Meeting Minutes

B. Habitat Issues - Report of the Habitat Steering Group
C. Salmon Management
1. Sequence of Events and Status of Fisheries.
2. Risk Analysis for Oregon Coastal Coho Plan Amendment.
3. Draft Plan Amendments and Preliminary Draft.

Environmental Impact Statement

4. Comprehensive Review of Hooking Mortality and Encounter Rates.
D. Dungeness Crab Management - Review Status of Legislation and Determine Need for Council Plan
E. Coastal Pelagic Species Management
1. Anchovy Biomass Estimate and Quotas for 1998 - 1999 Season.
2. Draft Plan Amendments.
F. Groundfish Management
1. Status of Federal Regulations and Other Activities.
2. Report of Congressional Hearing.
3. Proposal to Allow Landing of Fish in Excess of Cumulative Limits.
4. Status of Fisheries and Inseason Adjustments.
5. Preliminary Results of Oregon Enhanced Data Collection Project.
6. Draft Plan Amendments.
7. Lingcod and Rockfish Allocation.
8. Stock Assessment Priorities for 1999.
9. Exempted Fishing Permits for Depth-Specific Sampling and ''Fish for Research'' in 1998.
10. Capacity Reduction Program.
G. Administrative and Other Matters
1. Report of the Budget Committee.
2. Status of Legislation.
3. Report on the National Ocean Conference.
4. Appointments to Advisory Groups.
5. Research and Data Needs and Economic Data Plan.
6. Approve September 1998 Agenda.

Advisory Meetings

The Habitat Steering Group meets at 10 a.m. on Monday,June 22, to address issues and actions affecting habitat of fish species managed by the Council.

The Scientific and Statistical Committee will convene on Monday, June 22, at 8 a.m. and on Tuesday, June 23, at 8 a.m. to address scientific issues on the Council agenda.

The Groundfish Management Team will convene on Monday,

June 22, at 8 a.m. to address groundfish management items on the Council agenda.

The Groundfish Advisory Subpanel will convene on Monday, June 22, at 3 p.m. and on Tuesday, June 23, at 8 a.m., and will continue to meet throughout the week as necessary to address groundfish management items on the Council agenda.

The Enforcement Consultants meet at 7 p.m. on Tuesday,June 23, to address enforcement issues relating to Council agenda items.

The Budget Committee meets on Monday, June 22, at 1 p.m., to review the status of the 1998 Council budget and develop a 1999 budget.

Although other issues not contained in this agenda may come before these groups for discussion, in accordance with the Magnuson-Stevens Fishery Conservation and Management Act, those issues may not be the subject of formal action during this meeting. Action will be restricted to those issues specifically identified in the agenda listed in this notice.

Special Accommodations

These meetings are physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Mr. John S. Rhoton at (503) 326–6352 at least 5 days prior to the meeting date.

Dated: June 1, 1998.

Bruce C. Morehead,

Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 98–15027 Filed 6–4–98; 8:45 am]

BILLING CODE 3510–22–F

DEPARTMENT OF COMMERCE

[Docket No. 980422102–8102–01]

RIN 0660–AA13

Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy

AGENCY: National Telecommunications and Information Administration, Department of Commerce.

ACTION: Notice and request for public comment.

SUMMARY: The Department of Commerce, along with the Office of Management and Budget has been asked to report to the President on industry efforts to establish self-regulatory regimes to ensure privacy online and to develop technological solutions to protect privacy. The President also directed the Commerce Department and the Office of Management and Budget to ensure that means are developed to protect children's privacy online. The Department of Commerce requests comments on various aspects of Internet Privacy including the effectiveness of self regulation for privacy. Specifically, the Department of Commerce seeks comment on the staff discussion paper ''Elements of Effective Self Regulation for Protection of Privacy.'' It also asks for responses to specific questions concerning online privacy protection. In addition, the Department seeks input on the specific instances in which government action may be necessary to protect privacy on the Internet.

DATES: Comments must be received by July 6, 1998.

