Tools and Strategies for Protecting Kids from Pornography and Their Applicability to Other Inappropriate Internet Content

Computer Science and Telecommunications Board
Board on Children, Youth, and Families
The National Academies

Herb Lin, PhD
202-334-3191
hlin@nas.edu

Michele Kipke, PhD
202-334-3883
mkipke@nas.edu

Summary

The subject of controlling children's Internet access to pornography is charged politically and emotionally in the national debate. Other areas do provoke public concern, but pornography on the Internet is and has been a major focus of national debate for quite some time. Through its primary focus on Internet pornography and threats to children from sexual predators on the Internet, the final report will also, and to a lesser extent, include: (1) an objective description of the risks and benefits of various tools and strategies for addressing pornography that might be used to protect children from inappropriate material on the Internet; (2) an explication of how "packages" of different technological and non-technological tools and strategies can be used together to enable local approaches for protecting children from inappropriate material on the Internet; and (3) case studies of how different communities have approached the problem of protecting children from exposure to pornographic material on the Internet and, again, what those lessons teach about other inappropriate material. Providing a better understanding of different tools and strategies can promote a more reasoned consideration of various public policy options as well as more informed approaches that are locally implementable. The study is expected to provide a foundation for a more coherent and objective local and national debate on the subject of Internet pornography, but will avoid making specific policy recommendations that embed particular social values in this area.

This study originated in a Congressional mandate to the Attorney General by the U.S. Congress in Public Law 105-314 (Protection of Children from Sexual Predators Act of 1998) Title IX, Section 901. The requesting legislation is attached.

Origin

Public Law 105-314 (Protection of Children from Sexual Predators Act of 1998) Title IX, Section 901, mandated that "not later than 90 days after the date of enactment of this Act, the Attorney General shall request that the National Academy of Sciences, acting through its National Research Council, enter into a contract to conduct a study of computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet, in order to develop possible amendments to Federal criminal law and other law enforcement techniques to respond to the problem."

In response to this Congressional mandate, the Computer Science and Telecommunications Board and the Board on Children, Youth, and Families of the National

Research Council (NRC) developed a proposal to convene a committee of experts to explore the pros and cons of different technology options and operational policies needed to support the use of those options. As the result of discussions with the Department of Justice's Office of Juvenile Justice and Delinquency Prevention, the Department of Education, and various private companies in the information technology industry, the study's scope was altered in two ways. The first is that the study now includes non-technological strategies as well as technology options for protection, on the grounds that technology options are one, but only one, element of a comprehensive approach to protection. The second is that the study will be an inquiry that centers on pornography as the primary systematic focus of "inappropriate content", with other areas addressed as appropriate for context-setting purposes, explored incidentally rather than systematically and only as they arise in the context of discussions about specific tools and strategies used in relation to Internet pornography.

Detailed Description

Policy Context

The potential applications of the Internet to enhance and transform K-12 education are well-known today, and many public policy decisions have been taken to provide Internet access for educational purposes. Coupled with the steadily increasing fraction of U.S. classrooms and schools connected to the Internet over the past five years (Note 1), the growing ubiquity of networked information technologies in the home (Note 2) has enabled large numbers of school-age children to reach the Internet. Easy access to the Internet (and related commercial online services) has many advantages for children -- educational materials; online friendships and pen pals; access to subject matter experts; recreation, hobby, sports information; and so on.

At the same time, easy access to the Internet raises many concerns about access of children to inappropriate materials. Of all of the subject areas that might be regarded as inappropriate, pornography is perhaps the area that generates the most pointed societal concern. As a result, there is a reasonably broad social consensus on the undesirability of exposing minors to such material.

Successfully dealing with concerns about pornography and other inappropriate materials is arguably a necessary condition for fully exploiting the educational potential of the Internet. Otherwise, fears about exposure to such material will result in efforts to that may well detract from the positive educational benefits of using the Internet (Note 3).

As a vehicle for understanding the pros and cons of various approaches to protecting kids from inappropriate material on the Internet, pornography is particularly compelling for two reasons. One reason is that, as noted above, pornography is an area that arouses significant concern across a broad cross-section of society. The second reason is that despite this broad social concern about pornography, judgments about what counts as pornographic vary widely. Because the specifics of public concern about pornography thus vary by community, effective approaches to deal with community concerns must account for such variation, and how to account for varying community concerns is a point that is common to dealing with a wide range of material that might be regarded as inappropriate.

