Network Working Group	J. Morris	
Internet-Draft	CDT	
Intended status: Informational	H. Tschofenig	
Expires: April 21, 2011	Nokia Siemens Networks	
	B. Aboba	
	Microsoft Corporation	
	J. Peterson	
	NeuStar, Inc.	
	October 18, 2010	

TOC

Policy Considerations for Internet Protocols
draft-morris-policy-cons-00.txt

Abstract

Without doubt the Internet infrastructure developed far beyond the expectations of the original funding agencies, architects, developers, and early users. The society's current use and expectations often lead to the need to take the economical and political context in which technology is deployed into consideration.
This document aims to make protocol designers aware of the public policy-related questions that may impact standards development. This document contains questions, as opposed to guidelines or strict rules that should in all cases be followed. This document provides a framework for identifying and discussing questions of public policy concern and serves as an umbrella for related policy documents.

Status of this Memo

Table of Contents

1. Introduction

TOC

This document suggests public policy questions that the authors believe should be considered and possibly addressed within the IETF when it is working on new or revised standards or protocols. This document offers questions to be considered, rather than guidelines to be followed. These questions are somewhat similar to the "Security Considerations" section required in IETF documents.

This document is inspired by and directly modeled on RFC 3426 [RFC3426] (Floyd, S., “General Architectural and Policy Considerations,” November 2002.), entitled "General Architectural and Policy Considerations" and published by the Internet Architecture Board (IAB) in November 2002. In RFC 3426, the IAB raises architectural questions that should be considered in design decisions, without asserting that there are clear guidelines that should be followed in all cases. This document attempts to follow in the spirit of RFC 3426 by raising questions to be considered without asserting that any particular answers must be followed.

This document is motivated by the recognition that technical design decisions made within the IETF and other standards bodies can have significant impacts on public policy concerns. One well known and in the meanwhile historical example of this possible impact can be found in the standardization efforts around IPv6 on Ethernet networks. [RFC2464] (Crawford, M., “Transmission of IPv6 Packets over Ethernet Networks,” December 1998.), published in December 1998, specified that the interface identifier of an IPv6 address was constructed in a way that it uses the unique MAC address associated with the Ethernet interface adapter. After the publication of RFC 2464, a significant policy concern arose because the use of the unique and unchangeable MAC address would significantly reduce a user's ability to conduct private and/or anonymous communications using IPv6. The IETF responded to those concerns by publishing RFC 3041 [RFC3041] (Narten, T. and R. Draves, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6,” January 2001.) entitled "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" in January 2001. Privacy concerns relating this aspect in IPv6 still exist today.

The goal of this document is that potential public policy impacts of technical design decisions will be identified and considered during the initial design process. Some would refer to this approach as "privacy by design". This type of policy consideration already happens in many cases within the IETF, but not in any systematic way or with any assurance that public policy concerns will be identified in most cases. We will provide some examples throught this document.

The goal of the document is not to suggest that the IETF should "do" policy in the sense of intentionally conducting extensive debates on public policy issues. However, many of the actions taken within the IETF have an impact on public policy concerns. This document seeks to encourage the IETF to acknowledge those times when a design decision might affect a policy concern, so that the community can make a reasoned decision on whether and how to address the concern in the particular situation.

Public policy concerns often cannot be avoid: Some beneficial technologies might have secondary harmful impacts, and the benefits may outweigh the harms. More generally, some technologies (such as those that facilitate government surveillance) might intentionally compromise a public concern such as privacy. Similarly, the inherent goal of some technologies (such as those that discriminate among traffic to provide assured levels of quality of service) might simultaneously be viewed by some as beneficial and by others as harmful.

In all of these cases, there may well be good reasons to develop the technology notwithstanding the asserted harms to a policy concern. The main goal of this document is simply to suggest that impacts on a public concern should not happen without clear recognition of the impacts, and without appropriate consideration of whether it is possible to minimize harmful impacts while still meeting the design requirements.

---

2. Scope

TOC

This document cannot possibly predict and identify all possible societal impacts of future IETF protocol and architectural design decisions. It does try, however, to identify a broad range of possible public policy impacts that experience suggests are most likely to arise.

There are two broad categories of public policy impacts that this document does not seek to cover with any thoroughness. First, this document does not articulate the full range of concerns raised by traditional security problems in the network. The IETF is already appropriately focused on security issues, and those in the Security Area are well able to identify and articulate the types of technical design decisions that can lead to security problems. Many of the privacy concerns highlighted in this document raise related security concerns.

