Study G-300 June 2, 2014

Memorandum 2014-23

State and Local Agency Access to Customer Information from Communication Service Providers: Report of Stanford Law & Public Policy Initiative

In 2013, the Legislature enacted Senate Concurrent Resolution 54 (Padilla), which directs the Commission[1] to make recommendations to revise the statutes that govern the access of state and local government agencies to customer information from communications service providers. The revisions are intended to do all of the following:

(1) Modernize the law.
(2) Protect customers' constitutional rights.
(3) Enable state and local agencies to protect public safety.
(4) Clarify procedures.

In 2013, the Stanford Law School expressed interest in assisting the Law Revision Commission with this study, as part of its new "Stanford Law and Public Policy Initiative."[2]

Stanford Law Professor Robert Weisberg supervised a team of Stanford Law students who worked to develop policy reports for the Commission's use. Some of those reports provide background information and analysis on governing law. Those reports will be helpful as the staff continues to work our way through those authorities.

The most recent report focuses on societal expectations of privacy and how they might vary by context. The report also considers how a statute addressing government access to communication information might be framed to avoid

1. Any California Law Revision Commission document referred to in this memorandum can be obtained from the Commission. Recent materials can be downloaded from the Commission's website (www.clrc.ca.gov). Other materials can be obtained by contacting the Commission's staff, through the website or otherwise.

The Commission welcomes written comments at any time during its study process. Any comments received will be a part of the public record and may be considered at a public meeting. However, comments that are received less than five business days prior to a Commission meeting may be presented without staff analysis.

2. See generally Minutes (Aug. 2013), p. 2.

obsolescence as communication technologies change. That report is attached for the Commission's consideration.

The students making contributions to the attached report are:

Elizabeth Berardi
Connie Dang
Sam Dippo
Gary Dyal
Sol Eppel
Farbod Faraji
Matthew Forbes
Ryan Nelson
Krisina Zuniga

The staff greatly appreciates the assistance provided by the Stanford Law School, its Public Policy Initiative, Professor Weisberg, and the students who have worked on this project.

Respectfully submitted,

Brian Hebert
Executive Director

MEMO TO THE CALIFORNIA LAW REVISION COMMISSION
FROM: STANFORD LAW SCHOOL "POLICY LAB"
(Research Practicum on State Law Enforcement
Access to Customer Records of Communication Companies)
June 2014

In this memo,[1] we address two important questions posed to us by the Commission in anticipation of its June meeting. (1) What is the current state of valuation of privacy of electronic stored or communicated data by citizens, and, as a corollary, is that valuation in a state of historical or generational flux? (2) Should any new legislation operate at a high level of generality so it can apply to varieties of technology current and not yet developed, or should it include or allow for elaboration of special rules to deal with new technologies?

In responding to these questions we draw on a variety of sources: Published research, policy documents of government and nongovernment institutions, and extensive personal interviews with experts in business, technology research, legal and policy advocacy, and academia. Because of the need for promptness in helping prepare for the June meeting, our responses are presented here in somewhat summary and informal style, generally without formal citation, although fuller documentation will be made available. We use a variety of simple graphics for emphasis, to enable quick reading.

PUBLIC VIEWS OF PRIVACY IN THE DIGITAL ERA

Voluminous research is available on public attitudes about privacy, and about how people view the proper balance among privacy, law enforcement, national security, business efficiency, and other values. A fair reading of this research generates these tentative conclusions:

Assessing "how much" Americans (or Californians) value privacy in the abstract has limited value. Obviously we value privacy but once the question is put in terms of reasonable limits on privacy, opinion quickly becomes very divided and highly dependent on the framing of the values or interests that are posed as counterbalances to privacy—most obviously anti-terrorism enforcement. Respondents (understandably) blur their views on what does violate the law and should be held to violate the law, and views on defining reasonable expectations of privacy are often tautologically contingent on perceptions of the current law and current private technology mechanisms protecting privacy.

Here are a few examples of recent polls, drawn from a vast library of recent surveys.[2]

- Dan Balz and Claudia Deane, *Differing Views on Terrorism*, Washington Post, January 11, 2006: In a telephone poll conducted on January 5-8, 2006 by the Washington Post and ABC News, 1,001 adults were asked, among other things, about their views on

[1] In a separate set of documents, to be delivered in early summer, we will be presenting a series of detailed research memos on the major legal and technological predicates for potential legislation in the area of protecting electronic private data.
[2] A fuller synthesis of these surveys appears at the end of this memo in Appendix 1

privacy rights and government surveillance measures. The authors report the following: "Americans overwhelmingly support aggressive government pursuit of terrorist threats, even if it may infringe on personal privacy, but they divide sharply along partisan lines over the legitimacy of President Bush's program of domestic eavesdropping without court authorization." The poll found that nearly two in three Americans believe that federal agencies involved in anti-terrorism activities are intruding on the personal privacy of their fellow citizens, but fewer than a third said such intrusions are unjustified. Those surveyed were more narrowly divided, however, over whether the federal government is doing enough to protect the rights of both citizens and terrorism suspects. Most Americans said they paid close attention to the controversy over Bush's domestic spying program, and a bare majority of those surveyed (51%) said it is an acceptable way to fight terrorism, while 47% said it is not. 44% were worried that the Bush administration would go too far in compromising constitutional rights in order to investigate terrorism. 32% placed a higher priority on the federal government respecting personal privacy than investigating possible terrorist threats, up 11% from 2003.

- Link:http://www.washingtonpost.com/wp-dyn/content/article/2006/01/10/AR2006011001192.html

- Anderson Robbins Research/Shaw & Company Research, Fox News Poll, *Boston Marathon Bombings*, April 16, 2013: A poll conducted by Fox News following the bombing in Boston last year showed little support for changes in the scope of government surveillance. According to Fox News, when asked "Would you be willing to give up some of your personal freedom in order to reduce the threat of terrorism?" for the first time since before 9/11, more said they would not (45%) as compared with those who said they would (43%), with 12% saying they didn't know.
- Link:http://www.foxnews.com/politics/interactive/2013/04/17/fox-news-poll-boston-marathon-bombings/

- Washington Post Poll, *Boston Marathon Bombings*, April 17-18, 2013: A Washington Post poll indicated that the public was more concerned (48%) that the government would go too far to investigate terrorism than that it would not go far enough (41%).
- Link: http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_20130418.html

Surveys and scholarly research reveal wide varieties and degrees of trust and faith in the privacy protection they receive from private companies.[3]

- Ponemon Institute, *2012 Most Trusted Companies for Privacy*, January 28, 2013: The Ponemon Institute has released the 2012 version of a report listing the companies that

[3] But consumer willingness to consent to collection and disclosure is heavily contingent on the way questions are framed. See To Opt-In or Opt-Out? It Depends on the Question, Communications of the ACM, February 2001. In this paper, researchers Steven Bellman, Eric Johnson, and Gerald Lohse argue that: "Using the right combination of question framing and default answer, an online organization can almost guarantee it will get the consent [for information collection] of nearly every visitor to its site." Further, they found that "...if marketers wanted most people to say 'yes' to their privacy policy, all they have to do is make 'yes' the response recorded if a consumer takes no action." They conclude: "Regulation that genuinely aims to promote consumer from privacy infringement should also stipulate the form of the question asking for a consumer's consent."

consumers trust the most with respect to the handling of their personal information and data. Out of 217 organizations rated in the most trusted companies list, American Express (AMEX) ranked as the most trusted. In general, consumers rated companies in the healthcare, consumer products, and banking industries higher than Internet and social media companies and non-profits (charities). 78% of respondents reported to perceive privacy and the protection of their personal information as very important or important to the overall trust equation. The report also found that "the importance of privacy has steadily trended upward over seven years." While most individuals say protecting the privacy of their personal information is very important, 63% of respondents admit to sharing their sensitive personal information with an organization they did not know or trust. 59% of respondents believe their privacy rights are diminished or undermined by disruptive technologies, such as social media, smart mobile devices and geo-tracking tools. 55% say their privacy has been diminished by virtue of perceived government intrusions. Only 35% of respondents believe they have control over their personal information, and this result has steadily trended downward over 7 years. The number one privacy-related concern expressed by 61% of respondents is identity, closely followed by an increase in government surveillance (56%). The rankings were generated from a final sample of 6,704 respondents. [4].