The need for parental or teacher involvement in controlling what children can see and read from the Internet is often cited. But as a practical matter, children are likely to have some degree of unsupervised access to the Internet or other online services (e.g., in homes with more permissive parents or simply because of the unfeasibility of continuous parental monitoring of children's Internet use). This reality has led policy-makers to consider various legislative approaches that penalize parties that make pornography available to children and/or require third

parties (e.g., content providers, online service providers) to take affirmative steps to restrict the access of minors to such material. Furthermore, this reality has fed public expectations (or at least desires) for a technological solution to the problem (see below).

At issue are three basic problems. The first problem involves a characterization of material, especially images, that minors should not be allowed to view. The law distinguishes between "obscenity" and "indecency", granting a much higher degree of protection to the latter than the former. Pornography per se is not defined legally at all. But whether a given image is obscene (or indecent, for that matter) is difficult to determine objectively. Indeed, it was a Supreme Court Justice who observed that "I can't define it [obscenity], but I know it when I see it." Furthermore, the same image or text can have different meanings and interpretations depending on context. (A recent example is the publication on the Web by the U.S. Congress of the Starr report.)

A second problem is that even if a specific definition of "pornographic" can be stipulated, any technical approach for distinguishing between pornographic and not pornographic material will be imperfect. That is, any means will suffer from both false positives (i.e., material identified as pornographic that a reasonable observer would determine to be not pornographic) and false negatives (i.e., material identified as not pornographic that a reasonable observer would determine to be not pornographic). For example, technical approaches to blocking pornographic material can also result in non-pornographic material being blocked, including artwork, medical images, and the like (false positives), in addition to allowing some fraction of objectionable pornographic material (false negatives). Any plausible and useful methodology for distinguishing between pornographic and non-pornographic must weigh false positives against false negatives and the harm that results from each.

The third problem is that minors must be differentiated from adults if minors are designated as a class of individuals that must be shielded from pornographic or other inappropriate material. It is problematic even when transactions are conducted in a face to face manner. For example, an individual showing a driver's license as proof of age may be showing a falsified license, or may obtain the materials on behalf of an underage friend. In cyberspace, where face to face interactions are not possible, verification of age is much more difficult.

These three problems underscore a key point that is often overlooked in political debates over protecting children on the Internet -- as with all technology, technologies for protecting children on the Internet cannot be viewed as definitive "solutions" in the absence of an appropriate social, cultural, educational, and policy context. Focusing only on the technology to provide protection ignores the potentially larger benefits available from multiple points of control, such as those that might be made available through acceptable use policies in libraries, Internet safety education undertaken in schools, and active involvement from parents.

Technical Context

Technology can provide tools that can help prevent children from accessing on the Internet pornographic and other inappropriate content. Indeed, the legislation requesting this study focuses primarily on technological approaches for controlling electronic transmission of pornographic images. A recent paper (Note 4) notes that decisions on what content can be passed to what recipients are based on three types of information:

- the specific content of the item (e.g., does the item contain a picture of overt sexual activity);
- the recipient's jurisdiction (e.g., is the recipient located in San Francisco, California or in Memphis, Tennessee);

- the recipient's type (e.g., is the recipient an adult or a minor).

The authors of this paper argue further that the architecture of today's Internet denies some or all of the relevant information to any party on whom responsibility might be placed to control access, thus making the imposition of access controls on content particularly difficult.

While technology could facilitate the easier imposition of access controls, the adoption of such controls might well entail other consequences. For example, the imposition of access controls may inhibit technological innovation and increase vulnerability to hardware and software failures. Technologies that facilitate the imposition of access controls would provide a generalized ability to regulate based on jurisdiction and recipient characteristics even for issues beyond content control (to include denial of information to certain recipients based on jurisdiction or type), or provide governments with the ability to regulate access based on the content or the origin of specific pieces of information.

Despite such difficulties, the technical solutions proposed (for either voluntary or mandatory use) generally involve one or more of the four following techniques.

