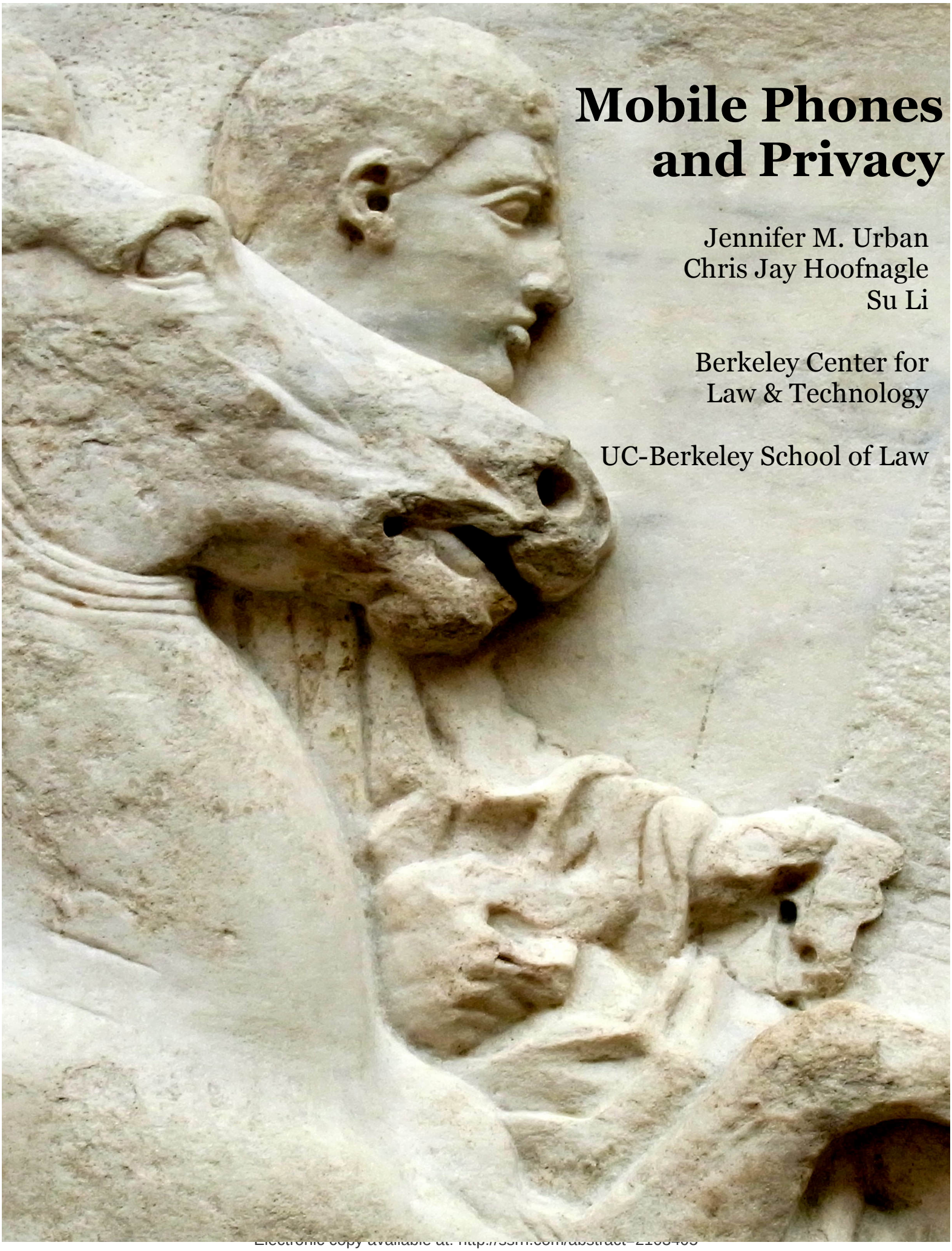

Mobile Phones and Privacy

Jennifer M. Urban
Chris Jay Hoofnagle
Su Li

Berkeley Center for
Law & Technology

UC-Berkeley School of Law

Mobile Phones and Privacy

Jennifer M. Urban,* Chris Jay Hoofnagle† & Su Li‡

Berkeley Consumer Privacy Survey

BCLT Research Paper§

July 11, 2012

* Jennifer M. Urban is Assistant Clinical Professor of Law at UC Berkeley Law, and Director of the Samuelson Law, Technology & Public Policy Clinic.
† Chris Jay Hoofnagle is a Lecturer in Residence at UC Berkeley Law and Senior Staff Attorney to the Samuelson Law, Technology & Public Policy Clinic.
‡ Dr. Su Li is Statistician of Empirical Legal Studies at UC Berkeley Law.
§ The underlying survey research for this paper was fully funded by Nokia, Inc. as part of an unrestricted research gift to the Berkeley Center for Law and Technology. The cover image is from the Parthenon Frieze.

Introduction: Privacy and mobile phone data

Mobile phones are a rich source of personal information about individuals. Both private and public sector actors seek to collect this information. Many mobile applications seek identification information, location data, and other user information.[1] Facebook, among other companies, recently ignited a controversy by collecting address book information from users' mobile phones via its mobile app.[2] And a recent Congressional investigation found that law enforcement agencies sought access to wireless phone records over one million times in 2011.[3] As these developments receive greater attention in the media, a public policy debate has started concerning the collection and use of information by private and public actors.

To inform this debate and to better understand Americans' attitudes towards privacy in data generated by or stored on mobile phones, we commissioned a nationwide, telephonic (both wireline and wireless) survey of 1,200 households. The survey questions covered in this paper focused on known ways that mobile phones and service providers are likely to store data, and on likely scenarios under which service providers—including mobile "app" providers—are likely to collect and share information about consumers. We also explored issues surrounding law enforcement access to data stored on phones.

We found that Americans overwhelmingly consider information stored on their mobile phones to be private—at least as private as information stored on their home computers. This is perhaps unsurprising, given that we also found widespread understanding that sensitive personal information such as text messages, contact lists, and voicemail is stored on phones, and that substantial percentages of respondents with smartphones used them to engage in activities that might generate sensitive information, including visiting websites, using social networking services, and using location services.

Given that Americans consider information on mobile phones to be private, it is in turn unsurprising that they also overwhelmingly reject several types of data collection and use drawn from current business and law enforcement practices. Specifically, large majorities reject the collection of contact lists

---

[1] *See generally* Julia Angwin & Jennifer Valentino-Devries, *What They Know—Mobile*, Wall Street Journal, available at http://blogs.wsj.com/wtk-mobile/.
[2] Jennifer van Grove, *Your address book is mine: Many iPhone apps take your data*, VENTUREBEAT, Feb. 14, 2012, available at http://venturebeat.com/2012/02/14/iphone-address-book/.
[3] Representative Ed Markey, *Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers*, Jul. 9, 2012, available at http://markey.house.gov/press-release/markey-law-enforcement-collecting-information-millions-americans-mobile-phone-carriers.

stored on the phone for the purposes of tailoring social network "friend" suggestions and providing coupons, the collection of location data for tailoring ads, and the retention of location data by wireless service providers for longer than one year. Additionally, large majorities favor requiring permission from a judge before law enforcement officers search mobile phones seized during an arrest.

This study follows our previous work examining attitudes towards mobile payments systems,[4] in which we found that Americans also overwhelmingly oppose the revelation of contact information (phone number, email address, and home address) to merchants when making purchases with mobile payment systems, and that they express an even higher level of opposition to systems that collect information about consumers through their mobile phones while they are browsing in a store.

In each of these studies, we sought to gather information about Americans' understanding and attitudes about information on their phones and current or likely near-future mobile information collection, sharing, and use scenarios.

Overall, our findings suggest that Americans are likely to reject a variety of uses of mobile phone data that are attractive to merchants, marketers, and law enforcement officials. This suggests that the value proposition offered to consumers by service providers, and the cost-benefit analysis offered to citizens by government officials, should be especially clear and compelling for desired uses of mobile phone data. As it is, services are sometimes resistant to clearly explaining the privacy implications of services. This means that in addition to ex ante interventions such as clearer disclosures and choice mechanisms, consumers should have ex post remedies that allow them to exit these exchanges whole.

Further, the high level of rejection expressed by respondents makes questions about the transparency of mobile data collection and use, the availability of realistic, privacy-friendly alternatives in the market, and questions about what privacy protections should govern this collection and use, especially salient. Our results suggest that Americans may support limitations on the collection, transfer, and retention of mobile phone data. And the results strongly suggest that transparency about how mobile data is collected and used, along with robust user controls and procedural and technical privacy safeguards, may be necessary to avoid backlash against programs that rely on mobile data.

---

[4] Chris Jay Hoofnagle, Jennifer M. Urban, and Su Li, *Mobile Payments: Consumer Benefits & New Privacy Concerns* (April 24, 2012), available at: http://ssrn.com/abstract=2045580.