ADDRESSES: Mail written comments to Jane Coffin, Office of International Affairs, National Telecommunications and Information Administration (NTIA), Room 4898, 14th St. and Constitution Ave., NW, Washington, DC. 20230, or email comments to privacy@ntia.doc.gov. Messages to that address will receive a reply in acknowledgment. Comments submitted in electronic form should be in ASCII, WordPerfect (please specify version), or Microsoft Word (please specify version) format. Comments will be posted on the NTIA website at http://www.ntia.doc.gov. Detailed information about electronic filing is available on the NTIA website, *http://www.ntia.doc.gov*. Paper submissions should include three paper copies and a version on diskette in a format specified above.

FOR FURTHER INFORMATION CONTACT: Jane Coffin, NTIA, (202) 482–1890.

SUPPLEMENTARY INFORMATION:

Background

The rapid growth in the use of the Internet, for both personal and commercial purposes, has led to increased public concern about personal privacy. The promise of information technologies—their ability to facilitate the collection, re-use and instantaneous transmission of information—can, if not managed carefully, diminish personal privacy. A Framework for Global Electronic Commerce, issued by the Administration on July 1, 1997, recognizes that it is essential to assure personal privacy in the networked environment if people are to feel comfortable doing business online.

There are a number of statutory or regulatory regimes that continue to apply in an online environment (e.g., the Fair Credit Reporting Act). For Internet industries and commercial activities not covered by statute or regulation, however, the Administration has called on the private sector to develop self-regulatory mechanisms to protect privacy online. The President directed the Department of Commerce and the Office of Management and

Budget to work with the private sector to develop and implement effective, consumer-friendly, self-regulatory privacy regimes. These regimes should enable consumers to choose how their personal information will be used, ensure adoption of and adherence to fair information practices, and provide for prompt, efficient dispute resolution.

The Administration supports private sector efforts to implement effective self-regulatory privacy regimes for the Internet. These include mechanisms for facilitating consumer awareness of privacy principles and the exercise of choice about whether and under what circumstances to disclose personal information online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution. The Administration also anticipates that technology tools will empower consumers to exercise choices about their privacy. If, upon evaluation, this approach proves not to be effective, other government action may be needed.

The Department of Commerce has talked with industry, members of the academic community, public interest groups and the international community to consider what characteristics of a self regulatory program would be necessary to protect privacy effectively. The Department seeks the views of the public regarding the draft discussion paper, ''Elements of Effective Self Regulation for Protection of Privacy'' (''the draft discussion paper'' published below), which proposes the elements that should be present in a self regulation regime that effectively protects privacy online, while encouraging industry to craft methods of implementing those elements that best serve its needs and the needs of its consumers. The Department also seeks comment on issues surrounding self regulation and online privacy. Specifically, the Department seeks information on the following:

1. The discussion paper sets out nine specific characteristics of effective self regulation for privacy: awareness, choice, data security, data integrity, consumer access, accountability, consumer recourse, verification and consequences. Which of the individual elements set out in the draft discussion paper do you believe are necessary for self regulation to protect privacy? To what extent is each element necessary for effective self regulation? What are the impediments and costs involved in fulfilling each element of a self regulatory scheme? What are the competing interests in providing each element? How would the inclusion of each element affect larger, medium sized, and smaller companies? What advantages or disadvantages does each element hold for consumers? What are the challenges faced by companies in providing each element? How do these challenges depend upon the size and nature of the business?

2. The draft discussion paper notes that individual industry sectors will need to develop their own methods of providing the necessary requirements of self regulation. How might companies and/or industry sectors implement each of the elements for self regulation?

3. Please submit examples of existing privacy policies. In what ways do they effectively address concerns about privacy in the information to which they apply? In what ways do they fail?

4. Are elements or enforcement mechanisms other than those identified in the draft discussion paper necessary for effective self regulation for privacy protection? If so, what are they? How might they be implemented? In addition to the fair information practices and enforcement mechanisms stated in the discussion draft, are there other privacy protections or rights essential to privacy protection?

5. Should consumer limitations on how a company uses data be imposed on any other company to which the consumer's information is transferred or sold? How should such limitations be imposed and enforced?