- technically identifying images or text that are potentially inappropriate. For example, if the concern is pornography, text can be scanned for particular words -- an imperfect scan at best, but nevertheless one that might detect some non-trivial fraction of potentially pornographic text. More sophisticated approaches might call for some degree of machine-based understanding of text to identify potentially pornographic material. Pornographic images pose a different problem, because the technology for image understanding and interpretation is still less mature than those for text. A very simple scan of image files for large amounts of flesh tone, for example, is the most basic kind of image recognition technology, but obviously one that can result in a high false positive and false negative rates. More sophisticated techniques employ some combination of features that perform a rudimentary pattern recognition on image files; these techniques are capable of greater selectivity in their identification of potentially pornographic images.
- tagging images or text that are judged to be inappropriate for viewing or access by children, an approach exemplified by the Platform for Internet Content Selection (PICS). Under the PICS approach, content is tagged with a machine-readable label that is generated by the judging party (for example -- is this image pornographic or non-pornographic?). The judging party can be the content provider (whom the PICS approach enables to voluntarily label the content it creates and distributes), or a third party (to whom a parent or teacher can turn to judge the appropriateness of material). (Note 5)
- Identifying sites on which pornography or other material inappropriate for children may be found. This approach depends on a third party judging the appropriateness of a given site for minors; a list of inappropriate sites is then published (and generally integrated into Internet access software that prevents access to those sites).
- restricting access to certain sites (or material) to adults-only. Typically, sites using this approach require the use of a credit card on the assumption that only adults will have access to a valid credit card number.

All of these approaches are imperfect. For example, scanning for flesh tones eliminates historic art and medical information. Tagging content relies on a judgment of a third party that may not comport with the judgment of "pornographic" in any particular situation, and may be much less relevant in the context of user-generated content that may be objectionable. Site-specific approaches deny access to non-pornographic material located on them, and furthermore, sites containing pornographic material emerge daily, so any given list of suspect sites is incomplete by the time it is distributed.

Finally, considerations of how to proceed in the face of technology's imperfections are exacerbated by high rates of technological change. One complication is the fact that a new and

better technology is almost always around the corner, leading to (unrealistic) hopes that the next technology will be sufficient in itself provide a perfect (or at least an adequate) solution. A second complication is that policies and procedures that are tied to specific technologies may be rendered obsolete by changes in technology.

It is for these reasons that non-technical dimensions of the problem must be considered.

Social Context

The issues beyond the technological involve those of society, culture, and development. Indeed, the larger context in which technology is embedded involves processes, incentives, laws, and policies have as much -- or more -- impact on the actual protection of children as does technology. For example, what steps do children, parents, schools, libraries, and other institutions need to take when a given technological approach fails to protect a child from pornographic or other inappropriate material or prevents access to desirable content? How do/should parents, schools, libraries, vendors, and other institutions carry out their responsibilities for protecting children from pornographic or other inappropriate material? Such questions are inherently social and cultural.

Furthermore, individuals under the age of 18 -- commonly known as "children" or "minors" -- in fact span a very broad developmental range. What may be developmentally inappropriate for a young child may be more appropriate for a teenager. (For example, a site providing a detailed scientific description of human reproduction may be more appropriate for the latter than the former.) Developmental considerations are thus critical when determining how the Internet may be associated with both risks and opportunities among children and adolescents.

A third social dimension is that the existence of differing philosophies of social control over the definitional process. One philosophy asserts that individual communities have the right (and obligation) to define what is objectionable. A second philosophy, rarely stated but often implicit as the motivating force behind certain policy positions, is the idea that a particular definition of objectionable -- namely one supported by specific advocates with a specific social agenda -- is appropriate for all communities.

Finally, different venues of access must be considered. Controls on exposure to certain types of material that operate in one venue (e.g., school) may be obviated by unrestricted access to all types of material in another venue (e.g., home). Comprehensive restrictions thus require coordinated action among stakeholders that do not always act in such a manner. On the other hand, a choice could be made to allow different degrees of access to objectionable material in different venues (e.g., more restrictive in school, less at home). Either choice might be appropriate depending on the evidence that comprehensive restrictions are needed, the politics of attempting coordinated action, and other non-technical factors.