Mobile data collection is a feature of American daily life

The mobile phone occupies a central role in many Americans' lives.[5] We text, talk, store photographs, play apps, get directions, and use social networking services through mobile devices. Many of these activities generate extensive records of our associations with other people, our locations, what we read, and our thoughts about the world.

This trend is only growing as more people use app-enabled[6] smartphones and the phones' capabilities grow. Mobile services provide many benefits, including—to name only a few—richer communications, useful services,[7] and greater access to Internet resources.[8]

Privacy risks raised by mobile data collection and use

Widespread collection and use of mobile phone data, however, also raises substantial new privacy risks. There are at least three ways in which the integration of mobile phones into daily life—indeed, into every aspect of daily life—potentially exposes individuals to new privacy risks.

First, as evidenced by our results as well as previous studies, very rich sets of personal information—text messages, phone numbers called, photographs, and contact information, to name a few types—are stored on the great majority of Americans' mobile phones. Users choose to store some of these

---

[5] According to the Pew Internet & American Life Project, 88 percent of Americans have a wireless phone, and 46 percent of Americans have a "smartphone." Aaron Smith, *Nearly half of American adults are smartphone owners*, Pew Research Center's Internet & American Life Project, Mar. 1, 2012, available at http://pewinternet.org/Reports/2012/Smartphone-Update-2012/Findings.aspx.

[6] The percentage of American adults who have downloaded an app to their phones doubled between 2009 and 2011. Kristen Purcell, *Half of adult cell phone owners have apps on their phones*, Pew Research Center's Internet & American Life Project, Nov. 2, 2011, available at http://pewinternet.org/Reports/2011/Apps-update.aspx.

[7] Services range from location-based direction and mapping services, to games, to e-book readers. *See, e.g.*, Kathryn Zickuhr, *Three-quarters of smartphone owners use location-based services*, Pew Research Center's Internet & American Life Project, May 11, 2012, available at http://pewinternet.org/Reports/2012/Location-based-services.aspx; Lee Rainie, Kathryn Zickuhr, Kristen Purcell, Mary Madden, Joanna Brenner, *The rise of e-reading*, Pew Research Center's Internet & American Life Project, Apr. 5, 2012, available at http://libraries.pewinternet.org/2012/04/04/the-rise-of-e-reading/#fn-419-3 (noting that 29% of e-book readers consume them via cell phones).

[8] Indeed, for some Americans, mobile phones alleviate a lack of other options for accessing the Internet. Aaron Smith, *17% of cell phone owners do most of their online browsing on their phone, rather than a computer or other device*, Pew Research Center's Internet & American Life Project, June 26, 2012, available at http://pewinternet.org/Reports/2012/Cell-Internet-Use-2012.aspx.

types of information, such as photographs, music, or contact lists; others, such as text messages, numbers called, and the unique identifiers on mobile phones, are stored automatically. Thus, like service providers, mobile devices themselves are becoming targets of law enforcement officers' and marketers' interest.

Second, many smartphone users use Internet browsers or install task-specific "apps" that may store further information (either on the phone or in another location) that is exceedingly rich. For example, as described below,[9] 56% of our respondents with cell phones use their phones to visit websites, and 42% use social networking services via phone-based apps. These activities can reveal communications with circles of contacts, health-related or other personal research queries, and a wide variety of intellectual and political interests, to name just a few revealing types of information. Sometimes these apps request information from other apps, thereby heightening privacy risks.

Third, as noted above, location awareness is a significant feature of mobile phones. Put simply, mobile phones are tracking devices. This has obvious benefit to their users—46% of our respondents with cell phones, for example, use location services like GPS and mapping services via their phones.[10] At the same time, our results show that people are concerned about the collection, storage, and use of location data.[11]

In earlier work, we detailed how some merchants have adopted systems to track consumers as they browse stores.[12] For instance, Navizon I.T.S. claims that it can track, "any Wi-Fi enabled smart phone or tablet, including iPhones, iPads, Android devices, BlackBerry, Windows Mobile, Symbian and, of course, laptops."[13] As with many other tracking technologies, it seems to be designed to operate without the knowledge of the individual. Navizon claims, "Unobtrusive surveillance / Navizon I.T.S. works in the background, quietly and unobtrusively locating Wi-Fi- enabled devices…No application is needed on the devices to be tracked. The only requirement is that their Wi-Fi

---

[9] *See infra* p. 7.
[10] *See id.*
[11] *See infra* Survey Results section. Others have found similar concerns, for example, that people are more comfortable broadcasting their locations from high-traffic locations, where they are less likely to be revealing detailed information about themselves in doing so. Eran Toch, Justin Cranshaw, Paul Hankes Drielsma, Janice Y. Tsai, Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, & Norman Sadeh, *Empirical models of privacy in location sharing* 129-138, at 134-137, *in* Proceedings of the 12th ACM international conference on Ubiquitous computing (Ubicomp 2010), available at http://doi.acm.org/10.1145/1864349.1864364.
[12] Chris Jay Hoofnagle, Jennifer M. Urban, and Su Li, *Mobile Payments*, *supra* note 4.
[13] NAVIZON, TRACK WI-FI ENABLED DEVICES INDOORS WITH FLOOR/ROOM-LEVEL ACCURACY, available at http://www.navizon.com/its.php.

radios be turned on, which is the default in most smart phones, tablets and laptops."[14]

These types of tracking systems, which have already been used by retailers,[15] are very likely to enable merchants to identify mobile phone users. Because some of these systems rely upon unique, unchangeable identifiers built into devices, users may have no way to avoid collection of data or tracking over time. And as noted above, law enforcement officials seek large amounts of cell phone information from service providers, including location data,[16] raising issues of government surveillance and process questions.

Survey results

In order to learn more about consumers' understanding and attitudes concerning privacy and mobile phone data, we commissioned a nationwide, telephonic survey of Americans. As in our mobile payments study, we formulated questions to reflect existing and probable data collection and use scenarios, based on current consumer and service provider behavior and likely service provider plans for new systems.

Overall, most Americans (91% of our respondents) own mobile phones, and about half (50% of all our respondents, and 54-56% of cell phone owners) own smartphones.[17] As described below, mobile phones are used for a wide variety of purposes. Americans overwhelmingly consider information stored on their phones to be private, and strongly reject systems that would rely on collecting and using contact data from their phones or tracking their locations. This strong rejection stands in sharp contrast to consistent trends among mobile app providers, marketers, and law enforcement officials, to

---

[14] *Id.*

[15] Annalyn Censky, *Malls stop tracking shoppers' cell phones*, CNN MONEY, Nov. 28, 2011, available at http://money.cnn.com/2011/11/28/news/economy/malls_track_shoppers_cell_phones/index.htm.

[16] *See* Markey, *supra* note 3.

[17] The Pew Research Center recently found similar numbers. Aaron Smith, *Nearly half of American adults are smartphone owners*, Pew Research Center's Internet & American Life Project Mar. 1, 2012, available at http://pewinternet.org/Reports/2012/Smartphone-Update-2012/Findings.aspx. We followed the methods in the Pew study in determining whether respondents own "smartphones." In our survey, 54% of cell phone owners claimed that they owned a "smartphone." We then followed up with a question that asked those respondents to state the kind of phone they had, and tallied responses that reflected smartphone ownership. Fifty-six percent of the responses clearly or very likely indicated that respondents owned smartphones—close to the 54% of cell phone owners who responded directly that they owned a smartphone, and within the 3.4-point margin of error. As such, we are reasonably confident that 54% is a close approximation of the true number of cell-phone-owner respondents who own smartphones. This is about 50% of our entire sample, including the 9% who did not own any mobile phone.

collect and use personal information stored on or transmitted by mobile phones. In addition, survey respondents rejected several value propositions implicit in recent app providers' data collection practices.

A wide variety of data is collected on or by mobile phones

As also found in the studies cited above, we found that survey respondents commonly use their phones for a wide variety of purposes,[18] as shown in the following table:

Which of the following things do you use your phone for?*	Yes	No	Don't Know/ Refused
Making voice phone calls	89%	11%	*
Sending and receiving text messages	85%	15%	*
Sending and receiving email	52%	48%	*
Playing games, such as "Angry Birds"	35%	65%	*
Visiting any type of website	56%	44%	*
Using social networking services, such as Facebook or Twitter, Foursquare or others	42%	57%	*
Making purchases	20%	80%	*
Listening to music	41%	59%	*
Using location services, such as GPS and map services	46%	54%	*
Taking photographs or videos	75%	25%	*

Table 1: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margins of error are from 1.8 to 3 percentage points. *For actual wording, see Appendix 2: Survey Question Q20.

