In an era of social networks, online databases, and cloud computing, more and more individuals’ personal information is available online and elsewhere. The ease of communicating information in the digital age has changed the way we live, learn, work, and govern. But such instant access to information also presents new challenges to our personal privacy. We depend more and more on evolving technologies and social norms that encourage the disclosure of personal information. What are our expectations for privacy in the digital realm? Is it reasonable to expect that information by and about us remain private? Who do I trust to protect my privacy?

This national conversation on privacy will give people with different perspectives an opportunity to learn more about the issues, weigh in on choices with fellow citizens, and consider options for action. Deliberative forums provide an opportunity for the public to have a voice on critical issues by weighing different approaches and considering costs, consequences, and tradeoffs. Trained moderators help participants listen to and understand the experiences and views of others and seek common ground for addressing this difficult problem. America’s libraries invite our communities to join this conversation about the tough privacy choices facing our nation.

Librarians around the United States developed this issue framework. They asked people to express their concerns about privacy. The specific concerns were wide-ranging, but for most people a common thread was uncertainty about how to go about protecting their privacy. They are uncertain about who to turn to and how to know what actions are effective. Thus, we ask: “Who do I trust to protect my privacy?”

Possible answers to this question clumped into three broad choices: the marketplace, the government, or my self.
The marketplace is the source of innovation in security and privacy protection technology and it also has a vested interest in privacy that secures the integrity of financial data.

The government has a responsibility to provide for public safety which includes identity protection and to secure the rights necessary to a free society.

I, my self, recognize that privacy values are individual and varied and that no one cares more about my needs than me.

Each of these approaches has strengths and weaknesses and requires trade-offs among differing values. Deliberating on them can help to clarify the common ground on which we can make public policies that impact privacy.

This issue framing is a joint project of the Intellectual Freedom Round Table and the Fostering Civic Engagement Member Interest Group of the American Library Association. We thank Texas Forums for hosting the project wiki at http://privacyframing.wetpaint.com/. The project implements a resolution adopted by the Council of the American Library Association on Wednesday, June 28, 2006. The resolution states:

That the Intellectual Freedom Committee, Intellectual Freedom Round Table, and ALA Fostering Civic Engagement Member Interest Group collaborate with other ALA units toward a national conversation about privacy as an American value.

For more information about privacy, see www.privacyrevolution.org
The issue framework on pages 5-6 is designed to stimulate public deliberation, which is a way of making decisions together that is different from discussion or debate. The purpose of deliberative forums is to inform collective action. As citizens, we have to make decisions together before we can act together, whether with other citizens or through legislative bodies. Acting together is essential for addressing problems that can’t be solved by one group of people or one institution. These problems have more than one cause and therefore have to be met by a number of mutually reinforcing initiatives with broad public participation. This framework is about such a problem.

Problems of this sort are difficult to solve because there is a difference between what is happening and what we think should be happening – but there is no agreement about what should be done. Expert information alone can’t answer these questions; they require people to exercise their best judgment. Public deliberation helps citizens make sound judgments and take collective action together.

We make sound judgments by weighing the likely consequences of various options for action against all that we hold dear. That is deliberation. Issue frameworks identify what is most valuable in each option. The guides also present the tensions that arise among options because of the differences in the things people value. This framework sets the stage for people to sort out and then work through the tensions – not to reach total agreement but to identify a common direction or way to act on a problem. A more complete understanding of the nature of the problem (and what people will and won’t do to solve it) often emerges from public deliberation. This shared understanding and sense of direction are prerequisites to effective problem solving.

Deliberation helps people make the difference they would like to make in our democracy. They integrate individual voices into a more reflective and shared, though not uniform, public voice. Community organizations, professional associations, and legislative bodies benefit from hearing
how citizens go about making up their minds when they confront the always difficult trade-offs that have to be made on every issue.

Forum sponsors include, but are not limited to, civic, service, and religious organizations, as well as libraries, high schools, and colleges. The forums are nonpartisan and do not advocate a particular solution to any issue, nor should their results be confused with referenda or public-opinion polls. (Text adapted from the National Issues Forums, Public Deliberation Statement, http://www.nifi.org/news/news_detail.aspx?progID=&workID=7773&catID=7773&itemID=8172)

Acknowledgements

This issue framework is based on the expressed concerns and ideas of citizens from around the United States who discussed the complex privacy issues that can affect people everywhere. The framework for discussion and deliberation will be used in communities—in public forums, in classrooms, in discussions broadcast on television and radio, and in exchanges in all print media.

The framing team that put together this guide was composed of librarians across the country. They conducted numerous interviews, test forums and other forms of public listening, in order to capture the way that citizens want to talk about privacy.

Members of the framing team are non-partisan and are committed to engaging the public in authentic ways that are genuine, honest attempts at open dialogue.

Contributing editors of the issue guide were Carolyn Caywood and Nancy Kranich.