Plan Of Action

Statement of Task

While a study limited to technology options would help to ensure that public debates over the appropriate approaches to address the problem would be technologically informed, a fully informed debate necessarily goes beyond technology. Thus, while the study will certainly provide a thorough examination of technological options (thus fulfilling the legislative mandate), it will also examine the full range of tools and strategies that can be used to protect children from exposure to pornographic material on the Internet. Many of these tools and strategies may be applicable to other forms of inappropriate material online. The study will focus on tools and

strategies for dealing with pornography and then, where appropriate, consider how these same tools and strategies could be used elsewhere. These topics will be addressed in the context of possible options for actions by educators, librarians, parents, industry groups, online service providers, legislators, law enforcement authorities, and policy makers.

To provide a systematic grounding for the analysis, the study will use pornography to illustrate the numerous dimensions of the issue. When appropriate, the discussion of particular tools and strategies will address their utility and applicability for dealing with other types of inappropriate material, though these other areas will not be addressed in a systematic or comprehensive manner. (In other words, other areas will be not be singled out for discussion per se, but rather will be addressed only as they are relevant to discussions of specific tools and strategies.)

For example, one strategy that can be useful as an element of a comprehensive approach for dealing with pornography is the local development, promulgation, and enforcement of acceptable use policies (AUPs). However, any implementation of an AUP must deal with a broad range of issues, only one of which is pornography. The discussion of AUPs would thus illustrate its applicability to other issues that are of concern to various communities, even as it focuses on what might be done about pornography.

This study is not expected to determine what kinds of material should be regarded as pornographic material that is inappropriate for viewing by minors. Instead, it will focus on articulating the various technical, social, and economic risks and benefits of different tools and strategies for protecting children from pornography on the Internet. Furthermore, it will discuss various "packages" of tools and strategies that would be effective for achieving different goals. But because any given goal embeds particular social values, the study will not make specific recommendations for what package should be adopted by the nation. The primary value of this study is to provide neutral, objective analysis of various options so that an informed national debate on the subject can take place.

An obvious question is how this proposal relates to the "GetNetWise" inititative announced on July 29. The answer is that GetNetWise is first and foremost an information resource for those concerned with protecting children on the Internet. That is, it provides information on tools (e.g., specific vendors offering filtering software) and safety tips (e.g., how to conduct yourself on the Internet). However, by design, GetNetWise eschews assessment or evaluation of these various tools.

This proposal takes the next step to explicate the pros and cons of various tools and strategies for protecting children on the Internet, not on a product-by-product or vendor-by-vendor basis, but rather in generic terms (e.g., what are the pros and cons of filtering software). This better understanding of the pros and cons of different approaches to such protection also forms the basis for an analysis of possible policy options at the federal, state, and local levels -- another area avoided by the GetNetWise initiative.

Expertise Required

This project will require perspectives including those of law enforcement, constitutional law, librarians, ethics, and educators, and parents, as well as technical expertise in networking technologies and image recognition. Recognizing the importance of social, cultural, and developmental considerations, the committee will also include individuals with expertise in child and adolescent development, psychology, sociology, and education**.** Nominations for the study committee will be solicited from a broad range of sources.

Preliminary Work Plan

The National Research Council will assemble a study committee of approximately 12-14 members with expertise in the areas outlined above. The committee will attempt to identify the range of tools and strategies that might be used to protect children from accessing pornography and, secondarily, other inappropriate material on the Internet (Note 6). Furthermore, through briefings, testimony, and public outreach (e.g., public forums in the fact-finding stages), it will seek to understand the risks and benefits of these different options. The committee will attempt to answer questions such as:

