Outreach to Patrons and the Public

This section introduces information and resources for libraries to host public discussions on privacy.

The civic engagement framework offers libraries a unique structure for engaging users in meaningful discussion, deliberation, and dialogue. This process emphasizes respect for all attitudes and opinions that are expressed, and enables libraries to truly begin a conversation on privacy values and concerns in their own communities. A sample handout for the civic engagement process is provided.

In addition to the overview provided here, more comprehensive materials for conducting a deliberative forum are available online at www.privacyrevolution.org. These include a full moderator’s guide, a full set of documents for participants, and a post-forum questionnaire.

The chapter on town hall meetings offers another possibility for libraries to engage citizens in discussion around issues of concern to the entire community.

We wish to acknowledge the work and leadership of ALA’s Fostering Civic Engagement Member Initiative Group (MIG) and the Intellectual Freedom Round Table (IFRT) in developing these tools and the framework for a national conversation on privacy.
Civic Engagement: Hosting a Deliberative Forum on Privacy

Nancy Kranich

- What are our expectations for privacy in the digital realm?
- Is it reasonable to expect that information by and about us will remain private?
- Whom do I trust to protect my privacy?

By sparking a national conversation on privacy, Choose Privacy Week will give people with different perspectives an opportunity to learn more about privacy issues, weigh in on choices with their 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 trade-offs. Trained moderators help participants listen to and understand the experiences and views of others and seek common ground for addressing difficult problems. America’s libraries invite our communities to join this conversation about the tough privacy choices facing our nation.

The purpose of public deliberation is to increase the likelihood of making sound, well-supported decisions about public issues. This is achieved by exploring and testing our ideas as we struggle with hard choices, considering the pros and cons of each option. Deliberation opens possibilities for new solutions and leads us to find common ground—mutual understanding of our differences and ways to act even with those differences.

Deliberative forums encourage dialogue and understanding about difficult issues facing our country and our communities. They offer opportunities for participants to listen to each other for deeper understanding, without advocating a position or debating opponents. With the help of trained moderators and issue guides, individuals are able to discover that their personal values and concerns often overlap with those who hold very different perceptions of problems and their possible solutions.

Privacy is a particularly slippery and amorphous issue, about which people hold a wide variety of opinions and beliefs. This section offers tips to help librarians plan to convene and moderate their own deliberative forums about privacy. For those who wish to learn how to moderate deliberative dialogues, ALA can offer guidance on locating a training institute. Below is a short overview of the process of convening and moderating a deliberative forum on privacy.

Deliberative Forum

**PRIVACY: WHAT’S AT STAKE? WHAT ARE THE ISSUES? WHAT DOES IT MEAN TO ME?**

Librarians around the United States developed this issue framework by asking 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 whom to turn to and how to know what actions are effective. Thus, we ask, “Whom do I trust to protect my privacy?” Three approaches emerge:

1. **The marketplace** is the source of innovation in security and privacy protection technology and has a vested interest in privacy that secures the integrity of financial data.
2. **The government** has a responsibility to provide for public safety, which includes identity protection, and to secure the rights necessary to a free society.
3. **I, myself,** recognize that privacy values are individual and varied and that no one cares more about my needs than me.

The charge to participants is to deliberate, work as citizens, and find opportunities for authentic talk about the motivations behind what people are saying. The forum begins with an overview, followed by deliberation for 1½–2 hours. Participants are encouraged to find common ground and will debrief about the process at its conclusion. A sample schedule for the forum is as follows:

- Welcome/overview of deliberative dialogue and the framing of the privacy forum: 20 minutes
- Personal Stake: 20 minutes
- Approach 1: Marketplace: 20 minutes
- Approach 2: Government: 20 minutes
- Approach 3: Myself: 20 minutes
- Next Steps and Reflections: 30 minutes
The moderator begins by selecting a recorder and introducing the ground rules. The group’s charge is to make choices about public issues by deliberating and weighing choices. Competing approaches to problems will be considered and all positions will be discussed, including the perspective of people who aren’t present. Key ground rules include:

- Everyone is encouraged to participate.
- No one or two individuals dominate.
- The discussion will focus on the choices.
- All the major choices or positions on the issue are considered.
- An atmosphere for discussion and analysis of the alternatives is maintained.
- We listen to each other. (Source: National Issues Forums Institute)

Participants then introduce themselves and their personal stake in the issue. Taking 1–2 minutes each, individuals give their first name and discuss what brought them to the forum, what their personal experiences with this issue are, and what concerns them most about this issue. Concerns of all participants are recorded.