Second, this document does not attempt to identify the enormous range of positive societal impacts that flow from network technology. The vast majority of the work of the IETF -- from the introduction of an entirely new method of Internet use to the fine tuning of an existing routing protocol -- yields concrete and important social benefits. This document does not discuss these positive benefits, but takes as a given

that technology proposals will not advance within the IETF unless at least some portion of the community views the proposals as beneficial. This document is by no means an exhaustive list of public policy concerns that relate to the Internet. This draft has instead focused on policy issues that the authors believe are most likely to arise in the IETF context. In addition, the views on public policy varies among countries and cultures to a certain degree.

---

3. Terminology

TOC

This document will use a limited number of defined terms, which admittedly will not be precisely applicable in all situations:
TECHNOLOGY shall refer to a technical standard or innovation being considered within the IETF, whether it is a "new" technology or standard or a modification to an "old" technology or standard.
END USER shall refer to the user at one or the other end of a network communication, or an automated or intelligent proxy for a user located at the end of the communication. Thus, a concern over, for example, the privacy of the End User would be applicable in cases where a client-side application communicated on behalf of an End User. In some contexts, a corporation or other organized collection of human users might stand in the role of an End User. In some but not all contexts, a communication might be from one End User to another End User; in other context, a communication might be between a Service Provider (defined below) and an End User.
ACCESS PROVIDER shall refer to the entity that most directly provides network access to an End User or Service Provider. In the case of End Users on the public Internet, a Access Provider will often be an Internet Service Provider that provides dedicated or dial-up network access. In other cases a Access Provider might be a company providing access to its employees, or a university providing access to its students and faculty.
SERVICE PROVIDER shall refer to an entity (human, corporate or institutional) that provides or offers services or content to End Users over the network (regardless of whether charges are sought for such services or content). Thus, for example, a web site would be viewed as a Service Provider.
A given entity (such as a company offering content on the web) might be viewed as an Access Provider (vis-a-vis its employees), as an End User (vis-a-vis the ISP from which it obtains network access), and as a Service Provider (vis-a-vis End Users elsewhere on the Internet).
TRANSIT PROVIDERS shall refer to one or more entities that transport communications between the Access Providers at either end of a communication. Transit Providers are often thought to transport packets of communications without regard to their content (other than, of

course, their destination), but increasingly some Transit Providers may handle traffic differently depending on the type of traffic.
THIRD PARTY shall refer to any individual or entity other than End Users, Access Providers, Service Providers, and Transit Providers. For a given communication, Third Parties could include, for example, governments seeking to execute lawful interceptions, hackers seeking to interfere with or intercept communications, or in some situations entities that provide, under contract, content or functionality to a Service Provider (such as, for example, an entity that serves advertisements for insertion in a web page).
In some cases the distinction between a Transit Provider and a Third Party may blur, if the Transit Provider manipulates or discriminates among traffic based on characteristics such as its content, sender, or receiver. Similarly, the line between a Service Provider and a Third Party may blur as more service functions are contracted out.

---

4. Potential Public Policy Concerns

TOC

Below are brief discussions of common categories of public policy concern that might be raised by technologies developed by the IETF. The discussions are not intended to present comprehensive analyses of the policy concern, but are intended to assist in identifying situations in which the concern is implicated and should be considered.

4.1. General Comments

TOC

The fundamental design principles of the Internet, including openness, interoperability, and the end-to-end principle, have themselves been critical contributors to the value of the Internet from a public policy perspective. Thus, as a first rule of promoting healthy public policy impacts, the IETF should continue to maintain and promote the architectural goals that it has historically pursued.
Because of this congruence between architectural values and public policy values, many of the design considerations in RFC 3426 [RFC3426] (Floyd, S., “General Architectural and Policy Considerations,” November 2002.), "General Architectural and Policy Considerations" directly promote an Internet that is supportive of good public policy values. As one of many examples, Section 12.1 of [RFC3426] (Floyd, S., “General Architectural and Policy Considerations,” November 2002.) discusses the value of user choice, and quotes [CWSB02] (Clark, D., Wroslawski, J., Sollins, K., and R. Braden, “Tussle in Cyberspace: Defining Tomorrow's Internet,” 2002.) to say that "user empowerment is a basic building block, and should be embedded into all mechanism