- What is the exposure of children to pornography and other inappropriate material on the Internet?
- What technical and non-technical approaches are used today to protect children from pornographic material (as well as other inappropriate material) carried by the Internet and print/film media? (Note 7)
- How does Internet dissemination of pornographic or other inappropriate material differ from the use of other media for such purposes? What are the implications of these differences?
- How effective are known approaches to controlling Internet access to pornography? To what extent are some approaches sensitive to the type of inappropriate material (e.g., pornography vs. hate speech or bomb-making)? How can those approaches be circumvented? What is the ease with which they can be circumvented? What measure of control remains under likely scenarios of circumvention?
- What are some of the current "best practices" used in classrooms and by communities to protect minors from exposure to pornographic or other inappropriate material?
- What are the "false positives" and "false negatives" associated with the technical approaches available today? What is their significance?
- What research is needed to develop new technical approaches and/or social strategies to protecting children from pornographic materials on the Internet?
- What is the social and economic impact of different technical approaches and/or social strategies to protecting children from pornographic materials on the Internet?
- How do the necessary tools and strategies change when pornographic materials are pushed onto children (as opposed to children seeking out pornographic materials on their own)?
- What are possible standards by which to judge the adequacy of different approaches? Can controls on Internet access to pornographic material be as "effective" (however that term is defined) as those for access through other media?
- What are some of the non-technological strategies that might be used by educators, librarians, parents, and local communities to protect children from exposure to pornographic materials on the Internet?

Note: for purposes of this study, it is important to draw a distinction between “operational policy” and “social” or “national” policy. Operational policy issues are narrow in focus and may be required to support any regime of technical controls other than pure “laissez-faire”; operational policy may refer to legislation, regulations, voluntary industry action, or consumer-level actions that relate to technical controls (e.g., technical controls of type X are mandated as an integral element of all computers sold in the U.S.). By contrast, social/national policy issues refer more broadly to issues such as what kinds of material are allowed to circulate on the

Internet and what is the social balance between the value of access to the Internet vs. the harm of access to pornography. Recognizing that operational policy and social policy are not always clearly separable, the study will endeavor to stay away from social/national policy questions on the grounds that it is inappropriate for this study to be involved in making judgments about what kinds of material are or are not acceptable for children to view.

The committee will convene in 7 meetings during the course of the study to solicit input from outside parties, deliberate over its findings and recommendations, and prepare its final report. The budget provides for extensive input to be sought from a wide range of public interest groups (including the American Civil Liberties Union, the Center for Democracy and Technology, and the Electronic Frontier Foundation; the Christian Coalition and the Family Research Council; the National Parent Teachers Association), lawmakers (e.g., the Congress), the Executive Branch (Department of Justice and FBI), and other interested groups.

In addition, we envision conducting two workshops within the first year in conjunction with this project. Workshops at the Academy are opportunities to convene groups of experts to address issues of pressing importance and to advise the deliberations of committees. While workshops are not intended or designed to result in consensus, findings, or recommendations, presentations and discussions at the workshops help committee members enhance their understanding of the matters before them. And, because workshops are open to the public (and in particular to staff from the executive and legislative branches), the papers presented at the workshops and the discussions conducted therein are opportunities for publicly airing information useful to the policy process before the release of a final report. (Briefing books for workshop participants containing background information, commissioned papers, and papers by speakers would also be made available to interested parties.)

One workshop will feature speakers knowledgeable about children's' use of and experiences on the Internet (at school, in the community, and at home), different non-technical approaches to the issue of protecting children from pornographic and other inappropriate material on the Internet, efforts to encourage and support children from not accessing pornographic materials on the Internet, and efforts to discourage individuals and businesses from inappropriately engaging or soliciting children on the Internet to engage in sexual activity or to view pornographic materials. This first workshop could also be used explicitly to solict the in-person views of Internet-using minors. Also, because the non-technological dimensions of the problem will change more slowly than the technologies involved, a workshop summary will be prepared that integrates the presentation of papers with the ensuing discussion. A second workshop would focus on a review of the technical options and associated operational policy considerations that can be used to help protect children from exposure to pornographic materials on the Internet, as well as the advantages and disadvantages of these options.

Depending on the availability of resources, a third workshop will be held, structured around a "design exercise" that will engage individuals from various community sectors and settings, including education; libraries; community-based agencies; churches and faith communities; business/industry, law enforcement; elected officials and other local policy makers; community leaders; parents; and teenagers. Prior to the workshop, background information would be distributed to workshop participants, describing a number of tools and strategies; this information would help to establish a common ground for workshop participants.