The moderator guides discussion to define the problem and discuss a course of action.

- What are the pros and cons of different approaches?
- What are the costs and consequences?
- What can we define as facts, trade-offs, and values?

**Whom do I trust to protect my privacy?**

After taking a moment to read about Approach 1, the marketplace, participants are asked:

- What do you like about the approach (pros)?
- What don’t you like (cons)?
- Why or why not?
- When someone makes what seems like an obvious and straightforward statement, sometimes it can be very helpful for the purposes of deliberation to ask “why?” or “why not?”
- How? This is another question that can be very effective in pushing people to think more deeply.

The moderator encourages participants to consider what is valuable to us.

- How has this issue affected you personally?
- When you think about this issue, what concerns you?
- What is appealing about the first option or approach?
- What makes this approach a good one—or a bad one?
- How did you come to hold the views you have?

Consequences, costs, and benefits are also at issue.

- What would be the consequences of doing what you are suggesting?
- What would be an argument against the option you like best?
- Is there a downside to this course of action?
- Can anyone think of something constructive that might come from the option which is receiving so much criticism?

The moderator also focuses discussion on inherent conflicts.

- What do you see as the tension among the options?
- What are the gray areas?
- Where is there ambiguity?
- Why is this issue so difficult to decide?

The group seeks a shared direction or common ground by considering:

- What trade-offs are we willing and unwilling to accept?
- What are we willing and unwilling to do as individuals or as a community in order to solve this problem?
- If the policy we seem to favor had the negative consequences some fear, would we still favor it?

Quiet time for personal reflection (2 minutes) encourages individuals to consider:

- How their thinking about the issue has changed;
- How their thinking about other people’s views has changed;
• How their perspective has changed as a result of what they heard in the forum.

Group reflection asks participants to consider:

• Has the way I’m thinking about or understanding this issue been affected by how we’ve worked our way through it? If so, how?
• Did I, as an individual, really grapple with the costs and consequences of each approach, even the one I liked most?
• Did we, as a group, really identify and work through the costs and consequences of each approach?
• If we did not thoroughly work through this issue in this forum, what should we do about that?
• What trade-offs are we willing to make, at this point, to work on this issue? Why?
• What trade-offs are we not willing to make? Why?
• Do we see any ways for taking action on this issue, with the information we now have?

• If not, what kind of information would help us see ways of acting on this issue?

Finally, a focus on next steps also allows participants to discuss a shared sense of direction or purpose, and any common ground for action.

• What do we still need to talk about?
• How can we use what we learned about ourselves in this forum?
• What are you going to do with what you learned today?

Close by thanking everyone for participating and tell them that you will share their concerns with the ALA Office for Intellectual Freedom.

All participants can visit www.privacyrevolution.org to learn more about Choose Privacy Week and participate further in the national conversation on privacy.
The Language of a National Conversation on Privacy: Sample Handout for Civic Engagement Deliberation

CAROLYN CAYWOOD

Civil liberties

Many people believe that privacy is necessary to human dignity and that without privacy no person can fully understand or express him- or herself. 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 about 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 www.law.umkc.edu/faculty/projects/ftrials/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 (www.hhs.gov/ocr/privacy/index.html) and financial information through the FTC’s administration of the Financial Privacy Rule (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 (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 FOIA disclosure protect confidential records such as an individual’s use of the library. 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 USA PATRIOT Act authorized searches of many sorts of records and documentation, and National Security Letters (NSLs) are used to require that existing records be preserved for searches. The Act expanded the scope of the Foreign Intelligence Surveillance Act (FISA) and the secret court established by that law. Librarians have challenged some searches as threatening First Amendment rights.

In response to heightened concern for public safety, the REAL ID Act of 2005 pushed drivers’ licenses toward becoming national identity cards but concerns about costs and privacy have led many states to pass legislation opposing Real ID. 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 (not the content viewed) will be monitored. 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, GPS tracking and EZ-Pass, injecting chips into 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 personal digital records has increased the risk of identity theft. And digital records security is an arms race with frequent reports of hacking and stolen laptops. Passwords and firewalls trade off convenience for security, and the more uncrackable the password, the more likely the user can’t remember it without a security-compromising note.