These activities generate a great deal of information about phone users' communicated thoughts (via, for example, text messages, and voicemail messages); intellectual life (via, for example, access to specific websites); relationships (via, for example, contact lists, numbers called, and text messages); and habits (via, for example, location services and calendar information). We therefore sought to understand what kind of information Americans stored, or believed to be stored, on their mobile phones.

[18] Note that this question was asked of the 91% of respondents who owned any kind of working mobile phone. A little more than half of those respondents stated that they owned smartphones. As such, some of the activities we asked about—for example, using social networking services—likely show lower percentages, in part, because they can only be engaged in by people using smartphones.

Again, we found that a high percentage of respondents store (or, for some more passively-collected categories, believe the phone to store) a wide variety of personal information.

Which of the following items, if any, is stored on your phone?*	Yes	No	Don't Know/ Refused
Text messages	78%	21%	1%
Contact information (as in an address book)	82%	17%	*
Email messages	48%	51%	1%
Voicemail messages	74%	26%	*
Photos or videos	75%	25%	*
Voice memos or notes	39%	60%	1%
Information about websites you have visited	37%	60%	3%
Passwords of websites you have visited or applications you have used	27%	71%	1%
Music	41%	58%	*
Information about your present location or where you have been	24%	70%	6%

Table 2: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margins of error are from 2.1 to 3 percentage points. *For actual wording, see Appendix 2: Survey Question Q21.

Americans consider information stored on mobile phones to be private

Given the richness of the information contained on mobile phones or transmitted to service providers from them, it is unsurprising that we found that Americans consider information on their phones to be private. We based this finding on respondents' answers to several questions, discussed next.

Data on mobile phones compared to data on home computers

We asked Americans whether they thought the information on their phones was more private, less private, or about as private as information on their home computers. We specified "home" computer in order to distinguish it from work machines, and to make certain that we were asking about a machine that (with a few exceptions) is searchable by law enforcement only with a warrant.

A large majority—78%—of Americans consider information on their mobile phones at least as private as that on their home computers. Fifty-nine percent consider it "about as private" and 19% consider it "more private."

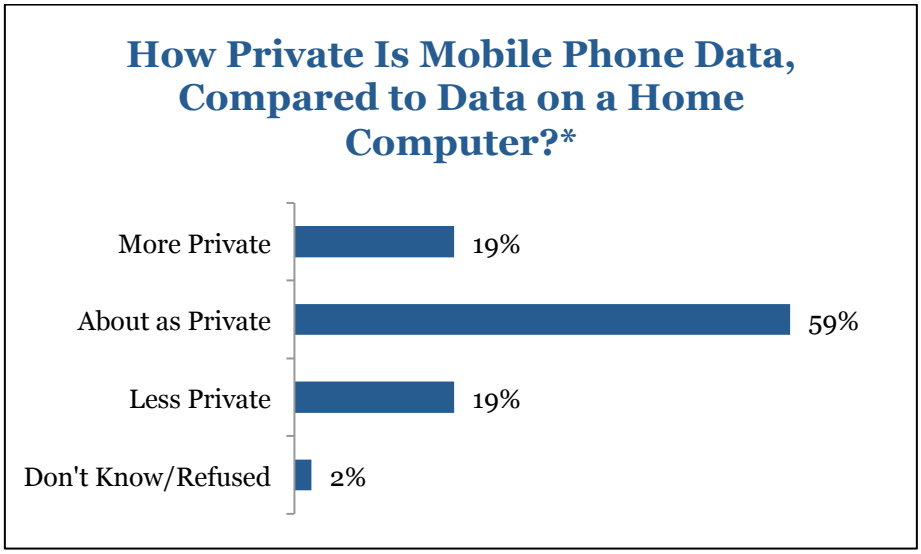

Figure 1: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margins of error are from 1 to 3 percentage points. *For actual wording, see Appendix 2: Survey Question Q22.

We think it uncontroversial that Americans consider information on their home computers to be "private" and thus that comparing its relative privacy to mobile phone data is likely to garner useful information about how private Americans consider that data to be. However, we also used two further sets of questions in order to check this assumption and to refine our understanding of respondents' attitudes toward mobile phone data: 1) under what circumstances should law enforcement be able to search a mobile phone when arresting its owner? and 2) to whom (if anyone) would respondents be willing to lend their phone?

Law enforcement searches of mobile phones during arrest

First, we asked Americans about searches of mobile phones when individuals are arrested. We asked whether law enforcement officers should have to get permission from a court prior to searching the phone of a person arrested on suspicion of committing a crime, if the person does not consent to having the phone searched.[19] Responses to this question help establish respondents'

[19] Of course, the standard that a court applies to such requests varies based on the type and location of the information to be searched. A more focused version of this question would have distinguished among warrants, court orders, and other procedures. However, this would have been confusing for respondents, especially in light of the amount of information we decided we needed to give about the scenario

general expectation of privacy in mobile phone data, as well as their specific preferences with regard to searches by law enforcement.

A large majority of respondents—76%—supported requiring officers to get permission from a court prior to searching a mobile phone in this situation. Twenty-two percent thought that permission from a court should not be required, and only three percent either did not know or declined to answer.

We hypothesized that Americans would respond differently if the information on the mobile phone were protected by a password. Such a protection might evince a stronger expectation of privacy of the citizen being searched. To test this hypothesis, we asked whether, in the same search after arrest scenario, officers should be able to guess the password on a password-protected phone without permission from a court or whether they should have to get permission from a court prior to guessing the password. Both results are shown in the table below:

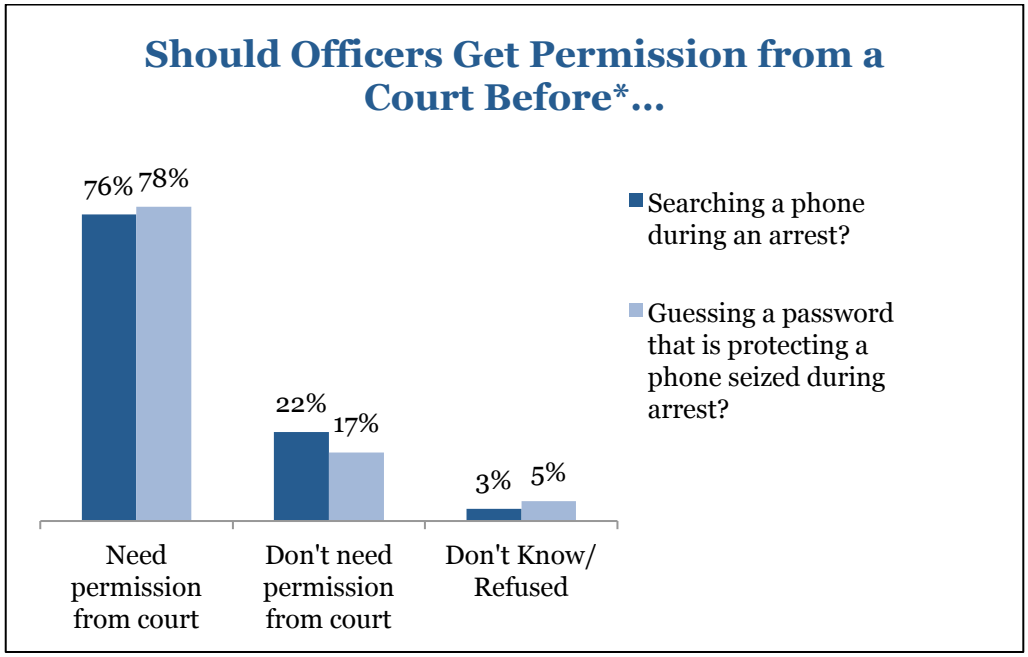

Figure 2: Based all respondents (*n = 1203*). Results are weighted to account for known demographic discrepancies. Margins of error are from 2.3 to 2.4 percentage points. *For actual wording, see Appendix 2: Survey Questions Q24 and Q24a.

We found little difference in response to the password-protected phone scenario, likely because such a large majority favored prior court permission

---

in order to avoid biasing the question in favor of or against the search, so we simplified the requirement. In order to avoid biasing the respondents for or against the search, we drafted the question to include basic, neutral facts about a search incident to arrest: the subject is suspected of committing a crime; the officer always searches through the arrestee's possessions; and the search of phone may include looking at texts or photos, seeing what calls have been made, and the like.

regardless of password protection. Respondents still overwhelmingly—78%—stated that the officer should have to get permission from a court before guessing the password. Slightly fewer—17%, down from 22%—stated that permission from a court should not be required, and slightly more—5%, instead of 3%—did not know or chose not to respond to the question. These answers, however, did not differ significantly from answers to the more general question.

This finding suggests that Americans' attitudes diverge from several cases in which courts have upheld searches of wireless phones during arrest, treating the phones as if they were any other container possessed by the suspect.[20]

Willingness to lend mobile phones

In a final set of questions intended to develop a basic understanding of respondents' expectation of privacy in their phones, we queried whether respondents would be willing to lend their phones for others' use. These questions followed qualitative research undertaken by others[21] that, using different methods, similarly considered respondents' attitudes toward lending their phones.