The "design exercise" of the workshop would involve workshop participants working in teams with representation from the various stakeholder groups (e.g., a parent, an elected official, a librarian, a teacher, a business leader, a teenager, a technologist, and a clergyperson). Each team (or teams) would be responsible for developing its own approach to protecting children from pornographic materials on the Internet, working intensively and independently for a full day. Such design exercises have the advantages that they (a) force participants from different backgrounds

and perspectives to interact with each other in a goal-directed manner, and (b) generate immediate feedback for ideas that result in intense, real-time scrutiny by people who understand the realities of implementation in a first-hand way.

At the end of this third workshop, the plans developed during the exercise can be compared and contrasted. As importantly, reports of the process used to generate the plan will inform the committee about potential implementation difficulties and provide greater clarity about the connection between goals and approaches.

Note that throughout the course of the project, there will be considerable effort to ensure the opportunity for public participation and comment, including public forums at the workshops, calls for public comment through the Internet and other media as appropriate, and the NRC's capabilities for accepting public input through its new interactive web pages. (Opportunities for public participation and comment will be targeted to all relevant stakeholders, including Internet-using minors.)

One unique opportunity for synergy exists with the Commission on Online Child Protection, established by the Child Online Protection Act to conduct a study regarding methods to help reduce access by minors to harmful material. The Commission's mandate to study "harmful material" is on its face broader than this study's scope and may lead it to examine many other form of inappropriate content, but the two efforts will certainly overlap with regard to access to pornographic material. While the appointment of this commission has not yet occurred, information that it develops throughout its operating life will be enormously helpful to the committee. The NRC envisions a formal liaison to this commission that will help to facilitate access to such information.

The results of the committee's deliberations will be summarized in a final report to be delivered to the sponsor 18-21 months from the date the contract is awarded. The time remaining in the 24-month project will be used for dissemination activities.

Responsiveness to the Legislative Mandate

The original legislation called for a study by the National Academy of Sciences to address four areas:

- The capabilities of present-day computer-based control technologies for controlling electronic transmission of pornographic images.
- Research needed to develop computer-based control technologies to the point of practical utility for controlling the electronic transmission of pornographic images.
- Any inherent limitations of computer-based control technologies for controlling electronic transmission of pornographic images.
- Operational policies or management techniques needed to ensure the effectiveness of these control technologies for controlling electronic transmission of pornographic images.

As noted above, a fully informed debate necessarily goes beyond technology. Thus, the study will examine the full range of tools and strategies to protect children from pornography. For example, a discussion of the capabilities of computer-based control technologies for controlling electronic transmission of pornographic images is an integral element of any discussion of filtering technologies, which will be an important element of the report. The inherent limitations of computer-based control technologies for controlling electronic transmission of pornographic images are an integral part of any discussion concerning what technology can and cannot do. Relevant operational policies or management techniques fall into the discussion of social and policy considerations in protecting children. And finally, research needed to improve computer-based control technologies will be addressed under the portion of the study

that deals with a research agenda to improve tools and strategies for protecting children from inappropriate material on the Internet.

Cast in terms of discussing the risks and benefits of various tools and strategies, the findings and conclusions of the report will be aimed at informing the public policy debate at different levels (federal, state, and local) over approaches to protecting children using the Internet. Recommendations will be formulated with respect to various goals that the nation, states, school districts, libraries, and parents might decide to pursue. In other words, the report will not establish what goals any of these entities and groups should have, but rather what are more and less effective means for achieving any given goal.

Finally, the legislation calls for the study "in order to develop possible amendments to Federal criminal law and other law enforcement techniques to respond to the problem." Legislative approaches and law enforcement techniques necessary to advance the achievement of various goals will be discussed explicitly in the report.

Roles of Sponsors

A consortium of private and public funding is sought to support this study. Consistent with the NRC's mandate to seek broad public input on matters related to this study, sponsors will be approached to provide:

- briefings on areas of concern at appropriate committee meetings (and written submissions in lieu of in-person testimony);
- nominations for committee members, briefers, and reviewers, as well as for appropriate site visits and/or regional hearings;
- liaisons to relevant interest groups and stakeholders.

In addition, sponsor representatives will be invited to attend all workshops and open sessions of the committee, and will receive all briefing materials.