- Link: http://www.ponemon.org/local/upload/file/2012 MTC Report FINAL.pdf

- Business Week/Harris Poll, *A Growing Threat*, March 20, 2000: Poll found that concern is rising over privacy on the Internet, with a clear majority (57%) now favoring some sort of laws regulating how personal information is collected and used. Regulation may become essential to continued growth in e-commerce, since 41% of online shoppers say they are very concerned over the use of personal information, up from 31% two years ago. In addition, among people who go online but have not shopped there, 63% are very concerned. When asked how concerned they were that various forms of communication (telephone, U.S. mail, fax, or email through the Internet) might be read or overheard by some other person or organization without their knowledge or consent, security concerns were highest for email (28% very concerned, 33% somewhat concerned, 24% not very concerned, 13% not concerned at all) followed by telephone (19% very concerned, 30% somewhat concerned, 31% not very concerned, 20% not concerned at all). 40% of respondent said that a policy that explicitly guarantees the security of their personal information would strongly encourage them to use the Internet more in general, and 40% said it would somewhat encourage them to use the Internet more. 56% said that if privacy notices allowed you to "opt out," letting you choose not to have your personal

[4]One special concern of consumers is cloud computing. Pew Internet and American Life Project: Cloud Computing Raises Privacy Concerns. Pew, Sept. 12, 2008. The study indicates that "cloud computing" applications, such as web-based email and other web apps, are raising new privacy concerns.
-- 69% of online Americans use webmail services, store data online, or use software programs such as word processing applications whose functionality is located on the web.
--90% of respondents said that they "would be very concerned if the company at which their data were stored sold it to another party."
--80% say "they would be very concerned if companies used their photos or other data in marketing campaigns."
--68% of "users of at least one of the six cloud applications say they would be very concerned if companies who provided these services analyzed their information and then displayed ads to them based on their actions."

information collected by a particular website, they would always choose to opt out. Finally, 57% of respondents believed that the government should pass laws now for how personal information can be collected and used on the Internet. The survey was a telephone survey of 1,014 adults.

- Link: http://www.businessweek.com/2000/00_12/b3673010.htm

Some experts believe that the average person, if asked, pays rhetorical lip service to privacy but does not value it very much in any consequential way:

- Larry Ponemon, *Why Should I Care About Digital Privacy?*, March 10, 2011: As a result of many studies of consumer behavior, Larry Ponemon has concluded that people just don't care about privacy, no matter how much lip service they might give the topic. In short, Ponemon's research shows that most U.S. adults—60%—claim they care about privacy but will barely lift a finger in an effort to preserve it. They don't alter Facebook privacy settings, they don't complain when supermarkets demand their phone numbers, and they certainly don't insist on encrypted e-mail. "I think it's partly because people are part of a large herd, they take a 'the lion is not going to attach antelope' mentality," said Ponemon. "And people are more scared of physical dangers than privacy risks. When that whole issue about groping and scanning at the airport came up, we did a study and found that people were more worried about getting cancer from the machines, and weren't overly concerned about privacy. It shows me that people feel they can't live without social networking, and they have to go on flights. So they just surrender." Ponemon argues, that despite the lack of demand for more privacy coming from consumers, there are plenty of societal ills that need fixing which don't initially arrive with widespread public support.

Similar, though more moderate, is this view:

- Patricia A. Norberg, Daniel R. Horne, and David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, Summer 2007: Discusses what the authors term the "privacy paradox"—the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors. The authors explore a common phenomenon today where consumers voice concerns that their rights and ability to control their personal information in the marketplace are being violated, but still freely provide personal data. The authors conclude, "There must be the realization that, unless consumers make the effort to truly understand what they are granting permission to, and to whom they are giving their personal information, their sense of personal privacy will continue to deteriorate. Especially, as people expand their usage of data-rich transaction channels such as the Internet, the need to comprehend where the data go increases dramatically." Finally, the authors argue that "[e]nlisting consumers as the first line of defense to protect their own privacy" is the most efficient means to ease everyone's concerns with the data collection race.
- Link:http://onlinelibrary.wiley.com/store/10.1111/j.1745 6606.2006.00070.x/asset/j.17456606.2006.00070.x.pdf?v=1&t=hvqd0xiy&s=dd16793f0 bebc5a1dcfeff049ab777b990a63734

Consumers rely heavily on self-help personal control of apps or other mechanisms to prevent excessive collection or use of personal data by private companies. This trend is more evident among better-educated consumers and will likely increase generationally.

- Jan Lauren Boyles, Aaron Smith, and Mary Madden, *Privacy and Data Management on Mobile Devices*, September 5, 2012: A nationwide survey by the Pew Research Center of 2,254 adults found that the majority of mobile phone users have uninstalled or avoided apps due to privacy concerns. According to the report, 54% of mobile users have decided to not install an app after discovering the amount of information it collects, and 30% of mobile users uninstalled an app after discovering that it was collecting personal information that they didn't wish to share. One in five cell phone owners have turned off the location tracking feature on their phone, and one in three have cleared their cell phone browsing or search history. Owners of Android and iPhone devices are also equally likely to delete (or avoid entirely) cell phone apps due to concerns over their personal information. Younger cell phone users were also twice as likely as older users to report that "someone has accessed their phone in a way that felt like privacy invasion."
- Link: http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/

- Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, March 26, 2002: In this report, Gellman identifies many behaviors that individuals engage in to protect personal information. These include, subscribing to called ID services, purchasing unlisted phone numbers, and entering false information on web sites. Gellman argues that "the costs incurred by both business and individuals due to incomplete or insufficient privacy protections reach tens of billions of dollars every year."
- Link: http://epic.org/reports/dmfprivacy.html

- Mary Madden, *Privacy Management on Social Media Sites*, February 24, 2012: This survey by Pew found that users are becoming more active in managing their social media accounts. The poll found that a majority of social network site users (58%) restrict access to their profiles, and women are significantly more likely to choose private settings. The poll also found that social media users who are college graduates are significantly more likely than those with lower levels of education to say that they experience some difficulty in managing the privacy controls on their profiles. Finally, both young and old alike choose private settings for their profiles, according to the poll.
- Link:http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/

Harris Interactive Survey, May 2005 (Stephen Pounds, Americans increasing protections of privacy, personal information, Palm Beach Post, May 02, 2005). A Harris Interactive national poll of 1,962 employed people performed for Office Depot found:

--67% shred credit-card offers and their bills.

--25% do not sign the back of their credit card so sales clerks will check their identification.
--7% use only cash for purchases so there's no paper trail.

Nevertheless, consumers probably hugely overrate their understanding of how much privacy protection they have:

Joseph Turow, Lauren Feldman, and Kimberly Meltzer, Open to Exploitation: American Shoppers Online and Offline (PDF), Annenberg Public Policy Center of the University of Pennsylvania, June 1, 2005. In a national poll of 1,500 Internet-using adults, Annenberg Public Policy Center asked respondents 17 questions, demonstrating wide ignorance of business practices and the use of personal information:

-80% knew that companies have the ability to track Internet users on the web.
-62% knew that a company can tell when someone has opened an email, even if the recipient did not respond.
-47% believed falsely that online merchants give consumers the opportunity to see their own data.
-49% believed falsely that banks send their customers e-mails asking them to verify their account (this is a common practice of "phishers," scammers who are attempting to break into individuals' bank accounts by fooling people into revealing their password).
-50% believed falsely that online merchants allow consumers to erase their personal information from the company's coffers.
-49% believed falsely that online merchants are required to disclose the names of their affiliates before transferring personal information to them.
-52% believed falsely that magazines were barred by law from selling their subscription lists.
-62% believed falsely that the law protects consumers for being charged different prices for the same item.
-64% believed falsely that their supermarket is barred by law from selling customer data.
-34% could correctly name one of the "big three" consumer reporting agencies (they are Equifax, Experian, and Trans Union).
-68% believed falsely that price comparison web sites such as Expedia or Orbitz must include the lowest airline prices.
-72% believed falsely that charities are barred by law from selling personal information without permission.
-73% believed falsely that banks are barred by law from sharing information with other companies and affiliates.
-75% believed falsely that the presence of a privacy policy on a web site means that the company cannot sell customers' information to others.
-76% believed falsely that the Federal Trade Commission will correct errors in credit reports.

A popular notion is that younger people value privacy less than their elders (and perhaps will effect a generational reduction in expectation or valuation of privacy as they become the next generation of adults). But expert views on this issue are varied and divided.

The most prominent research on this issue is by Danah Boyd.