whenever possible." User choice is a fundamental public policy concern, discussed more below.
[CWSB02] (Clark, D., Wroslawski, J., Sollins, K., and R. Braden, “Tussle in Cyberspace: Defining Tomorrow's Internet,” 2002.), titled "Tussle in Cyberspace: Defining Tomorrow's Internet," is itself a valuable exploration of the intersection between technology design and public policy concerns. A key premise of [CWSB02] (Clark, D., Wroslawski, J., Sollins, K., and R. Braden, “Tussle in Cyberspace: Defining Tomorrow's Internet,” 2002.) is that "different stakeholders that are part of the Internet milieu have interests that may be adverse to each other, and these parties each vie to favor their particular interests." Many of the "tussles" that [CWSB02] (Clark, D., Wroslawski, J., Sollins, K., and R. Braden, “Tussle in Cyberspace: Defining Tomorrow's Internet,” 2002.) analyzes are situations in which public policy considerations should be assessed in making design decisions. More broadly, [CWSB02] (Clark, D., Wroslawski, J., Sollins, K., and R. Braden, “Tussle in Cyberspace: Defining Tomorrow's Internet,” 2002.) provides to technology designers a conceptual framework that recognizes the existence of "tussles" and seeks to accommodate them constructively within a design.

4.2. Content Censorship and Control

TOC

As used here, the concept of censorship can encompass both governmental and private actions.

4.2.1. Government Censorship

TOC

[Editor's Note: Add more references in an upcoming version of the draft.]
"Censorship" is most commonly thought of as government-imposed control or blocking of access to content. Many believe that as a matter of public policy, censorship should be minimized or avoided. For example, in May 2003 the Council of Europe stated in its "Declaration on freedom of communication on the Internet" that "Public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers." [COE03] (Council of Europe, “Declaration on freedom of communication on the Internet,” May 2003.). But not all censorship is viewed by all as contrary to public policy. In November 2002 in [COE02] (Council of Europe, “Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems,”

November 2002.), the same Council of Europe specifically endorsed government regulation of "hate speech" on the Internet.
Harder to identify are technologies not intended for content control but which can be used to censor or restrict access to content. Any technology that creates or permits bottlenecks or choke-points in the network, through which significant traffic must pass, increases the risk of censorship. Governments seeking to censor content or restrict access to the Internet will exploit network bottlenecks (albeit often bottlenecks created by network topology not technology standards).

4.2.2. Private Control of Content

TOC

Governments are not the only entities that attempt to restrict the content to which Internet users have access. In some cases Access Providers (commonly Internet Service Providers) seek to control the content available to their customers. Some do so with full knowledge and consent of the customers (to provide, for example, a "family friendly" online experience). Others, however, favor certain content (for example, that of contractual business partners) over competing content, and do so without the clear understanding of their customers. Whether such private content control is contrary to public policy will turn on a host of specific considerations (including notice and alternative choice), but undeniably such content control raises policy concerns. These policy concerns are commonly phrased in terms of discrimination among content, and are discussed more fully in the next section.

4.3. Discrimination Among Users and Content

TOC

In a simplistic conception of the early Internet, all traffic of any kind was broken into packets and all packets were treated equally within the network. This idea has promoted a broad and strong perception of equality within the Internet -- one class of traffic will not take priority over other classes, and a lone individual's packets will be treated the same as a large corporation's packets.
Any technology that moves away from this notion of equality -- even technologies that are clearly beneficial -- raise significant public policy questions, including "who controls the preferential treatment," "who qualifies for it," "will it require additional expenditure to obtain it," and "how great a disparity will it create."
Thus, for example, quality of service and content distribution networks both raise questions about what and who will be favored, whether the rough equality of the Internet will be lost, and whether the

financially strong will come to dominate the Internet and make it less useful for the less well off.
The concern over discrimination addresses both discrimination based on identity of user, and on type of traffic. Content distribution networks enable, for example, individual web sites able to afford the CDN services to be delivered more quickly than competing web sites that are not able to afford such services. In contrast, a core focus of quality of service efforts is on the need to provide enhanced levels of service to some types of traffic (e.g., Internet telephony).
Concern about discrimination does not suggest that technologies that handle certain categories of traffic more efficiently should never be pursued. The concern, however, may in some cases suggest that an efficiency enhancement be structured so as to be available to the broadest classes of traffic or users.