We asked whether respondents would be willing to lend their phones to someone else to use for a few hours while they ran errands on their own. We chose this scenario because we wanted to be certain that respondents imagined giving their phone to persons who could then use it out of the owners' sight and control, rather than imagining standing nearby while a person made a quick phone call or some other scenario that gave the phone's owner some measure of knowledge and control over the use of the phone.

We asked respondents to consider this question for people in different categories of relationship to them, ranging from close family members to strangers.

Responses are shown in the table below. Unsurprisingly, respondents were most likely to lend their phones to those closest to them, and least likely to lend their phones to strangers. A bare majority—51%—responded that they would "definitely allow" a spouse or other close family member to use the phone, and an overwhelming majority—84%—would either "definitely allow" or "probably allow" this. Respondents were more evenly split on whether to

---

[20] *See e.g.*, *U.S. v. Curtis*, 635 F.3d 704 (5th Cir. 2011); *U.S. v. Finley*, 477 F.3d 250 (5th Cir. 2007); *People v. Diaz*, 244 P.3d 501 (Cal. Jan. 3, 2011).

[21] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter, *Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones*, *in* Proceedings of the 27th International Conference on Human factors in Computing systems (CHI 2009), available at http://dl.acm.org/citation.cfm?id=1518953&CFID=125066656&CFTOKEN=35359539; Jennifer King, *How come I'm allowing strangers to go through my phone?: Smart Phones and Privacy Expectations*, unpublished research manuscript, June 2012 (on file with authors).

allow close friends to use the phone, and for less close connections—acquaintances, work colleagues, and strangers—overwhelming majorities stated that they were unlikely to agree to lend the phone.

Would you allow these people to borrow your phone?*	Definitely Allow	Probably Allow	Probably Not Allow	Definitely Not Allow	Don't Know/ Refused
A spouse or other close family member	51%	33%	7%	9%	*
A close friend	26%	29%	18%	28%	*
An acquaintance	4%	11%	25%	59%	1%
A work colleague	6%	15%	21%	56%	2%
A stranger	1%	2%	7%	90%	*

Table 3: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margins of error are from 1 to 3 percentage points. The choices were rotated when read. *For actual wording, see Appendix 2: Survey Question Q25.

We then asked respondents the main reason why they would not allow some people to borrow their phones. Results are shown in the table below. "Privacy" and "Has a lot of personal information on it" were the most-mentioned responses, followed by responses that suggested the possibility of damage to or loss of the phone itself, and responses that expressed a more general lack of trust in what the person using the phone might do with it. Overall, concerns about private information—in some form—constituted the most common response. [22]

[22] We note that to some degree, the number of "privacy" responses may have been enhanced by priming effects caused by the fact that, in order to find out about relevant knowledge and preferences, we could not avoid asking questions about tracking, personal information, and the like, including some questions that specifically mentioned "privacy" or "private." Though the survey was not introduced as such, it is very likely that respondents gathered that they were being asked, at least in part, about privacy issues. We do not, however, think this is likely to undermine the central finding that a large majority of Americans in our sample think of information on their mobile phones as private, given respondents' answers to other questions and the uncontroversially personal nature of some information—such as contact lists and photographs—kept on most mobile phones.

What is the main reason you would not allow others to borrow your phone?*	Percent responding with this answer
Privacy	17%
Has a lot of personal information on it	12%
They may damage/lose/steal it	10%
Never know what they'll do with it/May abuse it/Takes away my control of the phone	10%
Trust issue	8%
It's mine/my phone/personal	7%
Need phone at all times	6%
Security	5%
Don't really know them	5%
Worried borrower would read emails or texts or look at pictures or contacts	4%

Table 4: Based on cell phone owners who would not lend their phones to all categories in Table 3 (*n = 1105*). Results are weighted to account for known demographic discrepancies. Margins of error are between 1 and 2 percentage points. *For actual wording, see Appendix 2: Survey Question Q26. *Note: Table reports first mention only. Responses of 2% or less are omitted. See Survey Question Q26 for further responses.*

Sharing information for marketing and advertising purposes

The rich, location-aware information that can be collected by mobile apps could be used for a variety of attractive services, marketing and business analytical purposes. We asked Americans about their preferences for engaging in information sharing for several marketing or service-oriented purposes that companies have already proposed or implemented, or that are likely in the near future.

Specifically, we asked whether respondents thought merchants should be able to contact them via a mobile phone number given at the point of sale to offer further information on products or services; whether they would be willing to share the contact list on their phone with an app in order to obtain more social networking contacts; and whether they would be willing to share the contact list in order for their contacts to also receive coupons from a coupons app they have chosen to download.

Each of these scenarios presents a value proposition to the consumer and a choice to accept the proposition or not. In developing the scenarios, we used

the value proposition implicit in their real-world counterparts (for example, the collection of contact lists by Facebook) in order to gain understanding of consumers' reaction to these value propositions. We note, however, that in real-world examples, consumers are often never actually presented with the specific value proposition to consider—collection occurs passively and without explicit permission. We discuss this further below.

Marketing contact via mobile phone

Telemarketing to wireless phones has been illegal since 1991, but firms may make sales calls to consumers with whom they have an established business relationship. This means that when a consumer gives contact information to a cashier, generally speaking, the business can start calling that consumer.

We explored whether consumers thought that an established business relationship justified telemarketing to customers. We asked respondents whether, if they provided their cell phone number to a cashier, the store should be able to call them later to offer more information about products and services. Seventy-four percent objected to this use of the cell phone number, an unsurprising result in light of the popularity of the Do Not Call Registry for objecting to telemarketing.[23] Twenty-four percent, however, agreed that the store should be able to call. (Three percent did not know or did not respond.)

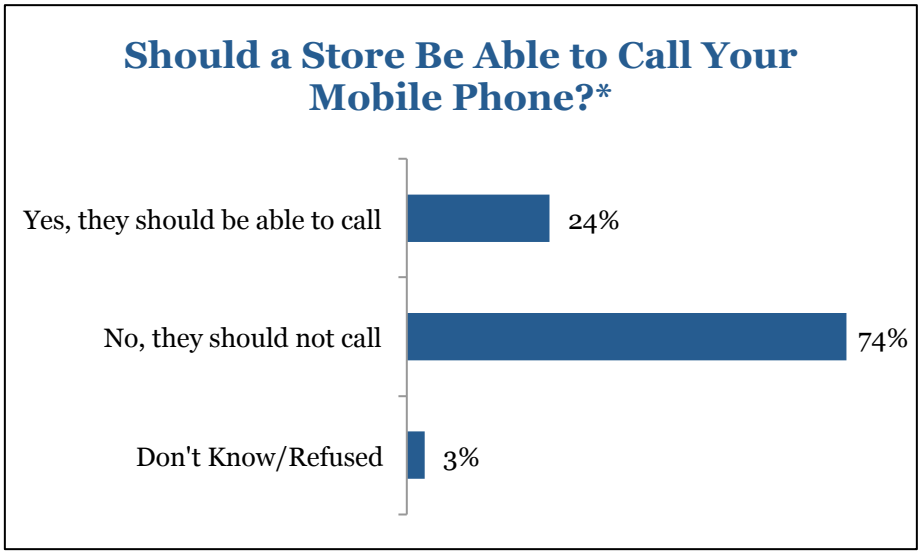

Figure 3: Based all respondents (*n = 1203*). Results are weighted to account for known demographic discrepancies. Margin of error is 2.5 percentage points. *For actual wording, see Appendix 2: Survey Question Q14.

[23] As of December 2011, 209 million numbers had been enrolled in the National Do-Not-Call Registry. FEDERAL TRADE COMMISSION, FTC SENDS BIENNIAL REPORT TO CONGRESS ON THE NATIONAL DO NOT CALL REGISTRY, Dec. 30, 2011, available at http://www.ftc.gov/opa/2011/12/dnc.shtm.

This finding is in line with our previous work finding that consumers consider their telephone numbers sensitive information, and are unlikely to accept having them shared at the point of sale via a mobile payments system.[24]

Data collection via apps

Depending on the configuration of a smartphone's operating system, mobile phone apps can be capable both of collecting information directly—for example, by tracking posts to social networking sites, data input by users, or reading, viewing, and listening practices—and of collecting information stored in other phone applications.

At least some app providers have configured their apps to collect data stored in other locations on the phone. In 2011, for example, Facebook garnered press attention for using its mobile app to collect contact lists from the phones of consumers who had the app installed.[25] Facebook used the contact lists to suggest additional "friend" contacts to those consumers. When the practice came to light, however, consumers expressed outrage.