6. Please comment specifically on the elements set out in the draft discussion paper that deal with enforcement (verification, recourse, and consequences) and suggest ways in which companies and industry sectors might implement these. What existing systems and/or organizations might serve as models for consumer recourse mechanisms, and explain why they might or might not be effective? Would a combination of elements from existing systems and/or organizations be effective? How might verification be accomplished? What would constitute adequate verification, i.e., in what instances would third-party verification or auditing be necessary, and in what cases would something such as self certification or assertions that one is ''audit-ready'' suffice? What criteria should be considered to determine the kind of verification that would be appropriate for a company or sector? What constitutes ''reasonable access?'' What are the costs/impediments involved in providing access? What criteria should be considered to determine ''reasonable access'' to information for a company or sector?

7. In the section on consequences, the draft discussion paper states that ''sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion.'' Identify appropriate consequences for companies that do not comply with fair information practices that meet this goal, and explain why they would be effective.

8. What is required to make privacy self regulation effective? Self-regulatory systems usually entail specific requirements, e.g., professional/business registries, consumer help resources, seals of accreditation from professional societies, auditing requirements. What other elements/enforcement mechanisms might be useful to make privacy self regulation effective? How have these enhanced or failed to enhance a self-regulation regime?

9. Self regulation has been used by the business community in other contexts. Please provide examples and comment on instances in which self regulation is used in an industry, profession or business activity that you believe would be relevant to enhance privacy protection. In what ways does self regulation work in these instances? In what ways does it fail? How could existing self-regulatory regimes be adapted or improved to better protect privacy?

10. Please comment on the extent to which you believe self regulation can successfully protect privacy online. Are there certain areas of online activity in which self regulation may be more appropriate than in others? Why?

11. Please comment on the costs business would incur in implementing a self-regulatory regime to protect privacy. How do these costs compare to the costs incurred to comply with legislation or regulation?

12. What issues does the online environment raise for self regulation that are not raised in traditional business environments? What characteristics of a self-regulatory system in a traditional business environment may be difficult to duplicate online? Does the online environment present special requirements for self regulation that are not present in a traditional business environment? Does the traditional business environment have special requirements that are not presented in the online environment? What are these requirements?

13. What experiences have you encountered online in which privacy has been at issue? In what instances has privacy appeared to be at risk? In what instances is it well protected? In what ways have businesses or organizations been responsive to privacy concerns? How difficult have you found it to protect your privacy online? What

circumstances give rise to good privacy protection in a traditional business setting or online?

14. The Administration's A Framework for Global Electronic Commerce cites the need to strike a balance between freedom of information values and individual privacy concerns. Please comment on the appropriate point at which that balance might be struck. What is the responsibility of businesses, organizations or webpages to protect individual privacy? To what extent do these parties have a right to collect and use information to further their commercial interests? To what extent is it the individual's responsibility to protect his or her privacy?

Elements of Effective Self-Regulation for Protection of Privacy

As set forth in A Framework for Global Electronic Commerce, the Clinton Administration supports private sector efforts to implement meaningful, consumer-friendly, self-regulatory regimes to protect privacy. To be meaningful, self-regulation must do more than articulate broad policies or guidelines. Effective self-regulation involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from noncompliance. This paper discusses the elements of effective self-regulatory regimes—one that incorporates principles of fair information practices with enforcement mechanisms that assure compliance with those practices.

A. Principles of Fair Information Practices

Fair information practices form the basis for the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the United States government. In 1980, these principles were adopted by the international community in the Organization for Economic Cooperation and Development's Guidelines for the Protection of Personal Data and Transborder Data Flows.

Principles of fair information practices include consumer awareness, choice, appropriate levels of security, data integrity, and consumer access to their personally identifiable data. While the discussion that follows suggests ways in which these principles can be implemented, the private sector is encouraged to develop its own ways of accomplishing this goal.