Copyright 2010, American Library Association, 50 E. Huron Street, Chicago, IL 60611
Who do I trust to

#3: Issue Map

What concerns people about privacy?

When asked about their privacy concerns, people responded that privacy is a right necessary to human dignity and individual integrity – a right they consider personal and individual. They often judge privacy within a family and especially between parent and child differently.

Many commented on the gossip culture that pervades media and affects our concept of privacy. Others expressed fear that partial and misinformation will result in them being misjudged. Several people revealed that they use new technologies to learn more about others to protect themselves. At the same time, they recognize that these same new technologies heighten their awareness of privacy implications.

Some say privacy is a lost cause because we no longer know how to protect it. Others question, “What are you trying to hide?” A number were willing to trade privacy for convenience and convenience for security. Still others believe that privacy is connected to financial security, health care, and employment prospects. Those who want government to protect their privacy often do not trust the government’s intentions or its ability to foil hackers. Though they invoke public safety and national security in opposition to privacy, many recognize security as necessary to protect privacy.

Approach 1: the marketplace

The marketplace is the source of innovation in security and privacy protection technology and it also has a vested interest in privacy that secures the integrity of financial data.

Actions to Implement

• Purchase security measures
• Use spending to reward business that respects privacy
• Use public opinion, boycott against intrusive business
• Adopt and distribute strong company privacy policies and procedures

Supporters Would Say

• Innovates to protect privacy
• Keeps up with new threats
• Is motivated to please customers
• ID theft threatens profits

Opponents Would Say

• Targeted marketing is invasive
• Data mining is profitable
• Susceptible to government pressure
• Public has limited leverage

Tradeoffs

• Savings through targeted sales
• Escalating security expense
Approach 2: the government

The government has a responsibility to provide for public safety which includes identity protection and to secure the rights necessary to a free society.

Actions to Implement
- Set up an office like Canada
- Use courts to enforce checks/balances
- Enact comprehensive legislation that protects privacy
- Publicize existing privacy laws and regulations

Supporters Would Say
- HIPAA, library, financial, and other confidentiality laws protect privacy
- Privacy implied in First Amendment
- Protecting rights is a government role
- Clarifies public value for public servants

Opponents Would Say
- No universal definition of what’s private
- Susceptible to demagoguery
- Cannot keep up with changing threats
- Always tempted by secrecy

Tradeoffs
- Public safety & national security
- Complex bureaucratic rules

Approach 3: my self

I, my self, recognize that privacy values are individual and varied and that no one cares more about my needs than me.

Actions to Implement
- Monitor personal credit, stay informed
- Join privacy organizations to demand transparent processes
- Pay cash, avoid EZ-Pass
- Opt out of participating in data collection when possible

Supporters Would Say
- “Who will watch the watchers?”
- Privacy desires vary among individuals
- Individual carelessness is main threat
- I’m the only one who can detect/correct errors or theft

Opponents Would Say
- Too hard, too much work
- Public is lazy, won’t demand privacy
- Individuals powerless and ignorant
- Can never be sure you’re safe

Tradeoffs
- Time, effort, and inconvenience
- No one to blame but self
Many people believe that privacy is necessary to human dignity and that without privacy no person can fully understand or express himself. Freedom of information access and freedom of expression can be limited by a fear of surveillance. Jeremy Bentham’s concept of the “Panopticon” exemplifies the control government can maintain by suggesting people might be observed. Conversely, anonymity can create a lack of responsibility that invites malicious behavior. Liberty needs a balance that encourages free expression without encouraging cruelty.

Privacy is different from confidentiality. Personal information is private when only the individual is privy to it. Personally identifiable information (PII) needed to serve a customer is protected to the extent of an organization's confidentiality policy. Another protection is “opt-in” which requires that the individual make a choice whether to share personal information. Informed choice depends on knowing how the information will be used, and protected, and how long it will be kept. Confidentiality relies on information security procedures and on records management practices.

While, the US Constitution does not explicitly state a right to privacy, courts have found that the First Amendment implies a right to privacy. The Third, Fourth and Fifth Amendments each address an aspect of privacy. The Fourth in particular requires “probable cause” for a search and limits searches to only what is described in the warrant. Justice Brandeis, in his influential dissent in Olmstead v. U. S. (1928) cited “the right to be left alone -- the most comprehensive of rights and the right most valued by civilized men.” See http://www.law.umkc.edu/faculty/projects/ftfrials/conlaw/rightofprivacy.html for cases.
Congress has addressed some aspects of privacy, for example, restricting use of the Social Security Number and regulating individually identifiable health information through HIPAA (http://www.hhs.gov/ocr/privacy/index.html) and financial information through the FTC’s administration of the Financial Privacy Rule (http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html). Other nations have taken different approaches to protecting privacy, for example, the Office of the Privacy Commissioner of Canada (http://www.priv.gc.ca/).