The controversy over Facebook's contact list collection was followed in February of this year by revelations that Path, another social networking company, was also uploading mobile address books to its servers via mobile phone apps without notice or consent, along with revelations that the practice was not limited to Facebook and Path. Close on the heels of the Path story were revelations that many app makers collected contact lists and stored them on their servers.

Backlash was swift, and has to date included a lawsuit against eighteen companies that allegedly collected contact data via apps,[26] a congressional demand to Apple to appear and explain its role in the practice,[27] and a decision by Apple to update the iPhone iOS to allow access to contact data only with explicit consumer permission.[28]

---

[24] Chris Jay Hoofnagle, Jennifer M. Urban, and Su Li, *Mobile Payments*, *supra* note 4.

[25] *See, e.g.*, Dan Tynan, *Facebook's phonebook fiasco*, IT WORLD (Aug. 11, 2011), at http://www.itworld.com/it-managementstrategy/192399/facebooks-phonebook-fiasco (describing the Facebook syncing feature).

[26] Chloe Albanesius, *18 Firms Sued Over App Privacy, Including Apple, Twitter, Facebook*, PCMAG.COM (Mar. 15, 2012), at http://www.pcmag.com/article2/0,2817,2401625,00.asp.

[27] *See, e.g.*, Fahmida Y. Rashid, *Congress Demands Apple Clarify Mobile Privacy Policy*, PCMAG.COM (Mar. 15, 2012), at http://securitywatch.pcmag.com/mobile-apps/295412-congress-demands-apple-clarify-mobile-privacy-policy.

[28] *See, e.g.*, Sandhya Raman, *Amid privacy uproar, Apple promises to detail app permissions*, FIERCEMOBILE CONTENT, Feb. 15, 2012, available at http://www.fiercemobilecontent.com/story/controversial-path-app-coming-microsofts-windows-phone/2012-03-26.

This reaction brings to mind other examples—such as DoubleClick's year 2000 attempt to combine web tracking and offline information, and the GoogleBuzz rollout—in which failing to develop sufficient privacy practices and transparency at the outset created enough backlash to cause companies to substantially change their plans.[29] As such, companies may be well served by knowing consumers' baseline attitudes before commencing with features that may have an impact on privacy.

In some cases, however, companies may prefer not to ask in advance—specifically because customers are likely to reject the value proposition if it is explained clearly. One salient example of this problem is elucidated by Douglas Edwards in his recent book about working at Google. Edwards discussed Google's first-party cookie policy:

> What if we let users opt out of accepting our cookies altogether? I liked that idea, but Marissa [Mayer] raised an interesting point. We would clearly want to set the default as "accept Google's cookies." If we fully explained what that meant to most users, however, they would probably prefer *not* to accept our cookie. So our default setting would go against users' wishes. Some people might call that evil, and evil made Marissa uncomfortable. She was disturbed that our current cookie-setting practices made the argument a reasonable one. She agreed that at the very least we should have a page telling users how they could delete their cookies, whether set by Google or by some other website.[30]

This anecdote also shows why the market can fail to produce privacy-friendly options for consumers. Even when companies know that consumers want more privacy, firms can have incentives to code in privacy-invasive options by default. Firms may also have incentives to hide the tussle. Google could have implemented compromise approaches that preserved some privacy, by using session cookies or by choosing cookies that expired after some short amount of time, but it did not.

This anecdote also speaks to those who criticize survey research on privacy as incomplete because it does not present the tradeoffs consumers experience in transactions. These critics argue that without a value judgment in terms of provision of services, consumers will always say that they value privacy but act contrary to their aspirations. That critique misses the point that consumers often have no realistic privacy-friendly option, and that popular services are almost always offered on a take-it-or-leave-it basis, with information collection maximized and little information about the

---

[29] Indeed, DoubleClick's shares lost nearly 90% of their value after the Federal Trade Commission opened an investigation. Stefanie Olsen, *FTC Drops Probe into DoubleClick Privacy Practices*, CNET.COM, Jan. 22, 2001, available at http://news.cnet.com/2100-1023-251325.html.

[30] Douglas Edwards, I'M FEELING LUCKY: THE CONFESSIONS OF GOOGLE EMPLOYEE NUMBER 59, at 341 (HMH 2011).

actual collection practices. In the Facebook example above, for instance, people were surprised by the contact list collection despite the fact that the feature was covered by Facebook's privacy policy.[31]

We do think that better information about value propositions offered by app makers and other service providers, and consumers' attitudes towards them, would beneficial to both consumers and companies.

As such, we wanted to understand Americans' baseline preferences when presented with value propositions where a firm acquires personal information to enhance offerings or to operate the service. As noted above, companies often do not actually present the value proposition and allow consumers to make a choice based upon it. Rather, the data may be passively collected without input from the consumer, leaving companies with little information about reactions to the value proposition until the collection is discovered and consumers react either positively or negatively.

We asked Americans about two scenarios related to the mobile app privacy issues discussed above. First, we asked whether respondents would be willing to share contact list information on their phones with a social networking app so that the app provider could suggest more connections. This scenario tracked Facebook's use of phone contact lists. Second, we asked whether respondents would be willing to share contact list information with a coupons app they had already chosen to download so that it could also offer coupons to people included in the contacts list. This second scenario was based on existing or planned coupon apps that collect contact lists and let users share coupons with contacts.[32]

Both scenarios were chosen for three main reasons. First, they each reflected actual business practices related to contact information stored on mobile phones engaged in or planned by app providers. Second, they each provided a clear value proposition for the consumer to consider: 1) provide contacts

---

[31] Indeed, Facebook had previously updated its notice to make the Contact Sync feature explicit. *See e.g.*, Charles Arthur, *Is your private phone number on Facebook? Probably. And so are your friends'*, GUARDIAN.CO.UK TECHNOLOGY BLOG (Oct. 6, 2010), at http://www.guardian.co.uk/technology/blog/2010/oct/06/facebook-privacy-phone-numbers-upload.

[32] For recent examples, *see, e.g.*, The Coupons App, last accessed July 11, 2012, available at https://play.google.com/store/apps/details?id=thecouponsapp.coupon&feature=search_result#?t=W251bGwsMSwxLDEsInRoZWNvdXBvbnNhcHAuY291cG9uIl0 (see "Permissions" tab, showing that the app can read, and in some cases use, email contact information, calendar information, GPS, and the device phone number, among other information); QR Rewards, last accessed July 11, 2012, available at https://play.google.com/store/apps/details?id=com.fairybinary.qrrewards&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5mYWlyeWJpbmFyeS5xcnJld2FyZHMiXQ (see "Permissions" tab, showing that the app can read contact data, and can also access GPS, information about phone calls, browser history, among other information).

in order to receive more connection opportunities; 2) provide contacts in order for those contacts to also receive coupon benefits. Third, they did not suggest any further uses of the contact information outside of the stated value proposition. While we expect that businesses would sometimes be tempted to use the lists for other reasons—perhaps, for example, in constructing social graphs or other profiling information for advertising and marketing purposes—such additional reasons are not necessarily part of the value proposition, and we wanted to understand respondents' attitudes toward the basic benefit offered by the proposition.

We found that Americans overwhelmingly rejected both scenarios. Eighty-one percent of respondents said they would "definitely not allow" (51%) or "probably not allow" (30%) sharing contact lists in order to receive more connection suggestions. Fourteen percent stated that they would "probably allow" this use of their contact lists, and only 4% that they would "definitely allow" it.

Rejection of the coupons app collection of contact list information was even stronger. Fully 93% of respondents said they would "definitely not allow" or "probably not allow" the coupons app to collect contact list information in order to suggest coupons to contacts; of these respondents, 75% "definitely would not allow" it. Only 4% would "probably allow" the collection, and only 2% would "definitely allow" it.

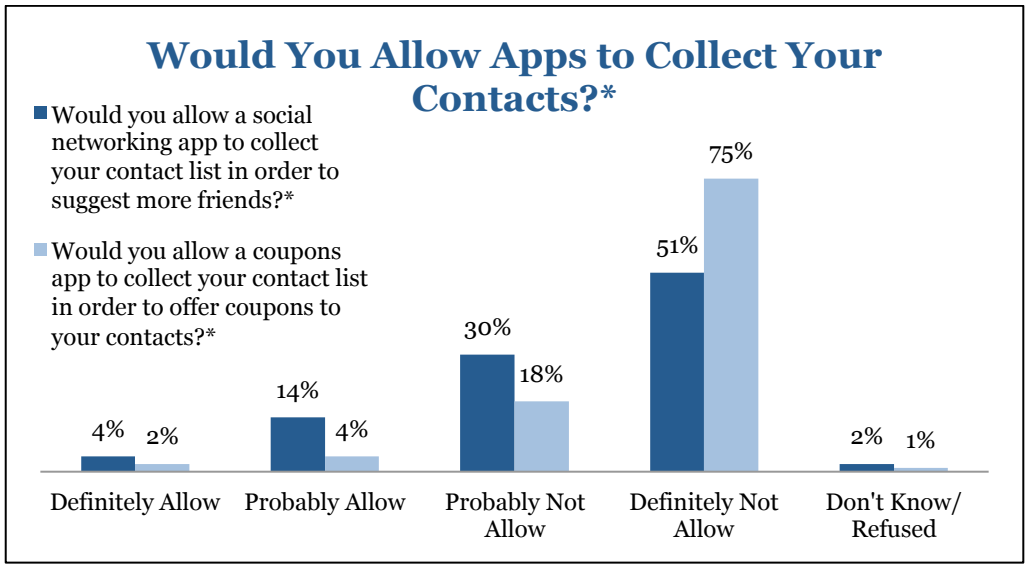

Figure 4: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margins of error are between 2.5 and 2.8 percentage points. *For actual wording, see Appendix 2: Survey Questions Q27 and Q28.

