4

For the next set of questions, we attempted to understand what limits Californians thought were appropriate for access to historical location data. We provided the following background information: "Now, I would like to ask you about possible rules and procedures to protect data that reveals the location of others. Suppose that the police wanted to determine where an individual was one week ago." Question 3 then asked: "Would you favor a law that required the police to tell the individual before obtaining location information from the cell phone company?" 72% of respondents supported or strongly supported requiring that notice be given to the individual being investigated, while 28% of respondents opposed or strongly opposed.



Notice is a commonly-accepted privacy protection, and requiring notice of access to location data allows the suspect to appear in court and challenge the government's rationale for obtaining the information. Thus, the question assumes that notice will cause some interference with law enforcement activity. Recall that under 18 USC § 2705, if serious adverse consequences will result from notice, the government can obtain an order directing the carrier not to give notice to the suspect.

For the next question, Question 4, we attempted to assess whether Californians would support strong judicial intervention before law enforcement accessed historical location data.[21] We asked with respect to historical location data: "Would you favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company?" The results were nearly identical to



[21] An earlier version of this report concluded that the answer to this question showed that Californians supported a probable-cause warrant standard for access to location information. After consulting with Professor Orin Kerr, we decided that the question was not specific enough to come to that determination, because it relied upon respondents to make a logical leap that the crime committed was connected to the location data sought by law enforcement. We nevertheless believe this question shows that Californians support strong judicial intervention in advance of law enforcement access to historical location data.

Question 3, with 73% of respondents supporting or strongly supporting this requirement, while 27% opposed or strongly opposed it.

These results show that Californians support judicial intervention and due process before historical location data are acquired by law enforcement. Californians also appreciate the difference between emergency and non-emergency contexts, and are accepting of real-time tracking by law enforcement in emergency situations.

The Westin Taxonomy Applied to Location Tracking

Professor Alan Westin has pioneered a popular "segmentation" of privacy attitudes among the American public.[22] In it, Americans are divided into three groups: "Privacy Fundamentalists," who place a high value on privacy and favor passage of strong privacy laws;[23] "Privacy Pragmatists," who see the relative benefits of information collection and favor voluntary standards for privacy protection;[24] and the "Privacy Unconcerned," those who have low privacy concern and have little objection to giving government or businesses personal information.[25]

We were interested to see how our sample of California residents fit into the Westin segmentation. We included the three questions (Appendix 2) Westin has used to divide respondents into these categories in our survey instrument.

---

[22] Ponnurangam Kumaraguru & Lorrie Faith Cranor, Privacy Indexes: A Survey of Westin's Studies, Dec. 2005, available at http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf.

[23] "Privacy Fundamentalists (about 25%). This group sees privacy as an especially high value, rejects the claims of many organizations to need or be entitled to get personal information for their business or governmental programs, thinks more individuals should simply refuse to give out information they are asked for, and favors enactment of strong federal and state laws to secure privacy rights and control organizational discretion." Opinion Surveys: What Consumers Have To Say About Information Privacy, before the House Commerce Subcommittee on Commerce, Trade, and Consumer Protection, May 8, 2001 (testimony of Alan K. Westin, Professor Emeritus, Columbia University), available at http://energycommerce.house.gov/reparchives/107/hearings/05082001Hearing209/Westin309.htm

[24] "Privacy Pragmatists (about 55%). This group weighs the value to them and society of various business or government programs calling for personal information, examines the relevance and social propriety of the information sought, looks to see whether fair information practices are being widely enough observed, and then decides whether they will agree or disagree with specific information activities -- with their trust in the particular industry or company involved a critical decisional factor. The Pragmatists favor voluntary standards over legislation and government enforcement, but they will back legislation when they think not enough is being done -- or meaningfully done -- by voluntary means." *Id*.

[25] "Privacy Unconcerned (about 20%) This group doesn't know what the "privacy fuss" is all about, supports the benefits of most organizational programs over warnings about privacy abuse, has little problem with supplying their personal information to government authorities or businesses, and sees no need for creating another government bureaucracy to protect someone's privacy." *Id*.