4.4. Competition and Choice

TOC

Critical elements of the Internet's development and success have been the ability to create new and innovative uses of the network, the relative ease in creating and offering competitive services, products, and methods, and the ability of Internet users to choose from a range of providers and methods. Anything that reduces innovation, competition, or user choice raises significant public policy concerns. Indeed, the need for competition and user choice is perhaps greater now than in earlier days of the Internet. There is a greater divergence today in the interests and agendas of users and service providers than in the past, and that divergence makes it more important that users be able to choose among service providers (in part to seek providers that they trust the most).
[CWSB02] (Clark, D., Wroslawski, J., Sollins, K., and R. Braden, “Tussle in Cyberspace: Defining Tomorrow's Internet,” 2002.)
extensively addresses the important need for competition and user choice, and provides detailed suggestions and guidelines for Internet designer to consider.

4.5. User Consent

TOC

A familiar public policy concern over user consent focuses on the use of personal data (as discussed more fully below under "Privacy"). The usage here, however, has a broader meaning: the consent (or lack of consent) of a user regarding an action or function executed by or within the network.
Many actions performed using IETF protocols require the specific initiation by a user, and the user's consent can fairly be assumed.

Thus, if a user transmits a request using SIP, the Session Initiation Protocol, it is safe to assume that the user consents to the normal handling and execution of the SIP request.
Other actions performed using IETF protocols are not initiated by a user, but are so inherently a part of normal network operations that consent can be assumed. For example, if in the middle of the network certain packets are slowed by congestion, it is safe to assume sufficient consent for congestion control mechanisms and rerouting of the packets.
Uncertainty about consent arises, however, in areas where IETF protocols can be viewed as deviating from some conception of "normal." A simple example relates to the evolution of caching, where as caching of various types of data became the norm, there emerged a need to be able to set flags to prevent caching, which in a sense can be thought of as a form of negative consent.
Middle boxes and other functions that deviate from the historic "norm" -- the end-to-end principle -- also can raise issues of consent. For example, Section 3 of [RFC3238] (Floyd, S. and L. Daigle, “IAB Architectural and Policy Considerations for Open Pluggable Edge Services,” January 2002.), titled "IAB Architectural and Policy Considerations for Open Pluggable Edge Services," explores a range of consent and data integrity issues raised by the OPES protocol proposals. As that analysis makes clear, the consent issue is not necessarily confined to the consent of the client in a client/server transaction, but may also involve the consent of the server to an action undertaken on the request of the client.

4.6. Internationalization

TOC

[RFC3426] (Floyd, S., “General Architectural and Policy Considerations,” November 2002.) calls on protocol designers to ask the key question about "Internationalization":

> "Where protocols require elements in text format, have the possibly conflicting requirements of global comprehensibility and the ability to represent local text content been properly weighed against each other?"

[RFC3426] (Floyd, S., “General Architectural and Policy Considerations,” November 2002.) explores the significant challenges raised by the need to balances these conflicting goals, and raises the possibility that the historic preference for the use of case-independent ASCII characters in protocols may need to change to accommodate a broader set of international languages.

4.7. Accessibility

TOC

The concept of "accessibility" addresses the ability of persons with disabilities to use the Internet in general and the full range of applications and network functions that are commonly available to persons without disabilities.

The W3C Web Accessibility Initiative (WAI) Technical Activity illustrates the concern and explains that a focus on accessibility is needed "to ensure that the full range of core technologies of the Web are accessible . . . . Barriers exist when these technologies lack features needed by users with visual, hearing, physical, cognitive or neurological disabilities, or when the accessibility potential in the technology is not carried through into the Web application or Web content. For instance, in order for a multimedia presentation to be accessible to someone who is blind, the markup language for the presentation must support text equivalents for images and video; the multimedia player used must support access to the text equivalents; and the content author must make appropriate text equivalents available. These text equivalents can then be rendered as speech or braille output, enabling access to the content regardless of disability or device constraints."

Many policy concerns about accessibility relate specifically to the user interfaces used by applications, and as such these concerns generally fall outside of the province of the IETF. But in the Applications Area and to a lesser extent elsewhere within the IETF, some design decisions could ultimately constrain the accessibility of applications based on IETF protocols.

The W3C's WAI initiative reflects a very well developed and comprehensive analysis of the technical and design issues raised by accessibility concerns.

[Editor's Note: A future version of this document will add text about multi-media emergency services support here.]