Product and Dissemination Plan

Using pornography and threats to children from sexual predators as the primary illustrative case, the final report for this project will include: (1) an objective description of the risks and benefits of various tools and strategies that can be used to protect children from inappropriate material on the Internet; (2) an explication of how "packages" of different tools and strategies can be used together to enable local approaches for protecting children from inappropriate material on the Internet; and (3) case studies of how different communities have approached the problem of protecting children from exposure to inappropriate material on the Internet. (However, the report will not endorse specific social goals, and thus the report will refrain from making recommendations on a specific package that should be adopted.) The report will be subject to National Research Council review procedures.

As is true of all Academy reports, an executive summary of the entire report will be prepared that highlights key findings and also specifically addresses the areas specified in the requesting legislation. In addition, a section of the report will be included that describes how the report addresses the areas mentioned in the original requesting legislation.

Workshop proceedings will be issued as interim outputs. These proceedings will include commissioned papers and briefing materials that are used to inform committee deliberations, but will not include findings, conclusions, or recommendations of the NRC. Proceedings will be made available publicly as soon as possible after the workshops involved. A summary of the first

workshop will be prepared that include a synthesis of the discussions at the workshops (though again this will not include findings, conclusions, or recommendations of the NRC). (While a workshop summary is not an NRC product, the NRC will work with sponsors to develop appropriate condensations for their own use, and of course, sponsors are free to circulate these documents as they see fit.)

In order to speed the release of the report, the NRC will transmit to the sponsor and publicly release the report in pre-publication form. In content, a pre-publication report differs from a final report only with respect to copy-editing details (e.g., spelling, grammar, complete references). Both the pre-publication report and the final report are identical with respect to the analysis, findings, conclusions, and recommendations, and both are approved products of the NRC. The publication of the final report would happen several weeks later.

Dissemination activities will target two audiences: "practitioner" communities (e.g., local school systems, libraries, parents) and government policy makers (at the federal, state, and local levels) in both the legislative and executive branches. The full report is intended as a comprehensive resource to both audiences, and will be made available on the Internet via the National Academies' World Wide Web server as well as in paper form. In addition, the content of the full report will be further disseminated through participation in relevant conferences and by publication of summary articles in relevant journals, as appropriate.

In addition, the "practitioner" communities will benefit from stand-alone articles, brochures, and report extracts that pay special attention to locally implementable tools and strategies entirely apart from policy decisions that are made at higher levels. Such materials would be oriented towards what these people can do -- as individuals and local communities -- to help protect children on the Internet.

Public Information About the Project

The Academy will post on its Web site (http://www.nationalacademies.org) a brief description of the project, as well as committee appointments, if any, with short biographies of the members, meeting notices, and other pertinent information, to afford the public greater knowledge of Academy activities, and an opportunity to make comments. The Web site will also include the project's on-going record of compliance with the requirements of Section 15 of the Federal Advisory Committee Act, 5 U.S.C. App. § 15. Sponsors will be provided compliance certification(s) in accordance with Academy procedures.

NOTES:

(1) According to the Department of Education, the fraction of U.S. schools with access to the Internet grew from 35% in 1994 to 89% in 1998, while the comparable fraction of U.S. classrooms rose from 3% in 1994 to 51% in 1998. See ***Internet Access in Public Schools and Classrooms: 1994-1998***, U.S. Department of Education, National Center for Educational Statistics, 1999.

(2) According to the National Telecommunications and Information Administration of the Department of Commerce, 36.6% of the U.S. population have personal computers (PCs), 26.3% have modems, and 18.6% have on-line access. See ***Falling Through the Net II: New Data on the Digital Divide***, available from http://www.ntia.doc.gov/ntiahome/net2/falling.html. Released July 1998.

(3) A recent study from the Annenberg Public Policy Center Found that parents in the U.S. are deeply fearful about the Internet's influence on their children while at the same time believing that

the Internet has important and positive educational potential. See Joseph Turow, ***The Internet and the Family:The View from Parents, The View from the Press***, Annenberg Public Policy Center, University of Pennsylvania, May 1999

(4) Lawrence Lessig and Paul Resnick, "The Architectures of Mandated Access Controls," Paper presented at the Telecommunications Policy Research Conference, October 4, 1998. See http://www.si.umich.edu/~prie/tprc/agenda98.html.