Democracy requires transparency rather than secrecy in government activity whenever possible without compromising security or individual citizen privacy. Freedom of Information Acts (FOIA) at federal and state levels help citizens maintain a check on government power, while exemptions to the FOI laws protect confidential records like library use. Both secrecy and invasion of privacy erode trust between the citizens and their government.

Since September 11, 2001, legislation and executive decisions have heavily impacted privacy. The USAPATRIOT Act authorized searches of many sorts of records and documentation and National Security Letters (NSLs) require that those records be preserved. The Act expanded the scope of the Foreign Intelligence Surveillance Act (FISA) and the secret court established by that law. In response to heightened concern for public safety, the REAL ID Act of 2005 pushes drivers’ licenses toward becoming national identity cards. Some government actions in response to terrorism have been taken without a vote, like the no-fly list.

**technology**

The capacities of new technology have led some people to declare “privacy is over.” As a general rule, people can have no expectation of privacy in a public place. Thus surveillance cameras cover many public accommodations and outdoor spaces. In libraries, there is an expectation that only behavior will be monitored, not content consulted. But cell phone cameras make the potential recording of one's image and actions ubiquitous. And technology once only available to spies seems poised to enter everyday life: satellite photos of one's home, tracking chips in one's pet, caller ID on phones, DNA research, even computer eavesdropping software.

Digital data storage offers the possibility of data mining and automated correlations that create a dossier without any reality checking. The ease of retrieving digital records like real estate transactions has increased the risk of identity theft. And digital record security is an arms race with frequent reports of hacking and stolen laptops. Passwords and firewalls trade off convenience for security.

The Internet and especially social networking open more areas where personal information can become public. Google has become a verb for investigating new acquaintances. Site registration requirements have taught some people to create fake identities. Spam and phishing emails can feel invasive even though there is no privacy threat, unless one responds. It is hard to know when online purchases and financial transactions are secure and what is safe over wireless networks.
commerce
Private enterprise can be a source of innovation in privacy technology. And businesses want to prevent theft of their goods and their records so they are also a market for privacy and security enhancements. RFID chips may be used to protect goods before sale, but may not be “killed” after the goods are bought. Credit information is vital to commerce and often the goal of identity theft. Cash transactions can protect privacy through anonymity.

It is to a retailer's advantage to know customer buying habits so a business may provide savings or convenience as a trade off, like the common grocery “customer loyalty” card. Online retailers may use cookies to recognize repeat visitors to a website or grant extra privileges to registered customers, like posting reviews on Amazon. Privacy policies may change and personal data may be sold, treated as an asset in bankruptcy proceedings, or mined by law enforcement. Telemarketers don't actually compromise privacy, unless one responds, but they feel invasive.

The needs of employers may impact the privacy of job applicants with background checks, drug tests, and investigations of online activity. However, HIPAA protects medical privacy to a far greater extent than in the past. Recent mass murders have presented a challenge to the privacy of mental health records of students and employees. Employee email and use of the Internet has little if any privacy protection.

social expectations
Mass media’s potential for nationwide gossip has altered expectations of privacy and created assumptions that reporters are invasive, that sources are anonymous, and that celebrities and politicians are fair game. This raises worries about exposure of youthful follies, as well as possible lies and mis-impressions. Snoopy neighbors are suspected of wanting to imposing moral judgments on others. Reality TV affirms that fame is more valued than privacy.

Most people seem to believe that other people are apathetic when it comes to privacy.

The relationships between children and parents and the appropriate level of privacy within a family is unique for each family. The main concern that parents express is that government rules will interfere with their family choices.

All public policy decisions involve trade-offs. Most decisions have losers as well as those who gain. Or a trade-off may be between short and long term results. Not only is it impossible to avoid trade-offs, it is crucial to acknowledge them and to try to compensate for them in making public policy decisions.
Privacy: What's at Stake? What are the Issues? What Does It Mean to Me?

#5: Post Forum Questionnaire

1. Are you thinking differently about this issue now that you have participated in this forum?
   □ Yes    □ No    If yes, how?

2. In your forum, did you talk about aspects of the issue you hadn’t considered before?
   □ Yes    □ No

3. What, if anything, might citizens in your community do differently as a result of this forum?

4. How many deliberative forums have you attended, including this one?
   □ None    □ 1 - 3    □ 4 - 6    □ 7 or more    □ Not sure

5. Are you male or female?
   □ Male    □ Female

6. How old are you?
   □ 17 or younger    □ 18 - 29    □ 30 – 49    □ 50 - 64    □ 65 or older

7. Are you:
   □ African American    □ Asian-American    □ Latino
   □ Native American    □ White/Caucasian
   □ Other (please specify)____________________

8. How much schooling have you completed?
   □ Less than 6th grade    □ 6th – 8th Grade    □ Some high school
   □ High School graduate    □ Some College    □ College Graduate
   □ Graduate School

Please fill out this form and leave it with the forum leader.