- *It's Complicated: The Social Lives of Networked Teens*, 2014: "Privacy doesn't just depend on agency; being able to achieve privacy is an expression *of* agency," writes Danah Boyd. In her book, Boyd argues that young people have more power and capacity than people might think and that teenagers' main weapon against privacy invasions is what she calls "social stenography." Boyd states, "Rather than finding privacy by controlling access to content, many teens are instead controlling access to meaning," by encoding and disguising the content they post on social media sites. Still, Boyd acknowledges that teenagers' power—especially the edge obtained by cyber-manipulating identity and privacy—has its limits.
- Link:http://www.danah.org/books/ItsComplicated.pdf; http://www.danah.org/papers/talks/2010/SXSW2010.html

Some key conclusions reached by Boyd:

--Teens express that just because they use the internet to connect to other people does not mean they are not concerned with privacy.

--While adults argue that a willingness to share in public spaces is incompatible with a desire for personal privacy, teens seek privacy in relation to those who hold power over them – thus, their parents, teachers and other immediate authority figures in their lives

--But teens are less concerned with the government and corporations.

--There has been a trend in the teen population to move to sites such as Twitter, Tumblr and Instagram over Facebook "because my parents don't know about it"

--For teens, achieving privacy is on-going because social situations are not static (because comments are visible for weeks or months, they can create problems long after they were written)\

--It is difficult to control privacy settings when the underlying affordances change regularly. For example, Facebook constantly alters its privacy settings, making privacy labor-intensive. Some teens can navigate this with ease, while others struggle because the focus is on access and control. But online, many social media sites encourage participants to spread information – making private conversations public.

--Especially because it is easier to share with all friends than manipulate privacy settings to limit the audience. This makes the evaluation backwards: instead of asking if the shared information is significant enough to broadcast publicly, teens ask if the information is intimate enough to require special protection.

--Another way teens use to control privacy: "social steganography" or encoding messages in plain sight. Thus even if control over the information itself is not possible, the meaning will not become accessible to unwanted viewers. Hence this is used as a way to navigate visibility.

But a skeptical view on any useful generational divide comes from Lee Tien, Senior Attorney with the Electronic Frontier Foundation:

> "The research I'm aware of is equivocal. I assume you're familiar with Danah Boyd's work? I think it's very dangerous to seek to adjust to a divide that is fairly hotly contested. Obviously, we're privacy advocates, so our view is predictable. It is usually industry or big data proponents that argues that the Facebook generation doesn't care about privacy. I have kids (now 17 and 22) and have watched them and their peers as social media has proliferated. I don't see them as caring less about privacy. I do see them as realizing as they approach adulthood that the things they say online can be used against them in ways they didn't when they were younger. I also see them slowly and dimly becoming more aware of the enormous market for personal information--but here they are like a lot of Americans, who don't understand data brokers, online tracking, the power of re-identification, etc."

A related view, more pessimistic than skeptical:

- Alessandro Acquisti, *Why Should I Care About Digital Privacy?*, March 10, 2011: Acquisti is seen as "sticking up" for consumers who might seem either too lazy or too disinterested to make changes to daily routines or Internet usage that might preserve their privacy. "On one end is attitude, and on the other is behavior, but in between there are many steps. It's not obvious what you should do to protect your privacy. And the more technology savvy among us have this feeling that we're giving it up, but we realize it is close to impossible to protect your personal information, not even if you start living like the Unabomber in a cabin. If you want to function as a normal person in society you have to." For many, he thinks, there is a sense of learned helplessness — the feeling that their privacy is lost anyway, so why go through the hassle of faking a supermarket loyalty card application? For others, the decision tree is so complex that it's no surprise they usually take the easier option. Acquisti thinks it's time that society erected some strict safety rules around privacy issues, and end the charade of 27-page end user license agreements that no one reads. The right answer for the majority of Americans who care about privacy but don't know what to do about it is for leaders to make some tough choices. "Participation in the public debate on privacy, put pressure on policymakers to provide some baseline protection for personal data," Acquisti says. "Technology can only do so much."
- Link: http://www.nbcnews.com/id/41995926/ns/technology_and_science/t/why-should-i-care-about-digital-privacy/ - .U4WY3K1dVMR

Thus while what people disclose obviously varies and is expanding and awareness of an ability to deploy self-help protection increases, it is not meaningful to say that people are coming to value privacy less than before (or more!). The contexts of social norms and

technology are so varied and mutually contingent that perceiving change in valuation in large abstract terms is not useful.[5]

A sensible conclusion from the above observations comes from Professor Daniel Solove:

- Daniel J. Solove, *Understanding Privacy*, March 2010: In this book, Daniel J. Solove provides a comprehensive overview of the difficulties involved in discussions of privacy and provides the following resolution: he argues that no single definition can be workable, but rather that there are multiple forms of privacy, related to one another by family resemblances. The key, he argues, is balancing. "Because privacy conflicts with other fundamental values, such as free speech, security, curiosity, and transparency, we should engage in a candid and direct analysis of why privacy interests are important and how they ought to be reconciled with other interests. . . . We determine the value of privacy when we seek to reconcile privacy with opposing interested in particular situations," Solove states. Thus, Solove provides a pragmatic, bottom-up approach to thinking about privacy, through which he supports enhancing and extending privacy rights relative to many other rights.

[5] As one related line of inquiry, our researchers interview some academic philosophers to glean the state of the intellectual terms of philosophical understandings of privacy . One striking, if contestable, inference is how little confidence there is among philosophers that a coherent conception of privacy is feasible--or useful.

For example, in his philosophical anthology on privacy, Ferdinand Schoeman describes the different theoretical approaches to privacy. Ferdinand David Schoeman, *Privacy: Philosophical Dimensions of the Literature*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand David Schoeman ed., 1984) Most immediately, Schoeman acknowledges that defining privacy and what it captures can be a divisive question. For example, privacy could be characterized as a right to control information about oneself. This conception seems to locate privacy in a person's personal power to disclose or withhold information. Alternatively, privacy could be viewed as a condition of limited access to a person. Put differently, under this theory privacy is more about third parties and their right to access information about the individual. Depending on which starting point one chooses, the paths to protecting privacy can look very different – and these two paths are only the beginning. Other fundamental questions include whether privacy is a basic right had by everyone or rather it is only a culturally created, and therefore relative interest that some societies value.

Under Judith Jarvis Thomson's view, there is no inherent right to privacy nor is there anything special about privacy. Judith Jarvis Thomson, *The Right to Privacy*, 4 PHILOSOPHY AND PUBLIC AFFAIRS 295–314 (1975). She argues that any privacy interest can be equally well explained by other interests or rights such as those relating to property or bodily security. Thomson also believes that there is little agreement on what privacy is. She argues that privacy is ultimately a cluster of rights, a cluster of rights that always intersect with or include rights to property and bodily security. In this sense, privacy does not have intrinsic value but are derivative of other rights. Thus, any violation of a privacy right is truly a violation of a more basic right.

Evgeny Morozov, taking a more critical view of the inherent value of privacy, argues that "privacy is not an end in itself but "a means of achieving a certain ideal of democratic politics, where citizens are trusted to be more than just self-contented suppliers of information to all-seeing and all-optimizing technocrats." Evgeny Morozov, *The Real Privacy Problem*, MIT Technology Review (Oct. 22, 2013), He warns that too little privacy can endanger democracy, but so too can too much privacy. In striking this appropriate balance of protection, Morozov believes that laws and market mechanisms are insufficient solutions to the privacy problem. Rather, Morozov calls for a civic or political solution where privacy protections are structured to serve great democratic ideals.

PREFRRED GOALS OF A NEW STATUTE

The clear consensus is that legislation should be at a general and "durable" level, not elaborated to account differently for particular technologies:

We interviewed John Grant, the "Lead" for Privacy and Civil Liberties team at Palantir, probably the nation's most important purveyor of data-mining software –to both government (including the CIA) and business (including the nation's largest banks and health care enterprises). We asked him: If the government's going to require extra process to data people share with third parties, how should the government decide what requires extra process? If law enforcement requests a certain *amount* of data? If law enforcement requests a certain *type or kind* of data? Do you think that expectations should vary with the context (e.g., by type of communication)?

> "I think we should look more at the use of the data as opposed to the type / amount."
>
> Whether I send you postal mail, email, talk on the phone, send you a text.... the format isn't important and neither is the possibility of covert surveillance.
>
> To me the issue is the intent of the communicants, gauged against their expectations in light of knowledge and law (that's not particularly precise, I know). If a friend and I go into a closed room to have a private conversation, it shouldn't matter that the room is bugged. If we speak on the phone, it shouldn't matter that we know the NSA does a lot of surveillance. The law (e.g. the Wiretap Act) establishes that the phone company isn't a party to our conversation and that the government isn't supposed to listen without following legal process.
>
> Much of the complexity here has to do with available precautions (I can't easily encrypt phone calls) and reliance on the law."