4.8. Personal Privacy

TOC

Individual privacy concerns are often divided into two components: First, "consumer privacy" (also termed "data protection") commonly addresses the right of individuals to control information about themselves generated or collected in the course of commercial interactions. Second, "privacy rights vis-a-vis the government" addresses individuals' protection against unreasonable government intrusions on privacy, including the interceptions of communications. In the IETF context, a third category of privacy concern -- privacy against private interception of or attacks on data or communications -- is largely covered by the IETF's focus on security considerations.

Although security considerations are crucial to privacy considerations, "consumer privacy" and "privacy vis-a-vis the government" raise significantly different issues than traditional security considerations. With security considerations, a key focus is on maintaining the privacy of information against unauthorized attack. Other forms of privacy, however, focus not on unauthorized access to information, but on the "secondary use" of information for which access was (at least temporarily) authorized. The question often is not "how can I keep you from seeing my information" but "how can I give you my information for one purpose and keep you from using it for another." The questions raised in Section 5 (Questions about Technical Characteristics or Functionality) above do not differentiate between the different categories of privacy, because for most purposes within the IETF, technologies that create risk for one type of privacy likely also create risk for other types of privacy. Once a potential privacy concern is identified, however, the different types of privacy concern may present different public policy considerations. Indeed, the policy considerations may well be in tension -- a technology that permits a lawful governmental interception of a communication may also increase the risk of unlawful private interception.
Privacy considerations are too numerous and multifaceted to be adequately addressed in this document. For a more detailed treatment please refer to [I-D.morris-privacy-considerations] (Aboba, B., Morris, J., Peterson, J., and H. Tschofenig, “Privacy Considerations for Internet Protocols,” October 2010.).

4.9. Privacy vis-a-vis the Government

TOC

Although privacy is internationally recognized as a human right, most governments claim the authority to invade privacy through the following means, among others:

- *interception of communications in real-time;
- *interception of traffic data (routing information) in real-time;
- *access to data stored by service providers, including traffic data being stored for billing purposes; and
- *access to data stored by users.

These means of access to communications and stored data should be narrowly defined and subject to independent controls under strict standards. Real-time interception of communications should take place only with prior approval by the judicial system, issued under standards at least as strict as those for police searches of private homes.

In 1999, in the "Raven" discussions, the IETF considered whether it should take action to build wiretapping capability into the Internet. Ultimately, as detailed in [RFC2804] (IAB and IESG, “IETF Policy on Wiretapping,” May 2000.), the community decided that an effort to build wiretapping capability into the Internet would create significant and unacceptable security risks.

---

5. Questions about Technical Characteristics or Functionality

TOC

In this section we list questions to ask in designing protocols. The issues raised by the questions are discussed in more depth in Section 5 (Questions about Technical Characteristics or Functionality). We are not suggesting that each of these questions requires an explicit answer -- some questions will be more relevant to one design decision than to another.

There is not a one-to-one correspondence between the questions listed in this section and the discussions in Section 5 (Questions about Technical Characteristics or Functionality). Instead, for each group of questions listed below, there are one or more references to later substantive discussions.

Some of the questions will be easy to answer for a given technology. Others will require creative thinking to assess whether a proposed technology might be misused to achieve a result not intended by the technology proponents.

This document addresses the most common and well-known areas of public policy concern, focusing on areas most likely to arise in the IETF context.

5.1. Bottlenecks, Choke-Points and Access Control

TOC

*Would the Technology facilitate any bottlenecks or choke-points in the network through which significant amounts of particular types of traffic must flow?

*Would the Technology permit a Third Party (including a government) to exert control over End Users' use of the Internet as a whole?

*Would the Technology permit a Transit Provider or Third Party (including a government) to exert control over the use of particular content, functionality, or resources?

*Would the Technology permit an Access Provider or Service Provider to exert control over particular content, functionality,

or resources, other than that known by the End User to be controlled by the Access Provider or Service Provider?

*Would the Technology permit Third Party (including a government) to require that particular content or functionality be confined (or "zoned") into, or excluded from, any particular subpart of the Internet (such as a particular Global Top Level Domain)?

> See discussions of "Content Censorship and Control", "Personal Privacy", "Discrimination Among Users and Content", "Competition and Choice", and "User Consent."

5.2. Alteration or Replacement of Content

TOC

*Would the Technology permit a Third Party to alter any of the content of a communication without (a) the express instruction or consent of the Service Provider and the End User, or (b) the knowledge of the Service Provider or the End User?

> See discussions of "Content Censorship and Control" and "User Consent."

5.3. Monitoring or Tracking of Usage

TOC

*Would the Technology permit the monitoring or tracking by a Third Party of the use of particular content, functionality, or resources?