Westin's own figures for these three segments for the U.S. population are as follows:

Table 2: Westin's Figures for Privacy Segments in U.S., 1995 – 2001

Year of Study	Privacy Fundamentalists	Privacy Pragmatists	Privacy Unconcerned
1995-1999[26]	25%	55%	20%
2001[27]	25%	63%	12%

Segmentation of our population is shown in Table 3:

Table 3: Westin Segments Applied to This Survey of Californians

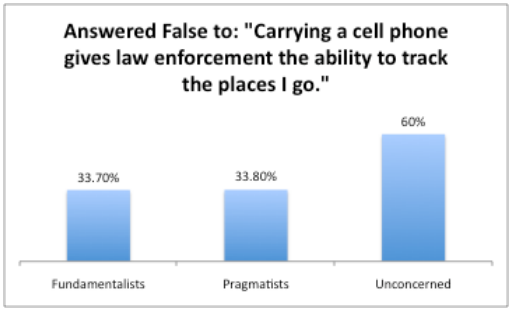
	Privacy Fundamentalists	Privacy Pragmatists	Privacy Unconcerned	Unclassified[28]	Total
Count	208	665	30	88	991
Percent of all respondents	21%	67%	3%	9%	100%
Percentage of those who could be classified	23%	74%	3%	N/A	100%

Westin notes that since he began conducting consumer privacy surveys, he has recognized "moving concerns from a modest matter for a minority of consumers in the 1980s to an issue of high intensity expressed by more than three-fourth of American consumers in 2001."[29] The changes in Pragmatists and the Unconcerned between 1999 to 2001 (the year for which most recent data is available), according to Westin, further reflects the rising popularity of the internet (and its attendant privacy risks), as well as heightened awareness of identity theft. In comparing our California-specific population to Westin's general population numbers, it is clear that Californians have even stronger privacy concerns; while Fundamentalists are slightly lower than Westin's 2001 numbers (23% in CA compared to 25% nationally), Pragmatists are over 10 points higher (74% in CA compared to 63% nationally), and the Unconcerned nine points lower (3% in CA

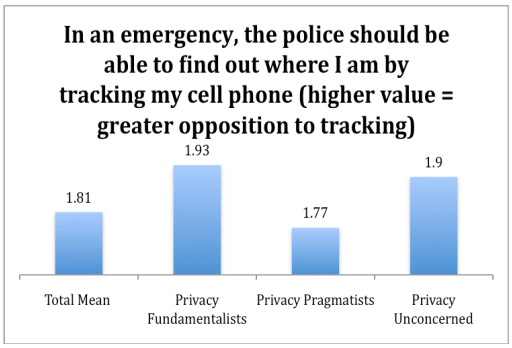
[26] Note: figures are approximate. Equifax-Harris Mid Decade Consumer Privacy Survey (1995), Equifax-Harris Consumer Privacy Survey (1996), IBM-Harris Multi-National Consumer Privacy Study (1999).
[27] *Supra* note 22.
[28] In order to be included in a segment, a respondent had to provide a valid answer to all three questions. Respondents who provided one or more invalid answers are unclassified.
[29] *Supra* note 22.

compared to 12% nationally). Considering the change in Westin's numbers in only two years, it is probable that a national survey conducted in 2008 would produce numbers more in line with our California findings.

In order to explore whether segmentation by privacy affiliation could be associated with specific privacy attitudes in our questions, we compared responses to Questions 1 through 4 between these three subcategories of respondents using different statistical methods. For Question 1 (Carrying a cell phone gives law enforcement the ability to track the places I go), a True/False question, we created a cross-tabulation of the values and calculated the chi-squared statistic in order to determine whether there was a statistically significant difference between expected and actual frequencies for each group's answers to this question. We found that the chi-squared value for the three categories was statistically significant;[30] however, responses for fundamentalists and pragmatists were nearly identical (66.3% of fundamentalists correctly answered "True," as did 66.2% of pragmatists), while the privacy unconcerned response differed dramatically (40% answered "True"). Accordingly, the privacy unconcerned are much more likely to be unaware of law enforcement's ability to track location by wireless phone than the other groups.