Another interviewee was Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation (specializing in free speech law, including intersections with intellectual property law and privacy law).

> "You would want to paint with a broad brush so as to ensure that you don't over-specify. Some may argue that location information is not communication records, but there is some uncertainty there. SCA has been clear that location information counts in their definition. If it's geo-locating your phone when you're not actually using it, it's a more difficult question. I worry about trying to divide up communications, recipe for more obsoleting the statute."
>
> Whether communication is "voice" or "text" or "video" or "electronic" doesn't seem to me to be very important to the level of privacy protection. My doctor might

communicate with my wife about her pregnancy, abortion, cancer, or contraception in any of these modes.

What matters is whether unauthorized/unintended access to it is a threat to her privacy. Or, from a government access perspective, whether we want cops or officials to go to a judge to get a warrant or other predicated order.

Note that the technical aspects of such communications *do* matter in terms of understanding the privacy threat model. The government often goes to the communication service provider, right? So it matters what that provider either normally does (e.g. Google holds your Gmail and thus can read it, transfer it, etc.) or could do (e.g. if a provider encrypts text messages, it matters whether it has the key or not)."

We asked similar questions of Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society.

?The legislature's goal should draft a durable statute that will not quickly become obsolete as communication technology advances. This will probably require a technology-neutral drafting approach that focuses on the different functional types of communication, rather than the technology used to effect communication (e.g., "voice communication," rather than "cell phones"). In addition to being more durable, this categorical approach would also allow the statute to group like things together for similar treatment. For example, if it makes sense to afford the same privacy protection to landline telephones, cellphones, and VOIP, then they could all be lumped together as "voice communication" and governed by a common rule. If it makes sense to extend the same treatment to video (e.g., skype), then the category could be broadened to "audio and video communications."

In general, Granick thinks we should focus more on updating the current scheme than on developing entirely new categorizations of communication types. From her perspective, this is purely pragmatic – we should go along with what we already have and know, rather than creating a new set of unknowns:

"I'm not sure I understand your approach or that it is in fact technology neutral. It seems like you have at least three categories voice, audio, and video. So far. What about still imagery, or computer simulated voices, or my voice augmented with a computer (autotune, anyone?). Or things that have all of those, like video games. What about electronic smells?

And then are you going to have other categories like metadata, transactional data, calling records?

Currently the law divides communications into three (or four) categories that depended on transmission (wire, electronic, radio and other). I don't see that the three categories I know about are as comprehensive, or that even given current technology they are durable or tech neutral.

Maybe it would help to ask what about the current scheme is outdated, or about to become outdated? What novel transmission technologies will fall outside of the wire, electronic, and radio categories?"

Granick also sees value in having state law use a similar scheme as federal law, but provide more protection. She had three main sets of recommendations for improving federal law that could be applied to improving the state law:

(1) Get rid of the ECS and RCS distinctions. Instead, apply the same standard to everything.

(2) Get rid of the content v. non-content distinction. Have the default standard be that everything requires a warrant, but bite off the low hanging fruit of what is clearly not content (e.g. subscriber info) and specify that these pieces of information get less protection. Right now, a big problem is that there are no clear lines to be able to define content and non-content, and so privacy is not adequately protected. A better label going forward might be sensitive v. non-sensitive, and the law should just assume that everything is sensitive unless it has specifically delineated a particular piece of information as non-sensitive.

(3) Have a clear and different standard for law enforcement to collect information for targeted purposes v. collecting in bulk. There should be different standards for when law enforcement is gathering information about one person than when it is gathering information about everyone. There should be a heightened standard when law enforcement is gathering information about many people.

From interviews with Nicole Ozer, Technology & Civil Liberties Policy Director, Chris Conley: Technology and Civil Liberties Staff Attorney, ACLU of Northern California"

"We supported and failed Leno bill requiring warrants for content. We think that if the government wants to get access, you need a warrant. That is what we push for. You don't need to make distinctions based on types of communication; you don't need to do that.

One is a question who has access? Are you going through an intermediary or not? Both oriented around the question of forms and communication are the same, is there is a service provider involved.

We have looked at location privacy bill (is that part of the scope here?). Location is a great example of the kind of records that end up incidentally getting swept up (but not incidentally, it's intrinsic to a certain form of communication); anything that tries to locate mobile device will end up getting location or allow location to be inferred.

"All classifications pose problems, ECPA made sense then, but is arcane now…it is an arbitrary decision most of the time. The concern with trying to write the

law based on certain classifications is that in the future the differences between something like audio and video may be very blurry. Soon it may not be that much different, and something new will come and this sets up a situation where courts will try to compare old and new categories (and it won't make sense to force them into this comparison).

Focus should be communication or any information transmitted, not kind-of-source or whether it is audio or whatever classification. The law should be the focused on the transmission of information, not what medium or type of communication or who the sender or receiver of information is.

We will likely see new intermediaries, new forms of communication. A lot of laws that regulate the Internet don't work anymore.

We are hesitant about breaking things into categories, that is a bad idea because ultimately the categories are too similar (or will become similar).

The more categories, the more you have to define, but have to define it in a way that is not over-inclusive and that it is different. It is really, really difficult to do.

This has been our experience with ECPA and state stuff –write in a tech neutral way, and the buckets are really hard to define or keep separate."

But even if the law properly eschews differential tretament of forms of technology, there is the separate and more difficult question of post-acquisition restrictions on use.

This is obviously an elaborate set of legal and technological; issues, but we think it work noting some comments from our interview with John Grant of Palantir:

- Yes. "You can [or should be able to] only use data for the use it was collected"
- "It should be for what people expect"
- "I don't expect it to market a profile" about who I am
- "The problem is how do you prevent it [the secondary, post-acquisition use]"
- You can design limits, but "it's really hard" to enforce those limits
- "You've got to look at the outcomes"
- It's easier for the private sector to impose limits because in government there's always an exigency exception and the exceptions always gobble up the rule.
- Or you could impose extra process on the acquisition on any data that could be used to derive personal information.
- At a certain number of data points, information becomes more accurate and revealing.
- Podesta report: Benefits of big data are big, and they outweigh the harms, so don't impose limits on secondary uses.
- Paul Ohm: "You could actually tax the amount of data" companies hold. "It would make the private sector really think about, 'Do I really need this [amount of data]?'"

- "We've thought about increasing the amount of access depending on the severity of the crime. Robbery maybe you can get a week [of location data], a murder maybe you get two years."
- A book called *The Leak*: A perfect digital memory is counter to how we've evolved as a species. "It's skewing how we think of things." "If you have a fight via email" then you re-read it even years later, you get mad again, while in the old days you may have forgotten about the fight.
- We're trying out a tool where "older data is faded, newer data is more opaque," to emphasize that old data is less meaningful.
- You've got to "think about outcomes" instead of what the data itself represents.
- Government should require extra process so that "you can't derive really non-obvious things from data." So if you're looking at where a car drives, you can't use that for proving whether someone's HIV positive, or has cancer, or is gay, unless you go through extra process. Then "there's still something in that reasonable expectation of privacy standard."

The clear consensus (explicit and implicit) of civil liberties-minded experts is that the most important form of protection is the requirement of judicial warrant. As noted in some detail below (and then summarized further below), faith in the power of the warrant process however over-confident or even naïve, so pervades these discussions, and the simplicity and flexible adaptability of the concept of the warrant itself has great valence if legislation is to work at a general and durable level.

Our sources for this consensus (interviews, legal advocacy statements, draft legislation, academic comment) are widespread and heterogeneous, and not easily documented (in part because much of it is indeed implicit--but very clear). But here is the gist. The reasons may lie in deep belief in the Framers' commitment to a warrant requirement (and of course a probable cause requirement) or faith in the independent judgment inherent in a judicial check on the other branches, or belief that the ideal model of a statutory privacy protection is Title III on wiretaps. Bu whatever the cause, almost all experts and advocates call for more protection for data gathering or use not currently regulated at all now, or at most regulated by subpoena rules, through the traditional warrant. Whatever the relevant form of data or communication, and however and wherever the warrant process needs to be inserted into law enforcement investigations, warrants are the way to go. Hence the call is for warrants in areas ranging from searches of cell phones incident to arrest, to, at the other extreme, drastic alteration of the federal ECPA and new ECPA-style state legislation that would eliminate the time-period difference that allows for some access to stored email data solely by subpoena.