Given these results, it is perhaps unsurprising that the backlash against Path's collection was so strong. Had Facebook, Path, and other companies actually presented consumers with the value proposition and the choice to share contact lists or not, survey respondents say they would have rejected it.

Location tracking via mobile phones

One of the most attractive features of mobile phones for marketers, app providers, law enforcement, and consumers themselves is their location awareness. Among many other possible uses, location awareness can allow law enforcement to track suspected criminals or missing persons, app makers to provide tailored mapping and direction information to consumers, and marketers to make location-specific offers to consumers.

As briefly described above, the location of mobile phone users can be tracked using a variety of methods, including methods that do not require the knowledge of the mobile phone user. Additionally, highly accurate location data is routinely stored by telecommunications service providers.

We asked Americans about location tracking and storing location information collected from mobile phones. First, we asked how long wireless service providers should retain the location data they collect about wireless phones on their network. We offered the following choices: Less than a year; one to two years; two to five years; indefinitely; or not at all.

A plurality of respondents—46%—answered that wireless phone location data should not be kept at all (this option was offered to respondents after all the other periods of retention). The next largest group—28% of respondents—answered that the data should be kept less than a year. Significantly fewer respondents chose longer retention timeframes, with 9% choosing one to two years, 6% choosing two to five years, and 7% choosing indefinite retention.

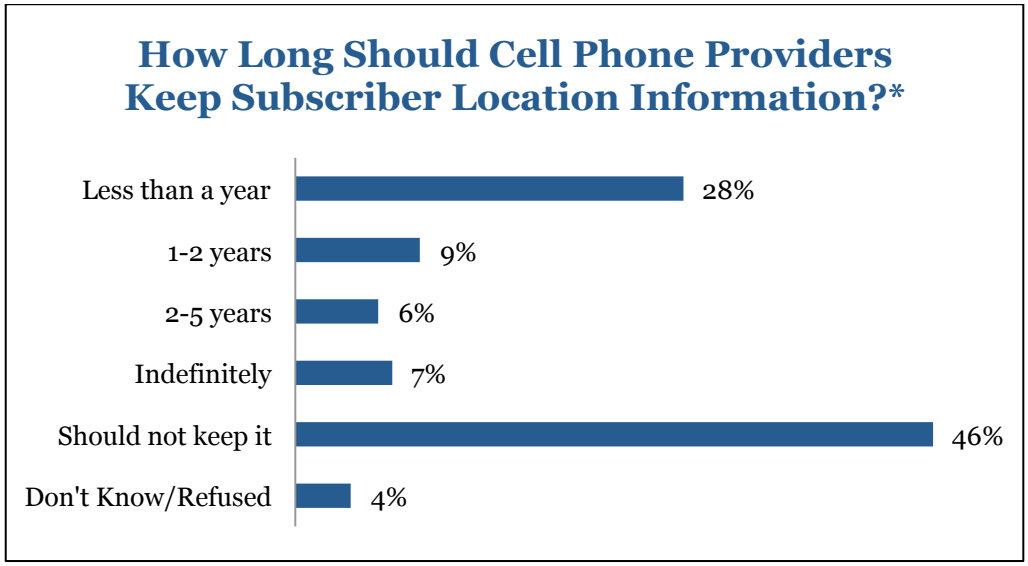

Figure 5: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margin of error is 2.8 percentage points. *For actual wording, see Appendix 2: Survey Question Q30.

Second, we asked respondents whether they would allow wireless service providers to use their locations to tailor advertising to them. This was overwhelmingly rejected. Overall, 92% of respondents said that they would "definitely" or "probably" not allow the use of location data for this purpose. (Seventy percent stated they "definitely" would not allow it, and 22% stated they would "probably" not allow it.) Only 7% would "probably allow" the use of location to tailor ads, and only 1% would "definitely" allow it.

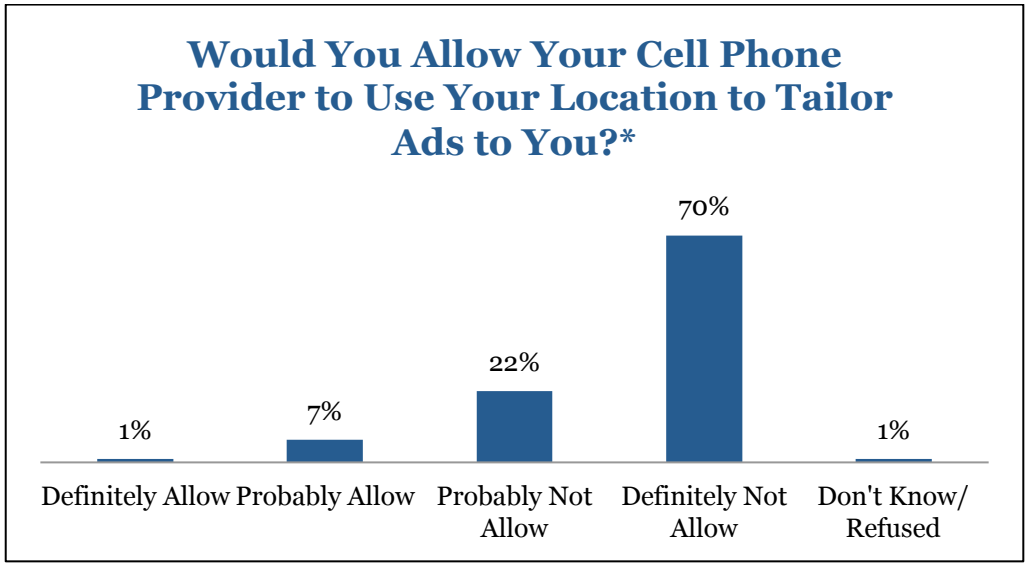

Figure 6: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margin of error is 2.7 percentage points. *For actual wording, see Appendix 2: Survey Question Q31.

Age and mobile privacy

Smartphone ownership

While all mobile phones can be tracked and all store sensitive information such as texts and contact lists, the enhanced capabilities of smartphones—especially web browsing, data collection, and sharing information via apps—create additional privacy risks. Smartphone use is growing,[33] as is the use of smartphones to access Internet resources,[34] geolocation services,[35] and app-based services[36]—all potentially privacy-sensitive activities.

---

[33] Aaron Smith, *Nearly half of American adults are smartphone owners*, *supra* note 5.
[34] Aaron Smith, *17% of cell phone owners do most of their online browsing on their phone*, *supra* note 8.
[35] Kathryn Zickuhr, *Three-quarters of smartphone owners use location-based services*, *supra* note 7.
[36] Kristen Purcell, *Half of adult cell phone owners have apps on their phones*, *supra* note 6.

We found significant age differences in the groups most likely to own and use smartphones. As might be expected, younger adults—those under 45 years old—are significantly more likely, as a group, to claim smartphone ownership than adults over 45. Members of the oldest cohort in our sample, adults 65 years and older, were significantly less likely to own smartphones than all other cohorts. And 78% of the second-youngest cohort, those 25-34, stated that they owned smartphones. This was significantly more than any other group, including 18-24 year olds (of whom 66% owned smartphones) and 34-44 year-olds (of whom 60% owned smartphones).

Smartphone Ownership Age Cohort	Mobile phone is a smartphone
18-24	66%*
25-34	78%**
35-44	60%*
45-54	44%
55-64	40%
65+	19%

Table 5: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margins of error are between 1 and 3 percentage points. *Represents significant difference compared with non-starred rows. **Represents significant difference compared with all other rows. For question wording, see Appendix 2: Survey Question Q18b.

Use of mobile phone features

Younger people—that is, people under 45 years old—are also significantly more likely to use their phones for visiting websites, social networking, texting, email, and games, an unsurprising result given their higher level of smartphone use.