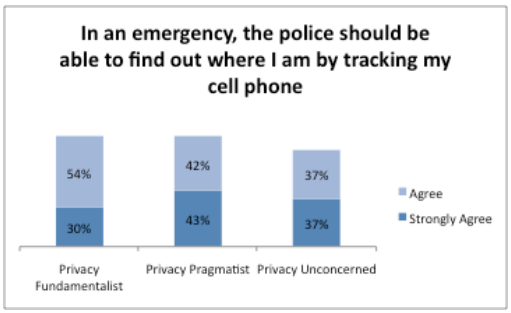


For Questions 2 through 4, which use a Likert scale ranging from one to four to gauge responses (see individual questions below for exact scale values), we compared the responses for each group using ANOVA, measuring the differences in means between each groups' responses. A statistically significant difference between groups allows us to infer that

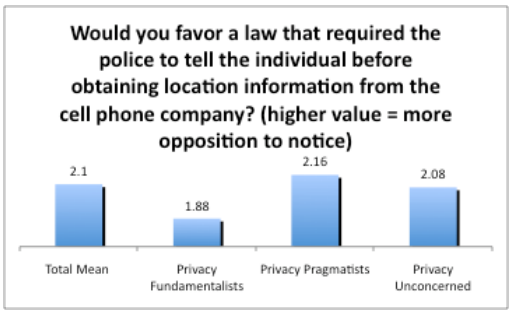


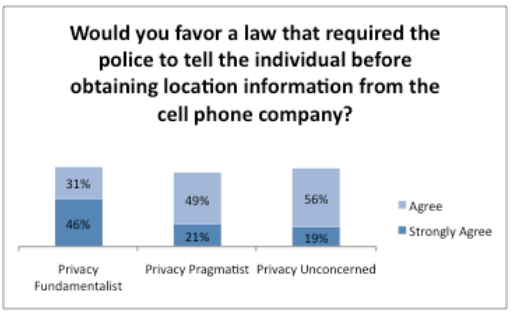
[30] x^2 =8.818, df = 2, p=.012

each group has significantly varying opinions about each question, and in fact statistically significant differences were found between groups across all three questions.[31] However, the attitudes professed among our fundamentalists, pragmatists, and the unconcerned did not align with Westin's descriptions of their attitudes. For instance, in Question 2, we found that the privacy unconcerned were more likely to oppose tracking in an emergency situation than pragmatists, and thus were more supportive of privacy in this context. This does not comport with Westin description of this group, which, "has little problem with supplying their personal information to government authorities or businesses…"[32]



Question 3 assessed whether respondents supported a common privacy protection—whether notice should be provided to an individual before their information is accessed. In this case, the privacy unconcerned expressed stronger support for the protection than pragmatists.

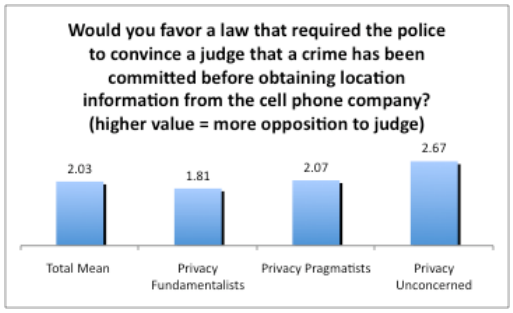


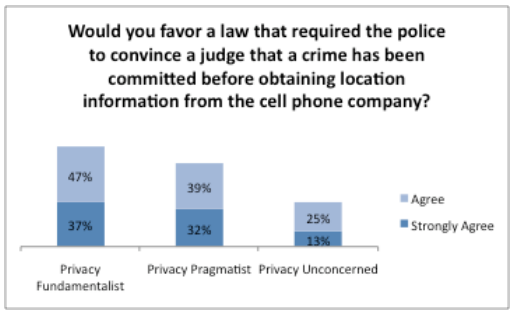


[31] Question 1: F=4.902, df=3, *p*=.002; Question 2: F=9.244, df=3, *p*=.000; Question 3: F=5.274, df=3, *p*=.001

[32] *Supra* note 22.

Finally, when we asked whether respondents favored obtaining permission from a judge before securing location data, responses to this question followed Westin's paradigm, with fundamentalists offering the strongest support for this measure and the unconcerned offering the weakest.





We hypothesize that this incongruity between Westin's segmentation and attitudes documented in this study could be indicative that these categories and their predictive power may be weakening over time, evinced in particular by the low number of unconcerned respondents in our population. As Westin himself notes, privacy issues have jumped to the forefront of American consciousness, in turn may have reduced the number of people who are unaware of or unconcerned with privacy issues.[33] Additionally, California is known for aggressive privacy protection, as evidenced by the creation of a state privacy office and scores of sectoral regulations,[34] and thus, our sample of California-only residents may skew towards more privacy sensitivity than a national sample. The incongruity could also be attributable to the subject matter—Westin has indicated that in certain contexts, for instance, medical privacy, individuals are more likely to identify themselves as privacy fundamentalists.[35] Similarly, location tracking may be triggering a more privacy sensitive response.