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 records, so they are also a market for privacy and security enhancements. RFID chips may be used to protect goods before sale, but some 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. Telemarketing feels like an invasion of privacy, and of course if one gives out information there is no guarantee how it will be used.

The needs of employers may impact the privacy of job applicants with background checks, drug tests, and investigations of online activity. However, HIPAA restricts uses of medical information 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-impresions, and may discourage candidates from seeking office. 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, but snoopy neighbors are suspected of wanting to impose moral judgments on others. Conversely, the challenge, “If you have nothing to hide, what are you afraid of?” is hard for many people to resist. There is also a continuing tendency to correlate what people read with how they are likely to behave.

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. This can cause conflict with library policy that protects the confidentiality of borrowers who are minors.

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.
Town Hall Meetings

CAROLYN CAYWOOD

When a community needs to deal with a local issue, a Town Hall process can be useful in generating new ideas and different perspectives, in getting at underlying values and priorities, in finding common ground and building understanding and respect, and in helping the community become better informed. Many local issues have privacy implications: for example, surveillance cameras, posting student grades, online real estate records, security of online payments, employee name badges, etc. But, be sure it is the right process for the particular issue at the present stage in decision-making. A Town Hall is not an appropriate process for a crisis. It does not produce statistically valid data and should not address highly technical questions. And it does not satisfy legal mandates for a Public Hearing.

A Town Hall functions best as a semi-formal meeting that begins with a presentation to address any gaps in knowledge that are necessary for informed discussion. This briefing should be short, non-technical, and even-handed. If this is followed by small group breakout tables, more voices and quieter voices can be heard. Decision-makers should be spread around the tables to listen and answer questions. If necessary, technical experts should float among tables to answer questions. Each table needs a facilitator and a recorder. Paper should also be available for written questions and comments. The recorder should try to capture specific phrases and points which can be compiled into a report of the meeting.

Each table should have about three questions to discuss. The questions should get at the public policy aspects of the issue—values, priorities, trade-offs. Avoid questions that invite participants to show off how much they know rather than deal with what they consider important. Do not waste the opportunity to learn how the participants really feel about the issue by asking vague, euphemistic, or slanted questions. Examples of good questions: “What should weigh most in a decision about whether to install red light cameras: traffic safety, revenue, or invasion of privacy?” “It is important for parents to bring preschoolers to the library and share books with them. It is important for the library to protect the confidentiality of readers. And it is important for borrowed books to be returned to the library. How do we balance these three needs?”

Logistics are important. Plan a time that is not a conflict for the participants you seek. Find a site that is comfortable and big enough with adequate projection equipment. Ensure that the breakout tables can talk without disturbing each other. Refreshments are always welcome. Do not depend on publicity—invite people who need to be at the table. And look beyond the usual representatives of particular groups.

Planners of Town Hall meetings need to determine the following and then share transparently with the community:

- How far along is the decision process? Town Halls are best used early on.
- How will the participants’ input be used? How will they be informed of the results of the Town Hall and later of the decisions that are eventually made?
- What specifically are participants being asked? Asking the right questions is critical—questions must be within participants’ ability to answer.
- What factors are not negotiable? Legal mandates, available funding, or safety may be a boundary on the discussion.
- What knowledge do participants need? It should not exceed what can be presented in a “briefing.”
- How have you ensured that diverse viewpoints are represented? Have all stakeholders been invited?

Resources

- www.theworldcafe.com/articles/aopq.pdf
- http://ctb.ku.edu/en/promisingapproach/
- www.everyday-democracy.org/exchange/Tag.41.aspx
- www.lwv.org/AM/Template.cfm?Section=Election_2008&template=/CM/HTMLDisplay.cfm&ContentID=9339
- www.thataway.org/?page_id=1442
- www.sfcg.org/resources/resources_tips.html
- http://discuss.ala.org/civicengagement/
- www.opal-online.org/archivecivic.htm
- www.csus.edu/ccp/publicinvolvement/
- http://privacyframing.wetpaint.com/