(5) PICS is part of a larger effort being managed by the World Wide Web Consortium on metadata, that is, data associated with Web content that represents information about that content in a way that is easy for machines to deal with. Metadata is intended to facilitate searching, helping authors to describe their documents in ways that search engines, browsers and Web crawlers can understand. The approach embodied in PICS has both supporters (e.g., Paul Resnick, "Filtering Information on the Internet", ***Scientific American***, March 1997), and detractors (e.g., Lawrence Lessig, "Tyranny in the Infrastructure", ***Wired***, July 1997).

(6) In this nomenclature, "tools" refer to technological means for protecting children from pornographic and other inappropriate materials on the Internet, while "strategies" refer to actions to promote or enhance such protection that can be taken by key stakeholders in the lives of children, such as parents, teaches, librarians, and federal, state, and local policy makers.

(7) In the non-networked world, such techniques include movie ratings, special (restricted) sections of video and book stores, opaque covers over pornographic magazine covers, reporting to law enforcement officials of suspected child pornographers by photo processing lab personnel, special hours of or channels for broadcast of certain cable TV shows, and so on.

Tentative Project Schedule

Month 1	Meeting 1 Briefings for the committee are open to interested parties.
Month 3	Meeting 2: Workshop #1 for 1_ days; meeting for 1_ days <u>Workshop topics (public workshop)</u> • Patterns of children's use of the Internet • Non-technical options for protecting children on the Internet, including acceptable use policies; parental guidance; safety education (for example) Non-workshop briefings for the committee held during the meeting are open to interested parties. Workshop briefing books (background materials, commissioned papers, workshop papers if available) will be made available to sponsors immediately.
Month 6	Meeting 3: Workshop #2 for 1_ days; meeting for 1_ days <u>Workshop topics (public workshop)</u> • Technical options for protecting children on the Internet, including mechanisms for filtering and age verification (for example) • Operational policy considerations needed to support various technical options Non-workshop briefings for the committee held during the meeting are open to interested parties. Workshop briefing books (background materials, commissioned papers, workshop papers if available) will be made available to sponsors immediately.
Month 7	Workshop #1 summary (including workshop discussions) delivered to sponsor
Month 10	Workshop #2 summary (including workshop discussions) delivered to sponsor
Months 7-10	Regional hearings and site visits for more gathering of information
Month 11	Meeting 4: meeting for 3 days Briefings for the committee are open to interested parties.
Month 13	Meeting 5: meeting for 3 days

Briefings for the committee are open to interested parties.

Month 15 Meeting 6: meeting for 3 days (probably closed meeting)

Month 18 Report release (in pre-publication form); paperless briefings for sponsor in advance of public release.

Months 19-24 Dissemination efforts, including

- Writing of pieces for practitioners (teachers, librarians, parents, IT vendors)
- Issuing final report in book form

Public Law 105-314
Protection of Children from Sexual Predators Act of 1998
Title IX, Section 901

SEC. 901. STUDY ON LIMITING THE AVAILABILITY OF PORNOGRAPHY ON THE INTERNET.

(a) IN GENERAL- Not later than 90 days after the date of enactment of this Act, the Attorney General shall request that the National Academy of Sciences, acting through its National Research Council, enter into a contract to conduct a study of computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet, in order to develop possible amendments to Federal criminal law and other law enforcement techniques to respond to the problem.

(b) CONTENTS OF STUDY- The study under this section shall address each of the following:

(1) The capabilities of present-day computer-based control technologies for controlling electronic transmission of pornographic images.

(2) Research needed to develop computer-based control technologies to the point of practical utility for controlling the electronic transmission of pornographic images.

(3) Any inherent limitations of computer-based control technologies for controlling electronic transmission of pornographic images.

(4) Operational policies or management techniques needed to ensure the effectiveness of these control technologies for controlling electronic transmission of pornographic images.

(c) FINAL REPORT- Not later than 2 years after the date of enactment of this Act, the Attorney General shall submit to the Committees on the Judiciary of the House of Representatives and the Senate a final report of the study under this section, which report shall--

(1) set forth the findings, conclusions, and recommendations of the Council; and

(2) be submitted by the Committees on the Judiciary of the House of Representatives and the Senate to relevant Government agencies and committees of Congress.