When it comes to accessing websites via mobile phones, there is a clear age-related difference between people under 45 and 45 and older. Large majorities of each cohort under 45—71% of 18-24 year olds; 79% of 25-34 year olds; and 66% of 25-44 year olds—used their mobile phones to access websites. There are no significant differences between any of these younger age cohorts with regard to this question, but each of them is significantly more likely to access the web via phone than all cohorts 45 and older.

Similarly, there is a clear split between cohorts 45 and younger and those 45 and older when it comes to using mobile phones to access social networking services, with younger cohorts significantly more likely to use their mobile phones for this purpose. Further, there is a trend that tracks age, starting

with people aged 35 and older and continuing through age 65 and above—older cohorts become progressively less likely to use social networking services via mobile phones.

Some of the most direct communications records created by mobile phones are texts and emails. Unsurprisingly, younger cohorts are significantly more likely than older cohorts to use text messages. This holds for each progressively older age group except for the youngest two cohorts (18-24 vs. 25-34), for which the differences are not significant. That said, all groups except those 65 and older use text messaging at high levels: 71% of 55-64 year olds text, and the percentage increases with each younger cohort. Well over 90% of respondents under 45 text, and more than 99% of youngest two (18-24 and 25-34) groups use texts. As for email, younger cohorts 45 and below are significantly more likely than the cohorts 45 and older to use mobile phones for email.

Those 25-34, in addition to be being significantly more likely to own smartphones than other groups, are—at 57%—significantly more likely than other age cohorts to use their phones to play games. And as with smartphone ownership, people under 45 are significantly more likely to play games than those 45 and older.

It is also useful to note, however, that many of the information-rich features of mobile phones are heavily used by most or all age groups. In addition to sending and receiving text messages, every age group, for example, takes photographs or videos with their phones in substantial numbers. People aged 25-34 lead the pack, with an overwhelming 92% using phones for this purpose, but majorities of all groups other than those 65 and older also take photos or videos with their phones. And those 65 and older still commonly use their phones for this purpose—45% of the 65+ age cohort take videos of photos with their phones.

Privacy attitudes

The fact that younger cohorts are more likely to use smartphones, and are more likely to use phones for purposes like social networking and web browsing could indicate that they are more comfortable with the privacy risks of these uses, and could also indicate that they are more likely to be interested in the benefits offered in our coupon and contact list scenarios.[37]

However, this is not what we found. First, large majorities of all respondents consider data on their phones to be at least as private as data on home computers, and younger cohorts were no exception. Indeed, those under 45 were more likely than those over 45 to respond that data on phones was *more* private than data on home computers. Twenty percent of 35-44 year

[37] *See supra* pp. 15-18.

olds, 23% of 25-34 year-olds, and fully 30% of 18-24 year olds responded that data on phones was more private.[38]

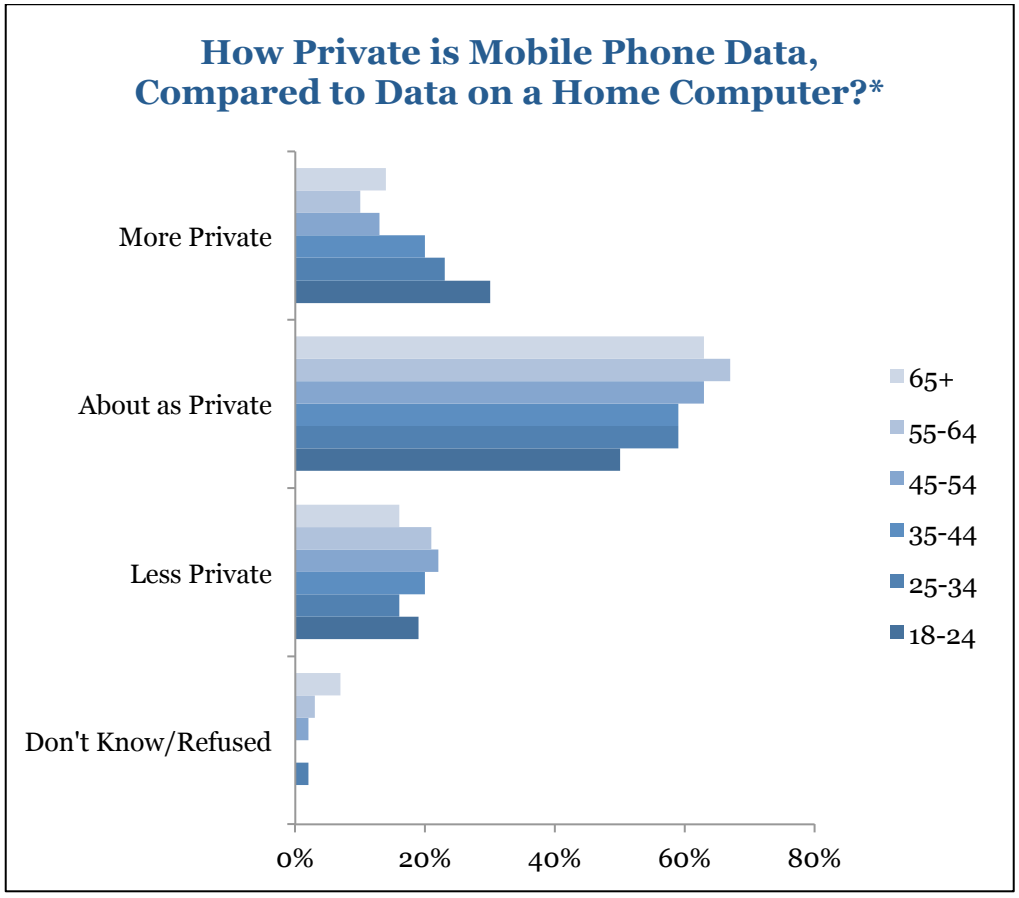

Figure 7: Based on cell phone owners (*n = 1119*). Results are weighted to account for known demographic discrepancies. Margins of error are between 1 and 2 percentage points. *For actual wording, see Appendix 2: Survey Question Q22.

Second, overwhelming majorities of all age groups rejected allowing a coupons app to use a phone contact list to offer coupons to people on that contact list. Over 90% of members of all age cohorts but 18-24 year olds rejected this proposition; 87% of 18-24 year olds rejected it.

[38] Our data does not tell us why this is the case. Younger cohorts may be more savvy to security and privacy risks, or more sensitive to privacy concerns about the data on their phones. For the youngest cohorts, it may be related to the likelihood of having another means of getting online—18-24 year olds, for example, may rely on their phones more than older cohorts because they are more likely to be limited to phones for Internet access. *See* Aaron Smith, "17% of cell phone owners do most of their online browsing on their phone," *supra* note 8. However, there were no significant differences among cohorts under 45 on this point, and our data does not provide evidence for these or other reasons.

One scenario was somewhat more likely to be accepted by younger cohorts: allowing a social networking app like Facebook to use contact list information in order to suggest more "friends." Those under 35 were significantly more likely to say that they would allow this than those 35 and older. However, younger cohorts still rejected the proposition in large majorities: 68% of 18-24 year olds stated that they would "definitely" or "probably" not allow the use, and 73% of 25-34 year olds stated the same.

Conclusion

The overall picture we developed from responses to this survey suggests that Americans both use a wide variety of mobile phone features and services that collect a rich set of personal information, and assign a strong privacy interest to that information. This includes the younger age cohorts who are most quickly adopting smartphones and their richest features.

At the same time, the market has produced few realistic, privacy-protective alternatives to the dominant, privacy-invasive online services. Greater transparency and consent requirements could help, but only if consumers can realistically make decisions that align more closely with their preferences for privacy than many of the value propositions available in the market today.

Under our current regulatory regime, firms can and do cram questionable demands for contact lists and other sensitive information in disclosures. This issue is exacerbated by the fact that providing meaningful, descriptive notices is genuinely difficult in most mobile environments.[39] Firms also sometimes condition rendition of service on disproportionate demands for personal data.

The gulf between private sector information demands and consumer preferences suggest that better disclosures and choice mechanisms alone will simply preserve the status quo. More aggressive interventions are necessary to create incentives for firms to reduce collection of personal information.

Particularly where privacy tradeoffs have not been made clear, consumers need the ability to change their minds and walk away from a service. While the Federal Trade Commission has so far focused upon improving consumers' positions ex ante, increasingly we need to consider ex post

---

[39] However, some researchers are developing models that build both meaningful notice and privacy-friendly decision-making possibilities into the mobile interface. *See, e.g.*, Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker & Jinghai Rao, *Understanding and capturing people's privacy policies in a mobile social networking application*, 13 PERSONAL AND UBIQUITOUS COMPUTING 401-412 (2008).

interventions, such as a right to delete information associated with an account, so that the consumer can exit whole.[40]

Among public sector actors, there is also a gulf between user expectations and the law governing access to information about wireless phone usage. While law enforcement officials make more requests for data each year, our respondents evinced strong support for substantial limitations on the retention of wireless phone usage data. This study shows that Americans support direct limits on law enforcement activities, as well. In particular, respondents thought that some prior court oversight is necessary when police seek to search a wireless phone when arresting an individual.