1. Awareness. At a minimum, consumers need to know the identity of the collector of their personal information, the intended uses of the information, and the means by which they may limit its disclosure. Companies are responsible for raising consumer awareness and can do so through the following avenues:

- *Privacy policies.* Privacy policies articulate the manner in which a company collects, uses, and protects data, and the choices they offer consumers to exercise rights in their personal information. On the basis of this policy, consumers can determine whether and to what extent they wish to make information available to companies.
- *Notification.* A company's privacy policy should be made known to consumers. Notification should be written in language that is clear and easily understood, should be displayed prominently, and should be made available before consumers are asked to provide personal information to the company.
- *Consumer education.* Companies should teach individuals to ask for relevant knowledge about why personal information is being collected, what the information will be used for, how it will be protected, the consequences of providing or withholding information, and any recourse they may have. Consumer education enables consumers to make informed decisions about how they allow their personal data to be used as they participate in the information economy. Consumer education may be carried out by individual companies, trade associations, or industry public service campaigns.

2. Choice. Consumers should be given the opportunity to exercise choice with respect to whether and how their personal information is used, either by businesses with whom they have direct contact or by third parties. Consumers must be provided with simple, readily visible, available, and affordable mechanisms—whether through technological means or otherwise—to exercise this option. For certain kinds of information, e.g., medical information or information related to children, affirmative choice by consumers may be appropriate. In these cases companies should not use personal information unless its use is explicitly consented to by the individual or, in the case of children, his or her parent or guardian.

3. Data Security. Companies creating, maintaining, using or disseminating records of identifiable personal information must take reasonable measures to assure its reliability for its intended use and must take reasonable precautions to protect it from loss, misuse, alteration or destruction. Companies should also strive to assure that the level of protection extended by third parties to whom they transfer personal information is at a level comparable to its own.

4. Data Integrity. Companies should keep only personal data relevant for the purposes for which it has been gathered, consistent with the principles of awareness and choice. To the extent necessary for those purposes, the data should be accurate, complete, and current.

5. Consumer Access. Consumers should have the opportunity for reasonable, appropriate access to information about them that a company holds, and be able to correct or amend that information when necessary. The extent of access may vary from industry to industry. Providing access to consumer information can be costly to companies, and thus decisions about the level of appropriate access should take into account the nature of the information collected, the number of locations in which it is stored, the nature of the enterprise, and the ways in which the information is to be used.

6. Accountability. Companies should be held accountable for complying with their privacy policies.

B. Enforcement

To be effective, a self-regulatory privacy regime should include mechanisms to assure compliance with the rules and appropriate recourse to an injured party when rules are not followed. Such mechanisms are essential tools to enable consumers to exercise their privacy rights, and should, therefore, be readily available and affordable to consumers. They may take a variety of forms and businesses may need to use more than one depending upon the nature of the enterprise and the kind and sensitivity of information the company collects and uses. The discussion of enforcement tools below is in no way intended to be limiting. The private sector may design the means to provide enforcement that best suit its needs and the needs of consumers.

1. Consumer recourse. Companies that collect and use personally identifiable information should offer consumers mechanisms by which their complaints and disputes can be resolved. Such mechanisms should be readily available and affordable.

2. Verification. Verification provides attestation that the assertions businesses make about their privacy practices are true and that privacy practices have been implemented as represented. The nature and the extent of verification depends upon the kind of information

with which a company deals—companies using highly sensitive information may be held to a higher standard of verification. Because verification may be costly for business, work needs to be done to arrive at appropriate, cost-effective ways to provide companies with the means to provide verification.

3. Consequences. For self-regulation to be effective, failure to comply with fair information practices should have consequences. Examples of such consequences include cancellation of the right to use a certifying seal or logo, posting the name of the non-complier on a ''bad-actor'' list, or disqualification from membership in an industry trade association. Non-compliers could be required to pay the costs of determining their non-compliance. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may be liable for deceptive practices and subject to action by the Federal Trade Commission or appropriate bank or financial regulatory authority.

Shirl Kinney,

Deputy Assistant Secretary and Administrator.

[FR Doc. 98–15063 Filed 6–4–98; 8:45 am]

BILLING CODE 3510–60–P

DEPARTMENT OF COMMERCE

Patent and Trademark Office

Patent Term Extension

ACTION: Proposed collection; comment request.