This study is the first of many conducted by UC Berkeley's Samuelson Clinic using 2007 Golden Bear survey data; in future studies, we will continue to engage in analysis of the Westin segmentation. These future studies should elucidate issues surrounding the segmentation, their predictive value, and whether they represent the nuanced, context-dependent attitudes that individuals hold on privacy.

---

[33] *Id*.
[34] CALIFORNIA SENATE OFFICE OF RESEARCH, CONSUMER PRIVACY AND IDENTITY THEFT: A SUMMARY OF KEY STATUTES AND GUIDE FOR LAWMAKERS (Saskia Kim, Ed., 2008).
[35] *Supra* note 22.

Conclusion

Californians support quick access to location data in emergency contexts, but in non-emergency contexts, when law enforcement seeks historical location data, they support limits on law enforcement access. Californians support giving notice to individuals before their location data is access by law enforcement. They also support judicial intervention before this data is accessed.

When applying the Westin privacy segmentation, we found that generally, the Westin privacy segmentation was not predictive in assessing Californians' attitudes towards privacy of wireless phone location data.

Appendix 1: Survey Questions and Responses

Question 1: Individuals now own many technological devices to make life easier, such as cell phones. I am going to ask some questions concerning these technologies and your privacy.

True or false: "Carrying a cell phone gives law enforcement the ability to track the places I go."

Results:

Valid%	%	N	VALUE	LABEL
65.1	61.2	606	1	True
34.9	32.8	325	0	False
	5.6	55	8	Don't Know
		4	9	Refused/Missing Data
-----		----		
100%		931/991 valid cases		

Mean: .65 Median: 1.0 Mode: 1 Std. Deviation: .477

Question 2: Tell us how strongly you agree or disagree with the following statement:

In an emergency, the police should be able to find out where I am by tracking my cell phone. Do you Strongly agree, agree, disagree, or strongly disagree?

Valid %	%	N	VALUE	LABEL
40.6	39.9	395	1	Strongly agree
42.8	42.0	416	2	Agree
11.3	11.1	110	3	Disagree
5.3	5.2	5.2	4	Strongly disagree
	1.6	15	8	Don't Know
		3	9	Refused/Missing Data
-----		-----		
100%		973/991 valid cases		

Mean: 1.81 Median: 2.0 Mode: 2 Std. Deviation: .835

Question 3: Now, I would like to ask you about possible rules and procedures to protect data that reveals the location of others. Suppose that the police wanted to determine where an individual was one week ago.

Would you favor a law that required the police to tell the individual before obtaining location information from the cell phone company?

Would you: Strongly support, support, oppose, or strongly oppose this?

Valid %	%	N	VALUE	LABEL
25.0	24.2	116	1	Strongly support
47.5	45.9	220	2	Support
19.5	18.8	90	3	Oppose
8.1	7.8	37	4	Strongly oppose
	3.3	16	8	Don't Know
		1	9	Refused/Missing Data
---		---		
100%		512/991 valid cases		

Mean: 2.11 Median: 2.0 Mode: 2 Std. Deviation: .871

Question 4: Now, I would like to ask you about possible rules and procedures to protect data that reveals the location of others. Suppose that the police wanted to determine where an individual was one week ago.

Would you favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company?

Would you: Strongly support, support, oppose, or strongly oppose this?

Valid %	%	N	VALUE	LABEL
32.4	31.1	157	1	Strongly support
40.8	39.1	198	2	Support
18.4	17.6	89	3	Oppose
8.3	8.0	40	4	Strongly oppose
	2.2	21	8	Don't Know
		5	9	Refused/Missing Data
---		---		
100%		506/991 valid cases		

Mean: 2.03 Median: 2.0 Mode: 2 Std. Deviation: .918

Appendix 2: Westin Segmentation Questions

In order to calculate membership in one of Westin's three privacy segments, we categorized respondents based on their answers to the following three questions, using Westin's rationale: "Privacy Fundamentalists are respondents who agreed (strongly or somewhat) with [Question 1] and disagreed (strongly or somewhat) with [Question 2 and Question 3]. Privacy Unconcerned are those respondents who disagreed with [Question 1] and agreed with [Question 2 and Question 3]. Privacy Pragmatists are all other respondents."[36] Respondents who did not provide a valid answer for all three of these questions were considered invalid for the purposes of this categorization.