Caution is required here, because warrants are no panacea. This was the concern raised by some of the Justices in the recent oral argument in *Riley v. California* (the cellphone search case about to be decided by the Supreme Court), where the defense-side lawyers were pressed on whether they placed too much faith in the warrant solution and whether and how they might be calling for an augmented and more elaborate warrant process for Smartphone data. The concern has also arisen in an area currently covered only by the Fourth Amendment, and not

statute – the conventional search of computer hard-drives. See Judge Kozinski's remarkable opinion in *United States v. Comprehensive Drug Testing*, Inc., 579 F.3d 989 (9th Cir. 2009).

We close here with a more detailed summary of overall recommendations about possible legislation. This summary is gleaned by our researchers from interviews with numerous law and technology experts (including the ones cited above) but most notably gleaned from discussions with Jonathan Mayer, a lawyer/computer scientist serving as Scholar at the Stanford Center for Internet and Society:

These ideas represent for us the most thoughtful and fully elaborated observations on what the Legislature needs to attend to in this area. These ideas are far more complex than the straightforward notion that statute law should require a warrant for across-the-board forms of data collection and use. We offer them as a stimulant to commission and legislative deliberation:

1--The Legislature needs to determine answers to certain empirical questions.

2--Second, there are a few relatively easy changes the Legislature could make based on various gaps and inadequacies in current state and federal statutes.

3--There are more complex solutions, technological change is, according to Mayer, unlikely to dramatically alter the basic nature of the problem the Legislature is seeking to address.

Where more information is needed: in order for the Legislature to make informed decisions about the law, we believe that it must thoroughly collect the following information.

- How do California agencies currently use existing law?
    - What are the factual circumstances that make up >90% of requests for information under ECPA and California Criminal Procedure in California law enforcement agencies? What types of records do they involve? At what stage of the investigation is this information sought?
    - How many requests are denied by electronic service providers and on what grounds?
    - How often is a gag order requested preventing electronic service providers from providing notice to the target of investigations? How often is notice ultimately provided?

- What new technologies does law enforcement currently have (e.g., surveillance cameras, drones)?

- What technologies and capabilities is law enforcement seeking to develop (e.g., bulk metadata collection and analysis)?

Immediately implementable fixes: Due to the outdated nature of current state and federal statutes in this area, the Legislature has an opportunity to implement some concrete fixes to existing law.

- Change procedural steps
    - Require law enforcement or service providers to give notice to customers
    - Increase the judiciary's knowledge of technology and of the data requests they are approving

        - Create a resource of best practices for interchambers consistency in responding to requests under the statute.
        - In the legislative history and in guidance to judges, include descriptions about these kinds of requests in both technical and non-technical terms.

- Implement an ECPA-like statute governing access to electronic records that forgoes increasingly irrelevant distinctions present in ECPA and other states' statutes.
-
    - The 180-day threshold that eliminates the warrant requirement for data in long-term storage is nonsensical and should not be adopted.

        - This dichotomy appears to be based, among other things, on outdated assumption that little information is stored for long periods of time (due to previously high storage costs).
        - Enormous amount of personal data now in long-term storage makes access to stored content more intrusive than access to real-time communications.

    - Content vs. metadata: The legislature could clarify what is content and noncontent. We believe that the following contested categories of content should be explicitly considered "content" under the statute, and require a warrant.
    -

        - Subject lines of emails
        - URLs and browsing history
        - Location data
        - Search queries
        - Note that the more specific the legislature is about these above issues, the harder it is for the statute to seem "evergreen" and adaptable to changing circumstances.
        - Alternatively, the legislature could eliminate the distinction between content and noncontent information altogether (see discussion below)?

Longer-term thoughts: California has an opportunity to be forward-thinking with this new law by creating a new paradigm for thinking about the tradeoff between privacy and the needs of law enforcement.

- Based on our interview with Jonathan Mayer, we infer that the legislature need not worry too much about technologies that are on the horizon.

- Foreseeable changes in technology (i.e. self driving cars and wearable devices) do not require changes to the underlying legal analysis.
-
    - New technology may generate new content and user data, and much of this will be stored with third party service providers. But the underlying question is the same: how should we balance the needs of law enforcement with the desire for privacy?
    - These new, foreseeable technologies utilize the Internet, and how governments deal with privacy on the Internet is the knotty legal question that must be answered.

- Still, the legislature could create a transparent administrative body (or a judicial one, such as the U.S. Sentencing Commission) that tracks new consumer and law enforcement technologies and recommends changes to the Legislature.
-

- The legislature could consider replacing the current content/noncontent distinction with a new standard governing both access *and* use that more appropriately responds to the reality that third party providers are now storing levels of "noncontent" metadata not contemplated by previous regulations. Current laws largely govern access only. But the question of use is equally important, particularly given the susceptibility of metadata to increasingly advanced analytical capabilities. For example, the collection of a week's worth of phone records is less revealing than the collection of five years' worth of phone records subject to data mining. The focus in this example thus should be not just on *what* is collected, but also on *how much* is collected and *how it is being used*. In this vein, consider Justice Alito's concurring opinion in *United States v. Jones*, where he suggests that the collection of large amounts of personal data may violate the Fourth Amendment while the collection of smaller amounts of that very same data might not. 132 S. Ct. 945, 964 (Alito, J., concurring); *see also id.* at 954-57 (Sotomayor, J., concurring) (making a nearly identical point).

-
    - The principle behind the content/noncontent distinction is that the former is so revealing that it should be protected, while the latter is not. But the distinction no longer serves this principle. Thus, instead of asking whether the data law enforcement seeks to access is content or noncontent as a proxy for determining the data's impact on privacy, courts could use the following two-part standard:
    -
      (1) How revealing (of personal information) would the collection be? How revealing would certain uses be? (2) What showing must the government therefore make to get that information?
    -
        - Rendering operative the first part (how revealing access/use is) would likely end up being a Breyerian multifactor test that might include the following nonexclusive list of factors (none of which would be dispositive):

- The extent to which the collection or proffered use would reasonably reveal associations, thoughts, beliefs, habits, medical information, financial information, and the like.
- The extent to which collection/use would be as revealing as "content" is assumed to be (to account for Fourth Amendment case law).
- The amount of data being requested and the time period it covers.
- Whether such information is typically shared with or visible to third parties (other than the service provider) and, if so, the extent to which individuals believe that it will remain private with the third party.
- The extent to which individuals seek to protect the information (including whether individuals generally use passwords for the information).
- The extent to which a reasonable user is or should be aware of the use to which third parties put his/her information. Note that merely because something is in the user agreement does not mean that a reasonable user is or should be aware of it.
- The identity of the third party (e.g., a health insurance company vs. a social networking site).
- If applicable, the target's subjective intention in sharing the information with a third party, including the number of individuals the information was shared with (the more people it was shared with, the less private it is); whether the target asked the third party(ies) to keep it confidential; the reason the information was shared, and so on. This factor makes sense because publicly posting sensitive medical information on Facebook probably means the police don't need an order to get it, but merely revealing information to another should not automatically render it unprotectable.
- The target's own efforts at keeping the information secure. This should not be dispositive, however, since technology users have different understandings of how technology works and how to secure information, and inquiring into each user's state of mind on these issues could be overly complicated.
- Though not directly related to how revealing the information would be, courts could also consider the extent to which users can opt out of revealing information to or storing information with a service provider, both as a technical matter and as a social/economic one (e.g., a modern person can't really opt out of having an e-mail account).
- Note that other factors may be relevant; we can further discuss this if it is something that you think would be valuable..

■ Rendering operative of the second part of the standard would be easier.

The more revealing the access/use of information is, the greater showing the government would need to make to access or use the information in a certain way.

- This could be treated as a single, continuous standard where the showing required is positively correlated with the risk to privacy.
- Or, it could be treated as a standard with discrete categories: access/use that poses little to no risk to privacy requires merely a subpoena based on relevance; access/use that poses a medium risk requires reasonable articulable suspicion; and access/use that poses a high risk (e.g., a risk akin to the revelation of "content") requires a probable cause warrant. Where specific information is bucketed in this scheme could be determined by the Legislature, but the courts would likely be the ones responsible for incorporating technological advancements into this scheme.

- This test would work as follows: law enforcement would say what it wants and how it will use it; the judge would determine how revealing the information is and what standard applies; law enforcement would try to meet that standard; and if it does the judge would issue an order (possibly with access or use restrictions).