SUMMARY: The Department of Commerce (DOC), as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to comment on the continuing information collection, as required by the Paperwork Reduction Act of 1995, Public Law 104–13 (44 U.S.C. 3506(c)(2)(A)), and by the Patent and Trademark Office (Office) in the performance of its statutory functions of processing applications for patent term extension as required by the Hatch-Waxman Act, 35 U.S.C. 156.

DATES: Written comments must be submitted on or before August 4, 1998.

ADDRESSES: Direct all written comments to Linda Engelmeier, Departmental Forms Clearance Officer, Department of Commerce, Room 5327, 14th and Constitution Avenue, NW, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Requests for additional information should be directed to the attention of Karin L. Tyson, at the Special Program Law Office, Office of the Deputy Assistant Commissioner for Patent Policy and Projects, Washington DC 20231, by telephone at (703) 305–9285 or by facsimile transmission to (703) 308–6916.

SUPPLEMENTARY INFORMATION:

I. Abstract

The Patent and Trademark Office (Office), together with the Secretary of Health and Human Services and the Department of Agriculture administers the Hatch-Waxman Act, e.g. 35 U.S.C. 156. This Act permits the Office to restore the patent term lost due to certain types of regulatory review by the Food and Drug Administration or the Department of Agriculture. Only patents for drug products, medical devices, food additives, and color additives are eligible for extension. The maximum length that a patent may be extended (the maximum of patent term that may be restored) is five years.

The Hatch-Waxman Act requires that an application for patent term extension be filed with the Office within 60 days of a product (approved product) that was subject to regulatory review receiving permission for commercial marketing or use from the Food and Drug Administration or the Department of Agriculture. Under 35 U.S.C. 156(d)(1), an application for patent term extension must identify the approved product, the patent to be extended, and the claims of the patent that claim the approved product, a method of use of the approved product, or a method of manufacturing the approved product. It must also set forth sufficient information for the Commissioner of the Patent and Trademark Office to determine the eligibility of the patent for extension and to enable the Commissioner and the Secretary of Health and Human Services or the Department of Agriculture to determine the length of extension. In addition, the application for patent term extension must provide a brief description of the activities undertaken by the applicant during the regulatory review period with respect to the approved product and the significant dates of these activities. If the information supplied is not sufficient for the Commissioner to determine the eligibility of the patent for extension, the rights that will be derived from the extension, or the period of extension, the Commissioner may regard the application as informal and the applicant may provide a response, addressing any deficiencies. In addition, the Commissioner may require additional information; for example, to identify the holder of the regulatory approval or to elect a single patent for extension. An applicant may file a written declaration of withdrawal of an application for patent term extension. If a patent is finally determined not to be eligible for patent term extension, an applicant for patent term extension may request reconsideration of this decision.

Under 35 U.S.C. 156(d)(5), an interim extension for a patent may be granted if the regulatory review of a product is in the approval phase (i.e., the regulatory review period referenced in 35 U.S.C. 156(d)(5)(A) has begun), but the approval phase is expected to extend beyond the original expiration date of the patent. An application for interim extension is required to be filed in the period beginning six months and ending fifteen days before the term of the patent is set to expire. An application for interim extension must identify the product subject to regulatory review, the Federal Statute which requires its review, the patent for which interim extension is sought, including each claim of the patent which claims the product under regulatory review or a method of using or manufacturing the product, and information to enable the Commissioner to determine eligibility for extension under 35 U.S.C. 156(a)(1), (a)(2) and (a)(3). In addition, an application for interim extension must provide a brief description of the activities undertaken by the applicant during the applicable regulatory review period to date and the significant dates applicable to such activities. If the information supplied is not sufficient for the Commissioner to determine the eligibility of the patent for interim extension or the rights that will be derived from the interim extension, the Commissioner may regard the application as informal and the applicant may provide a response, addressing any deficiencies. In addition, the Commissioner may require additional information.

Under 35 U.S.C. 156(e)(2), an interim extension may be granted if the term of a patent for which an application for patent term extension has been submitted under 35 U.S.C. 156(d)(1), and which is eligible for extension, would expire before a certificate of extension is issued.