Westin Question 1: For each of the following statements, how strongly do you agree or disagree? First...

"Consumers have lost all control over how personal information is collected and used by companies."

Do you Strongly agree, agree, disagree, or strongly disagree?

Valid %	%	N	VALUE	LABEL
39.8	38.7	377	1	Strongly agree
33.1	31.7	314	2	Agree
13.5	12.9	128	3	Disagree
13.7	13.1	130	4	Strongly Disagree
	4.1	41	8	Don't Know
		1	9	Refused/Missing Data
-----		-----		
100%		949/991 valid cases		
Mean: 2.01	Median: 2.0	Mode: 1	Std. Deviation: 1.039	

[36] Westin 1999.

Westin Question 2: How about...

"Most businesses handle the personal information they collect about consumers in a proper and confidential way."

Do you Strongly agree, agree, disagree, or strongly disagree?

Valid %	%	N	VALUE	LABEL
12.9	12.2	121	1	Strongly agree
40.3	38.3	380	2	Agree
25.2	24.0	238	3	Disagree
21.6	20.5	204	4	Strongly disagree
	4.8	48	8	Don't Know
		1	9	Refused/Missing Data
-----		-----		
100%		942/991 valid cases		

Mean: 2.56 Median: 2.0 Mode: 2 Std. Deviation: .968

Westin Question 3: How about...

"Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today."

Do you Strongly agree, agree, disagree, or strongly disagree?

Valid %	%	N	VALUE	LABEL
10.9	10.2	101	1	Strongly agree
46.8	43.7	433	2	Agree
26.4	24.7	244	3	Disagree
15.9	14.9	148	4	Strongly disagree
	6.1	61	8	Don't Know
		4	9	Refused/Missing Data
-----		-----		
100%		926/991 valid cases		

Mean: 2.47 Median: 2.0 Mode: 2 Std. Deviation: .887

Appendix 3: Westin Segments Applied To Questions 1 Through 4

Please see Appendix 1 for more detail about these questions.

Question 1: True or false: "Carrying a cell phone gives law enforcement the ability to track the places I go."

	True	**%**	**False**	**%**	**Total**
Fundamentalists	128	66.3%	65	33.7%	193
Pragmatists	420	66.2%	214	33.8%	634
Unconcerned	12	40%	18	60%	30
Total	560	65.3%	297	34.7%	857

Question 2: In an emergency, the police should be able to find out where I am by tracking my cell phone. Do you strongly agree, agree, disagree, or strongly disagree?

	Strongly Agree	**%**	**Agree**	**%**	**Disagree**	**%**	**Strongly Disagree**	**%**	**Total**
Fundamentalists	59	29.6	108	54.3	20	10.1	12	6.0	199
Pragmatists	281	42.6	275	41.7	76	11.5	28	4.2	660
Unconcerned	11	36.7	11	36.7	8	26.7	0	0	30
Total	351	39.5	394	44.3	104	11.7	40	4.5	889

Question 3: Would you favor a law that required the police to tell the individual before obtaining location information from the cell phone company?

	Strongly Support	**%**	**Support**	**%**	**Oppose**	**%**	**Strongly Oppose**	**%**	**Total**
Fundamentalists	43	45.7	29	30.9	12	12.8	10	10.6	94
Pragmatists	66	21.0	154	49.0	71	22.6	23	7.3	314
Unconcerned	3	18.8	9	56.3	4	25.0	0	0	16
Total	112	26.4	192	45.3	87	20.5	33	7.8	424

Question 4: Would you favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company?

	Strongly Support	**%**	**Support**	**%**	**Oppose**	**%**	**Strongly Oppose**	**%**	**Total**
Fundamentalists	40	37.4	50	46.7	14	13.1	3	2.8	107
Pragmatists	105	31.5	131	39.3	63	18.9	34	10.2	333
Unconcerned	2	12.5	4	25.0	8	50.0	2	12.5	16
Total	147	32.2	185	40.6	85	18.6	39	8.6	456