- Note that vague standards (such as the one above) can permit courts to act flexibly when novel challenges arise, but it may also encouraged inconsistent rulings and rulings that are based on an insufficient understanding of technology and privacy. Thus, an administrative body that tracks new technologies and gathers statistics on these cases would help the Legislature assess the impact of a vague standard.

Final Note: A further consensus is privacy protection depends on both government and service providers. that consumers must – and (to some extent safely can) rely on the companies to exercise independent resistance to government demands:

Says John Grant of Palantir, asked. "Is the best approach to limit the government or limit the companies?"

> "You have to do both (companies and government). In practice, you can't have a one-sided approach, you have to make it unlawful for any private entity to voluntarily disclose to the government. You also have to limit the government's ability to get the information, maybe something like: "the government may neither demand or receive…"
>
> The provider thing, I am really torn about. Currently federal law and privacy law interpret the question of whether someone is a regulated private entity by asking what type of duty does the law require of the company. For example UC Berkeley is a public university, but since it doesn't really hold stuff out to "the public" it can't be regulated in the same way. This is the issue with entity-defined rule. Things change,

provider types and services, and we have to ask what assumptions are being made these entities.

The SCA's approach is to stop unauthorized access, but then make exceptions (Wiretap Act) (at least for content).

Got to build the walls up on both sides, and they have to match up pretty closely. Any time you don't do that, someone is probably trying to build a loophole. Even in the SCA, there are some loopholes that allow for disclosures by the provider (and the problem is that there is no reporting on it). That is a problem.

You really have to think, especially in light of metadata, there is not reason to make a categorical distinction between content and metadata. The value of metadata is so great that it doesn't make sense to distinguish it and content. We need to get the legislature to accept this. If you're worried about a law that will stand up over time, if its not facing very forward on records, on metadata, on location, it will obsolete very quickly.

Approach idea: warrant requirement for records and content (really simple) and then think about situations where you might need an exception, but the general approach would be to require a warrant. And I think the less you pay homage to third party records doctrine, the better you are."

And Grant fends off one optimistic speculation: Asked, "Will technology progress to the point where users will be able to protect their own civil liberties to the extent that added government process won't be necessary?." he responds"

- "I definitely disagree." We don't say, "If you flip on Palantir, it protects privacy and civil liberties." We say, "Palantir can protect policy that protects privacy and civil liberties." Someone has to set the "audit logs" and the "policies."
- Technology gives "building blocks" to policymakers, but you have to have the policy. And funding.
- "I was glad to see the PCAST and Podesta report"
- We need two decision makers, on top of the technology: "NSA encrypts the data, but the FISC has the encryption key"
- Private entities are forcing increased privacy protection through data sharing agreements. "If private company A shares information with private company B, A is liable for B's misuse of the information." Companies are taking more in sharing data."

But there is some reason for optimism about private sector protection:

- **Craig Timberg, *Apple, Facebook, Others Defy Authorities, Notify Users of Secret Data Demands*, Washington Post May 1, 2014**: "Major U.S. technology companies have largely ended the practice of quietly complying with investigators' demands for e-mail records and other online data, saying that users have a right to know in advance where

their information is targeted for government seizure." The authors argue that propelling the shift is the industry's eagerness to distance itself from the government after last year's disclosures about the NSA surveillance of online services. Companies that already routinely notify users have found that investigators often drop data demands to avoid having suspects learn of inquiries. Note, however, that the changing tech company policies do not affect data requests approved by the Foreign Intelligence Surveillance Court, which are automatically kept secret by law. Companies such as Apple, Facebook, and Microsoft are all moving toward more routinely notifying users, the article reports, where they had not previously disclosed these changes to users. Post-Snowden, companies have grown determined to show that they prize their relationships with customers more than those with authorities. Most now refuse to disclose the contents of e-mails or social media posts when presented with subpoenas, insisting that the government instead seek search warrants, which are issued only by judges and require the stricter legal standard of probable cause.

- Link: http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html?hpid=z1

- **Electronic Frontier Foundation, *Who Has Your Back? Protecting Your Data from Government Requests*, 2014**: The Electronic Frontier Foundation's 2014 findings saw major improvements in industry standards for informing users about government data requests, publishing transparency reports, and fighting for the user in Congress. For the first time in four year of putting together the report, all 26 of the companies earned credit in at least one category. The study also saw two companies make "enormous improvements" over the past year: Apple and Yahoo. The report concluded, "This has been a watershed year for companies taking a stand for user privacy, with more companies than ever publishing transparency reports and law enforcement guides, and publicly opposing mass surveillance. But there is still room for growth."
- Link: https://www.eff.org/who-has-your-back-government-data-requests-2014 - results-summary

APPENDIX I – DETAILED SUMAMRY OF POLLS AND SURVEYS ON PRIVACY

Mobile Phone Searches by Police

(1) Rasmussen Reports, Warrantless Mobile Phone Searches by Police

a. A poll conducted in early **May 2014** (shortly after oral arguments were heard by the U.S. Supreme Court on whether police must obtain a search warrant to search data on a cell phone incident to arrest) found that only 24% of American adults believe that police should be allowed to search the contents of an individual's cell phone without a warrant
b. 67% disagree and do not believe police should be able to search cell phones without a warrant
c. Poll: May 8-9, 2014, 1,000 adults
d. http://www.rasmussenreports.com/public_content/lifestyle/general_lifestyle/may_2014/24_support_warrantless_mobile_phone_searches_by_police

Government Surveillance Programs

(1) Pew Research/USA Today poll, NSA program (Government Surveillance)

a. A **January 2014** poll showed that ore Americans now oppose the NSA surveillance program, as opposed to an earlier poll in June 2013
b. 45% feel that Snowden's disclosures on the NSA spying program have helped the public interest, while 43% feel that it has harmed the public interest
c. 70% of Americans believe they should not have to give up privacy and freedom in order to be safe from terrorism (versus 26% who feel they do)
    i. There is some suggestion that the more time that passes since 9/11, the less freedoms the public seems willing to give up
d. Poll: January 15-19, 2014, 1,504 adults
e. http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/

(2) Gallup Poll, Government Surveillance Programs

a. A poll conducted in **June 2013** (shortly after the Edward Snowden revelations detailing the NSA spying program) found that 53% of adults disapprove of the federal government obtaining records from U.S. telephone and internet companies in order to compile call logs and communications without a warrant
b. 37% agree with the program, while 10% had no opinion
c. The poll found a partisan divide – with 49% of Democrats approving of the program versus 34% of Independents and 32% of Republicans
d. By contrast, 40% of Democrats disapproved of the program versus 56% of Independents and 63% of Republicans
e. 21% disapprove of the program, but said there could be circumstances when it would be okay for the government to carry out this program
    i. Creates a combined total of 58% of Americans who approve or approve under some circumstances
f. Of those who approve (37%):

i. 11% believe the program does not violate liberties
ii. 23% believe that terrorism is more important than privacy
iii. 4% expressed no reason

g. Of those who disapprove (53%):
   i. 21% said there are some circumstances when the program should be allowed
   ii. 30% said that there were no circumstances when it would ever be okay
   iii. 2% expressed no reason
h. The poll concluded that American views were similar to a 2006 Gallup poll that measured support for a government program that obtained records of the three largest U.S. telephone companies in order to create a database of the phone numbers dialed by Americans
   i. However, the partisan divide was flipped, with more Republicans supporting the program than Democrats
   ii. This suggests that partisan support for the incumbent President is likely to reflect the opinions within each group
i. Gallup also provided statistics for two other surveys conducted in June 2013 (Pew – discussed below – and CBS News)
   i. The wording of each poll may account for the difference in statistics
   ii. Gallup notes that if you account for the 58% that approve of the program or think that it could be okay in some instances, this aligns with the results in the Pew survey**(see below)
j. 35% "very concerned" about violation of their privacy rights – when asked whether they were concerned with the federal government having computerized logs of telephone calls or Internet communications stored in a database that it uses to track terrorist activity
   i. 25% are somewhat concerned
   ii. 21% are not too concerned
   iii. 21% are not concerned at all
   iv. 1% had no opinion
k. **"Implications:** Results from the Gallup poll indicate that Americans have somewhat flexible views about the government's surveillance program and/or that they are still forming their opinions on the issue. A majority of Americans say that they might find the type of government surveillance program that has come to light in recent days as acceptable under some circumstances, but less than half say they approve of the program as it stands."
   i. "The reactions to these types of government programs have remained constant over the past seven years, although Republicans and Democrats have essentially flipped their attitudes over that time period, reflecting the change from Republican President George W. Bush to Democratic President Barack Obama."
l. Poll: June 10-11, 2013, 1008 adults surveyed
m. http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx

(3) Pew Research/Washington Post Poll, NSA Phone Tracking (Government Surveillance)

a. A **June 2013** poll regarding whether the NSA's program tracking telephone records is an acceptable way for the government to investigate terrorism found that 56% supported the program
b. 41% said that the program was no acceptable
c. 2% expressed no opinion
d. The public is more evenly divided over the government's monitoring of email and other online activities to prevent possible terrorism
    i. 45% said the government should be able to monitor everyone's email
    ii. 52% said that should not be able to do so
    iii. 3% expressed no opinion
    iv. The poll found that views are largely unchanged since 2002, shortly after the 9/11 attacks
        1. Where 45% supported monitoring email, 47% were against it, and 8% expressed no view
e. The survey concluded that the NSA revelations did not alter fundamental public views about the tradeoff between investigating possible terrorism and protecting personal privacy
f. 62% believe that it is more important for the federal government to investigate possible terrorists threats, even if it intrudes on personal privacy (versus 34% felt privacy was more important)
    i. These numbers are similar to polls conducted in January 2006 (65% said it was more important) and November 2010 (68% said it was more important)
g. The poll only found marginal partisan differences
    i. 69% of Democrats said investigating possible terrorism was more important
    ii. 62% of Republicans felt the same
    iii. 59% of Independents felt the same
h. The poll did find a more significant divide by age
    i. 60% of older age groups (30-49, 50-64, 65+) support investigating terrorism even if it intrudes on privacy versus 51% of the younger age groups (18-29) feel the same way
        1. While the poll found that younger groups are against intrusions in general, when asked specifically about the NSA program and monitoring emails, their responses were aligned with the other age groups, suggesting that while they differ on the principle, in practice, they have similar views as older generations
i. The poll also found a partisan divide over the support for the Bush administration's surveillance program versus Obama's surveillance program, although the overall support of either program is the same
    i. 56% said the NSA program was acceptable
        1. 56% of Republicans said it was acceptable (41% said it was not)
        2. 64% of Democrats said it was acceptable (47% said it was not)
        3. 53% of Independents said it was acceptable (44% said it was not)
    ii. 51% supported Bush's program
        1. 75% of Republicans said it was acceptable (23% said it was not)

2. 37% of Democrats said it was acceptable (61% said it was not)
3. 44% of Independents said it was acceptable (55% said it was not)

j. The public is divided over internet monitoring in order to prevent possible terrorism (including monitoring emails)
   i. 45% said that the government should be able to monitor emails
   ii. 52% said they should not
   iii. The results are very similar to a July 2002 survey (45% supported monitoring emails, 47% were against it)
   iv. Partisan divide is much less significant (although it still exists) and, like the last question, the divide has flip-flopped based on the president-in-power's political party
k. Also of interest – the survey found that approximately a quarter were following government surveillance news stories very closely, with another 21% following it fairly closely
   i. 17% said they are not following too closely and 35% said not closely at all
   ii. This suggests that less than half of Americans are following these privacy issues closely in the news, with a significant gap by age, with the older groups following the reports much more closely than younger groups
   iii. Also, those who disagree with the programs are more likely to follow the stories "very closely"
l. Poll: June 6-9, 2013, 1,004 adults
m. http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

** The two surveys listed above (Gallup/Pew) were conducted within days of each other and shortly following the Edward Snowden revelations regarding the NSA surveillance program. The polls seemed to have contradictory outcomes, with the Pew poll showing "broad support" for the program, while the Gallup survey found more disapproval than approval. An article by the Pew Research Center attempts to account for the differences by suggesting that the way that questions are worded can produce different responses in those polled.

- In **July 2013**, one month after the first two surveys, it conducted a "question wording experiment" (with 2,002 adults):
- Survey respondents were asked if they would favor or oppose a government data collection program, but the wording of four elements of the program were described differently to different groups. These were:
  - (1) Whether metadata or content is being collected
  - (2) Whether phone calls or emails are being monitored
  - (3) Whether the program had court approval
  - (4) Whether the program is part of anti-terrorism efforts
- The last two ((3) and (4)) had a substantial effect on public sentiment
  - "Court approval" had 12 points higher support than when it was not mentioned
  - "Anti-terrorism efforts" had a 9% increase in support than when this was not mentioned as the goal
  - "Phone calls/emails" had the least support
    - But there was no difference in phone calls OR emails

- *Conclusions*: mentioning court approval or anti-terrorism goal increased support, but in every scenario (16 possible combinations), more respondents opposed than favored the program
- It suggests that how a survey is phrased can have a significant impact on the outcome of the results
- http://www.people-press.org/2013/07/26/government-surveillance-a-question-wording-experiment/

(4) A **May 2013** article describes the FBI's plan for a sweeping overhaul of surveillance laws that would make it easier to wiretap people who communicate using the Internet rather than traditional phone services (in response to the "going dark" problem whereby suspected criminals are no longer using traditional communication methods, making wiretaps often inefficient)

a. Would implement a legal mandate requiring companies like Facebook/Google to build into IM systems a capacity to comply with court wiretap orders
b. The proposal was met with concern by those worried it would stifle innovation in Silicon Valley
c. A revised proposal would fine companies who do not comply rather than require all companies to build a wiretap capacity and would expand the Communications Assistance for Law Enforcement Act of 1994 (CALEA)
    i. As of right now, a company must show that it tried to comply with the court order, but can show that they could not make the technology work
    ii. Instead, the proposal would be able to fine companies for not complying, after notice has been given and the company has had a chance to attempt to work out any technical problems
d. Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y. TIMES (May 7, 2013), http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?pagewanted=all&_r=1&.

(5) Rasmussen Reports survey, FBI Wiretap Proposal

a. In response to the above FBI proposal, Rasmussen Reports conducted a telephone survey regarding the proposal in **May 2013**
b. 17% of Americans favor making it easier for the FBI to wiretap Internet communications such as IM, Facebook chats and email
c. 67% oppose granting easier access to these types of communications
d. 15% are undecided
e. Survey: May 22-23, 2013 of 1,000 adults
f. http://www.rasmussenreports.com/public_content/lifestyle/general_lifestyle/may_2013/17_favor_making_fbi_wiretapping_of_internet_communications_easier

Privacy versus Terrorism – following the Boston Marathon bombing in April 2013:

(1) Fox News poll, conducted **April 16, 2013** (619 registered voters)

a. Most of the questions focused on terrorism (whether the public was concerned about future attacks) and the Boston Marathon bombing (whether the public had confidence that authorities would locate those responsible for the attacks)

b. One question asked whether the respondents would be willing to give up some personal freedom in order to reduce the threat of terrorism
    i. 43% said yes
    ii. 45% said no
    iii. 12% did not know
c. The results varied by partisan, age, gender, and income
    i. Partisan:
        1. Democrats: 51% said yes, 36% said no
        2. Republicans: 43% said yes, 47% said no
        3. Independents: 20% said yes, 58% said no
    ii. Gender:
        1. Men: 36% said yes, 55% said no
        2. Women: 49% said yes, 36% said no
    iii. Age:
        1. Under 35: 38% said yes, 51% said no
        2. 35-54: 40% said yes, 46% said no
        3. 55+: 49% said yes, 41% said no
        4. 65+: 51% said yes, 37% said no
    iv. Income:
        1. Under $50K: 40% said yes, 50% said no
        2. $50K+: 49% said yes, 41% said no
d. These results were slightly lower than past trends:
    i. May 2006: 54% said yes, 36% said no
    ii. Jan. 2006: 61% said yes, 27% said no
    iii. Jul. 2005: 64% said yes, 21% said no
    iv. Sept. 2002: 61% said yes, 24% said no
    v. June 2002: 64% said yes, 21% said no
    vi. Oct. 2001: 71% said yes, 20% said no
    vii. May 2001: 33% said yes, 40% said no
    viii. Aug. 1996: 60% said yes, 30% said no
e. This poll was significant as it was the first time since 9/11 that more said no than yes
f. http://www.foxnews.com/politics/interactive/2013/04/17/fox-news-poll-boston-marathon-bombings/