[40] Jan Whittington and Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 NORTH CAROLINA LAW REVIEW 1327 (2012), available at http://ssrn.com/abstract=2059154.

Appendix 1: Methods

The Berkeley Consumer Privacy Survey obtained telephone interviews with a nationally representative sample of 1,203 adult Internet users living in the continental United States. Telephone interviews were conducted by landline (678) and cell phone (525, including 235 without a landline phone). Overall, 6,906 working landlines and 8,688 working cell phones were dialed. The response rate for the landline samples was 16 percent. The response rate for the cellular samples was 14 percent. Statistical results were weighted to correct known demographic discrepancies.

The survey was conducted by Princeton Survey Research Associates International (PSRAI), and was fully funded by Nokia, Inc. as part of an unrestricted gift to the Berkeley Center for Law and Technology. The content of the survey was entirely composed by Berkeley Law's Chris Jay Hoofnagle & Jennifer M. Urban. Interviews were done in English by Princeton Data Source from January 27-February 12, 2012. Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is ± 3.4 percentage points.

Appendix 2: Survey questions

Note: Results are weighted to correct known demographic discrepancies.

TELEMARKETING

Q16 If you provide your wireless or cell phone number to a cashier, should the store be able to call you later to provide information about other products or services that the store offers?

24	Yes, they should be able to call
74	No, they should not call
3	Don't know/Refused

MOBILE DEMOGRAPHICS

Q18a Do you have a working cell phone?

91	Yes
9	No
*	Don't know/Refused

Q18b As you may know, some cell phones can now do things such as send and receive e-mail, access websites, display photos, and play videos. These cell phones are often called 'smartphones'. Is your cell phone a smartphone, or not, or are you not sure?

Based on cell phone owners (n=1119)

54	Yes, my cell phone is a smartphone
41	No, my cell phone is not a smartphone
4	Not sure/Don't know
*	Refused

Q 19 Which of the following best describes the type of cell phone you have? Is it an iPhone, a Blackberry, an Android phone, a Windows phone, a Palm, or something else?

Based on cell phone owners (n=1119)

24	Android
21	iPhone
12	(VOL.) Basic cell phone – unspecified
7	Blackberry
6	(VOL.) Samsung – unspecified
6	(VOL.) LG – unspecified
3	(VOL.) Flip phone – unspecified
2	Windows phone
2	Palm
2	(VOL.) Motorola – unspecified
2	(VOL.) Nokia – unspecified
2	(VOL.) Tracfone
1	(VOL.) HP Web OS – unspecified
1	(VOL.) Pantech – unspecified
*	(VOL.) Sidekick - unspecified
*	(VOL.) HTC – unspecified
6	(VOL.) Other (SPECIFY)
4	(DO NOT READ) Don't know/Refused

Q20 Now, thinking about your cell phone use, please tell me which of the following things you use your phone for. First/Next, (INSERT ITEM – READ AND RANDOMIZE)?

READ FOR FIRST ITEM, THEN AS NECESSARY: Do you use your phone for this, or not?

Based on cell phone owners (n=1119)

	Yes	No	DK/Ref
a. Making voice phone calls	89	11	*
b. Sending and receiving text messages	85	15	*
c. Sending and receiving email	52	48	*
d. Playing games, such as "Angry Birds"	35	65	*
e. Visiting any type of website	56	44	*
f. Using social networking services, such as Facebook or Twitter, Foursquare or others	42	57	*
g. Making purchases	20	80	*
h. Listening to music	41	59	*
i. Using location services, such as GPS and map services	46	54	*
j. Taking photographs or videos	75	25	*

Q21 Which of the following items, if any, is stored on your phone? First/Next, (INSERT ITEM – READ AND RANDOMIZE)?

READ FOR FIRST ITEM, THEN AS NECESSARY: Is this information stored on your phone, or not?

Based on cell phone owners (n=1119)

		Yes	No	DK/Ref
a.	Text messages	78	21	1
b.	Contact information (as in an address book)	82	17	*
c.	Email messages	48	51	1
d.	Voicemail messages	74	26	*
e.	Photos or videos	75	25	*
f.	Voice memos or notes	39	60	1
g.	Information about websites you have visited	37	60	3
h.	Passwords of websites you have visited or applications you have used	27	71	1
i.	Music	41	58	*
j.	Information about your present location or where you have been	24	70	6

MOBILE PRIVACY SUBSECTION

Q22 Please consider the types of information stored on your cell phone, such as text or email messages, or photographs. Do you consider this information to be MORE private, LESS private, or about as private as information stored on your home computer?

Based on cell phone owners (n=1119)

19 More private
19 Less private
59 About as private
2 Don't know/Refused

Q24 When a person is arrested on suspicion of committing a crime, a police officer searches through the person's possessions. The officer may search the person's cell phone by reading the text messages, photos, or seeing what calls were made. In your opinion, what procedures should officers have to follow when the person arrested does NOT consent to having their phone searched? Do you think (READ ANSWER CATEGORIES 1-2)?

76	Officers should have to get permission from a court prior to searching a phone, OR
22	Officers should be able to search the phone WITHOUT permission of a court
3	Don't know/Refused

Q24a Suppose the cell phone was protected by a password, should police have to get permission from a court before trying to guess the password and search the phone, or should they be able to try and guess the password and search the phone WITHOUT permission from a court?

78	Need permission from court
17	Don't need permission from court
5	Don't know/Refused

Q25 Imagine that someone needed to borrow a cell phone and use it for a few hours while they ran errands on their own. Would you lend your phone to: (READ AND ROTATE)?

READ FOR FIRST ITEM, THEN AS NECESSARY: Would you definitely allow, probably allow, probably NOT allow, or definitely NOT allow them to take your cell phone for a FEW HOURS?

Based on cell phone owners (n=1119)

		Definitely allow	Probably allow	Probably not allow	Definitely not allow	DK/Ref .
a.	A spouse or other close family member	51	33	7	9	*
b.	A close friend	26	29	18	28	*
c.	An acquaintance	4	11	25	59	1
d.	A work colleague	6	15	21	56	2
e.	A stranger	1	2	7	90	*

Q26 What is the MAIN reason why you would not allow others to borrow your phone? (RECORD OTHER SPECIFY – UP TO THREE RESPONSES. PROBE ONLY FOR CLARITY)

Based on those who would not let all named above borrow their phone (n=1105)

17	Privacy
12	Has a lot of personal information on it
10	They may damage/lose/steal it
10	Never know what they'll do with it/May abuse it/Takes away my control of the phone
8	Trust issue
7	It's mine/my phone/personal
6	Need phone at all times
5	Security
5	Don't really know them
4	Worried borrower would read emails or texts or look at pictures or contacts
2	I paid for it/I pay the bill
2	Borrower may use too many minutes/texts
2	Borrower may make charge calls/cause extra charges
2	They should have their own phone
2	Depends
2	Don't want to /just wouldn't/personal reasons/uncomfortable
3	Other
1	Don't know/Refused

Notes: Table reports first mention only. Only responses of 2% or greater are shown

Q27 Some social networking apps, such as Facebook, may collect the contact list information stored on your phone in order to suggest more connections/friends to you. Would you definitely allow, probably allow, probably NOT allow, or definitely NOT allow an app to do this?

Based on cell phone owners (n=1119)

4	Definitely allow
14	Probably allow
30	Probably not allow
51	Definitely not allow
2	Don't know/Refused

Q28 Now imagine that you just downloaded a coupons app. This app helps you find coupons when you are out shopping. The app can also send people listed in your phone's contact list coupons. In order to do so, this app needs to read your contacts list on your phone. Would you definitely allow, probably allow, probably not allow, or definitely not allow this coupons app to read your contacts list?

Based on cell phone owners (n=1119)

2	Definitely allow
4	Probably allow
18	Probably not allow
75	Definitely not allow
1	Don't know/Refused

LOCATION SUBSECTION

Q30 Cell phone service providers can track the location of all the cellphones on their networks. This location information is highly accurate and available even when the subscriber is NOT making a call.
How long should cellphone service providers keep information about subscribers' location? (READ ANSWER CATEGORIES 1-5)

Based on cell phone owners (n=1119)

28	Less than a year,
9	One to two years,
6	Two to five years,
7	Indefinitely
46	Or should they not be able to keep it?
4	Don't know/Refused

Q31 Some cell phone service providers are considering using information about subscribers' location in order to tailor advertisements to the subscriber. Would you definitely allow, probably allow, probably not allow, or definitely not allow your cellphone service provider to use information about your location to tailor advertisements to you?

Based on cell phone owners (n=1119)

1	Definitely allow
7	Probably allow
22	Probably not allow
70	Definitely not allow
1	Don't know/Refused