(2) Washington Post Poll, **April 17-18, 2013**, 588 adults by phone (following the Boston Marathon bombing)
a. In addition to questions relating to respondent interest in and reactions to the bombing, it also asked what worries them more: that the President will not go far enough to investigate terrorism (b/c of constitutional concerns) or that he will go to far (comprising constitutional rights)?
    i. 41% said not far enough, 48% said will go too far
    ii. Compare to previous polls:
        1. Jan. 2010: 63% said not far enough, 27% said will go too far
        2. Jan. 2006: 48% said not far enough, 44% said will go too far
b. http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_20130418.html

Cell Phone Internet/App Use, Social Media and Privacy

(1) An article dated **May 23, 2014**, states that Facebook and other social media sites are considering the implications of sharing and privacy concerns
   a. On Thursday, Facebook announced that it would give a "privacy checkup" to all of its users to show them what and to whom they share
   b. Social media sites are worried that users will share less if they believe their information is not private
   c. This is based in part on recent surveys which show that 9 in 10 internet users have taken steps online to remove or mask their digital footprints
      i. Survey of 1,002 adults by the Pew Research Center in July 2013
   d. Facebook's privacy concerns seem to highlight that privacy is "not an all or nothing issue for users…they want to be able to adjust the dials"
   e. http://finance.yahoo.com/news/privacy-please-facebook-under-pressure-130215204.html

(2) Pew Research Survey, Privacy and Data Management on Mobile Devices
   a. September 2012
   b. 88% of adults use cell phones of some kind; 43% of these download apps on their phones (versus 31% in 2011)
   c. Found that nearly 1/5 (17%) of cell owners use their cell phone for most of their online browsing
   d. Focus on app privacy policies – concern prompted the survey to see how cell phone users manage their personal mobile information
   e. 43% of cell owners download apps on their cell phone
      i. Of this group, 54% of app users have decided to not install a cell phone app when they discovered how much personal information they would need to share in order to use it
      ii. 30% of app users have uninstalled an app that was already on their cell phone because they learned it was collecting personal information that they did not wish to share
      iii. In total, 57% of all app users have either uninstalled or declined to install an app over privacy concerns
      iv. Men are more likely than women to uninstall an app but they are equally likely to avoid an app
      v. App users with some college education are more likely than those with only a high school education to choose to not install an app over privacy concerns
      vi. Younger owners are more likely than older owners to use apps; yet all age groups are equally likely to remove or avoid an app based on privacy concerns
      vii. There is no difference among iPhone and Android users
   f. Personal data management by cell phone users:
      i. 41% back up photos, contacts and other files in case their phone is lost or broken
      ii. 32% have cleared their browsing history or search history of their phone

iii. 19% have turned off location tracking feature on their cell phone because they were concerned that other individuals or companies could have access to that information

g. 12% of cell owners say they have had another person access their phone's content in a way that made them feel that their privacy had been invaded
   i. Among ages 18-24%, this figure rose to 24%
   ii. It was not clear "who" the person who access the phone was – if it was a friend, stranger, or law enforcement

h. Smartphone owners are more likely to engage in data management
   i. 59% back up their phone's content
   ii. 50% have cleared the search/browsing history
      1. Age correlates to this behavior, with 44% of 18-24 users having cleared their history, 36% of 45-54, but this number drops to 17% for those between 55-64 (and 11% for those 65+)
      2. Male owners are more likely to clear history than females (37% versus 28%)
   iii. 30% have turned off location tracking features
      1. Also age correlates to this as well – 32% of owners in their mid-20s to mid-30s have turned off this feature, while just 4% of those 65+ have done so
   iv. Twice as likely as other cell owners to have someone else access their phone in a way that made them feel their privacy was invaded
      1. This is highest in the younger age groups (24% for 18-24) and declines steadily among age groups (to 2% in 65+)

i. Survey: March 15-April 3, 2012, 2,254 adults

(3) Pew Research, Cell Internet Use **Spring 2012**

a. 17% of cell phone users do most of their online browsing on their phone rather than a computer or other device
   i. This is of 88% of adults who own cell phones, and of the
   ii. 55% use their phone to go online (up from 31% who used their phone to go online in April 2009 – this had steadily increased every year since 2009)

b. 31% of cell internet users mostly go online using their cell phone
   i. Which equals 17% of all adult cell owners

c. Young adults and non-whites are more likely to use their cell phone for the majority of their online activity
   i. 45% of 18-29 year olds
   ii. 51% of African-Americans (versus 24% for whites and 42% of Latinos)

d. Reasons:
   i. Cell phones are convenient – 64%
   ii. Cell phones better fit people's usage habits – 18%
      1. 6% say a cell is easier than a traditional computer
   iii. Cell phones fill access gaps – 10%
      1. Do not have access to a computer or internet access beyond their computer

e. Survey: March 15-April 3, 2012, 2,254 adults

(4) Pew Research Center, What Strategies do you use to protect your online identity?

a. July 2013

b. Found that 86% of internet users have taken steps online to remove or mask their digital footprints

c. 55% of internet users have taken steps to avoid observation by specific people, organizations, or the government

d. Steps taken:

i. Cleared cookies and browser history – 64%
ii. Deleted/edited something you posted in the past – 41%
iii. Set your browser to disable or turn off cookies – 41%
iv. Not used a website because it asked for your real name – 36%
v. Used temporary username/email address – 26%
vi. Post comments without revealing who you are – 25%
vii. Asked someone to remove something posted about you – 21%
viii. Tried to mask your identity – 18%
ix. Used a public computer to browse anonymously – 18%
x. Used a fake name/untraceable username – 18%
xi. Encrypted your communications – 14%
xii. Used service that allows you to browse the web anonymously – 14%
xiii. Given inaccurate info about yourself – 13%

e. Poll conducted: July 11-14, 2013

f. http://www.pewresearch.org/fact-tank/2013/09/05/what-strategies-do-you-use-to-protect-your-online-identity/

(5) Pew Research, Americans Increasingly View the Internet, Cellphones as Essential

a. February 2014

b. The survey asked Americans about six different communication technologies:

i. Internet
ii. Cell phones
iii. Television
iv. Email
v. Landlines
vi. Social media

c. 53% of internet users say it would be "very hard to give up"

i. 61% within this group said the internet was "essential" to them, either for work or other reasons
ii. Thus, 39% of all Americans feel they absolutely need to have access to the internet

d. 49% of cell phone owners said it would be "very hard to give up"

e. By contrast, there is a declining attachment to TVs and landline telephones (with 35% and 28% of those owners saying it would be "very hard to give up")

f. Only 11% said it would be "very hard to give up" social media

g. http://www.pewresearch.org/fact-tank/2014/02/27/americans-increasingly-view-the-internet-cellphones-as-essential/

Teens and Privacy:

(1) Pew Research, Teens and Mobile Apps Privacy

a. **July 26-Sept. 30, 2012** (802 teens) – survey
b. February 2013 (24 focus groups, 156 participants) – focus groups
c. Ages 12-17 – 78% of teens have a cell phone, 23% have a tablet computer, 82% own at least one
    i. 71% of teens that have one of the devices have downloaded an app
    ii. 58% of all teens have downloaded apps to a cell phone or tablet computer
    iii. Teens are more likely to download apps that are free than paid apps
d. 51% of teens avoid using certain apps due to privacy concerns
e. 26% of teen app users have uninstalled an app because they found out it was collecting personal information that they did not wish to share
f. 46% of teen app users have turned off location tracking features on their cell phone or in an app because they are worried about the privacy of their information
    i. Girls are more likely than boys to disable location-tracking features (59% versus 37%)
    ii. Focus group participants understood that the apps can access various data, such as location, contacts, pictures
    iii. Many limit location services unless it is necessary for the app itself (like Google Maps)
    iv. Other focus group participants expressed little concern with apps collecting their information, often because they already shared pictures and messages anyway
g. http://www.pewinternet.org/2013/08/22/teens-and-mobile-apps-privacy/

(2) Pew Research, Where Teens Seek Online Privacy

a. Ages 12-17
b. Day-to-day, teens state that they figure out sharing and settings on their own – by walking through the app or platform when they sign up, or by searching for their preferred platform
c. 70% have sought outside advice about how to manage some aspect of their privacy online at some point
    i. 42% ask friends or peers
    ii. 41% have talked to a parent
    iii. 37% have asked a sibling or cousin
d. Girls are more likely than boys to ask for help
e. Facebook users generally set their profile to either fully or partially private
    i. Those who seek advice are more likely to limit what certain groups can see versus letting all of their friends see the same thing
f. Study: July 26 – Sept. 20, 2012, 802 teens – survey
    i. Focus group – February 2013 (156 participants)
g. http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/