> See discussion of "Personal Privacy."

5.4. Retention, Collection, or Exposure of Data

TOC

*Would the Technology require or permit the retention of any information about individual packets or communications, or individual End Users, either (a) beyond the conclusion of the immediate network or communications event, or (b) for longer than a reasonably brief period of time in which a communications "session" can be concluded?

*Would the Technology permit the reading or writing of any file on an End User's computer without the explicit knowledge of the End User?

*Would the Technology permit or require that information other than location and routing information (such as, for example, personal information or search terms) be made a part of a URL or URI used for a communication?

*Would the Technology permit or require that personal or confidential information be made available to any Third Party, Transit Provider, or Access Provider?

> See discussion of "Personal Privacy."

5.5. Persistent Identifiers and Anonymity

TOC

*Would the Technology require or permit the association of a persistent identifier with a particular End User, or a computer used by one or more End Users?

*Would the Technology reduce the ability of a content provider to provide content anonymously?

*Would the Technology reduce the ability of an End User to access content or utilize functionality anonymously?

> See discussion of "Personal Privacy."

5.6. Access by Third Parties

TOC

*Would the Technology permit any Third Party to have access to packets to and from End Users without the explicit consent of the End Users?

*Would the Technology permit or require any Third Party to store any information about an End User, or an End User's communications (even with the knowledge and consent of the End User)?

> See discussions of "Personal Privacy" and "User Consent."

5.7. Discrimination among Users, or among Types of Traffic

TOC

*Would the Technology require or permit an Access Provider or Transit Provider to provide differing levels of service or functionality based on (a) the identity or characteristic of the End User, or (b) the type of traffic being handled?

*Would the Technology likely lead to a significant increase in cost for basic or widely-used categories of communications?

*Would likely implementations of a new mode of communication require such a financial or resource investment so that the mode would effectively not be available to individuals, or small or non-profit entities?

> See discussion of "Discrimination Among Users and Content."

5.8. Internationalization and Accessibility

TOC

*Would the Technology function with the same level of quality, ease of use, etc., across a broad range of languages and character sets?

*Would the likely implementations of the Technology be as useful to mainstream End Users as to non-mainstream End Users (such as, for example, End Users with disabilities)?

*Would the Technology likely reduce the ability of non-mainstream End Users (such as, for example, End Users with disabilities) to utilize any common application or network functions?

> See discussions of "Internationalization" and "Accessibility."

5.9. Innovation, Competition, and End User Choice and Control

TOC

*Would the Technology reduce the ability of future designers to create new and innovative uses of the Internet, or new methods to accomplish common network functions?

*Would the Technology likely reduce the number of viable competitive providers of any common application or network functions?

*Would the Technology likely reduce the ability of small or poorly- funded providers to compete in the provision of any common application or network functions?

*Would the Technology likely reduce the number or variety of methods available to the End User to accomplish common application or network functions?

*Would the Technology likely reduce the level of control the End User can exercise over common application or network functions?

> See discussion of "Competition and Choice."

---

6. Security Considerations

TOC

This document does not propose any new protocols or changes to old protocols, and therefore does not involve any security considerations in that sense. Many of the privacy issues discussed here also raise security issues, but this document is not intended to be a comprehensive look at security issues.

---

7. IANA Considerations

TOC

This document does not require actions by IANA.

---

8. Acknowledgments

TOC

We would like to thank Alan B. Davidson for his work on a prior version of this document.

---

9. References

TOC

9.1. Normative References

TOC

[RFC2316]	Bellovin, S., “Report of the IAB Security Architecture Workshop,” RFC 2316, April 1998 (TXT, HTML, XML).
[RFC4101]	Rescorla, E. and IAB, “Writing Protocol Models,” RFC 4101, June 2005 (TXT).
[RFC3426]	Floyd, S., “General Architectural and Policy Considerations,” RFC 3426, November 2002 (TXT).
[RFC2464]	Crawford, M., “Transmission of IPv6 Packets over Ethernet Networks,” RFC 2464, December 1998 (TXT, HTML, XML).
[RFC3041]	Narten, T. and R. Draves, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6,” RFC 3041, January 2001 (TXT).
[RFC3238]	Floyd, S. and L. Daigle, “IAB Architectural and Policy Considerations for Open Pluggable Edge Services,” RFC 3238, January 2002 (TXT).
[RFC2804]	IAB and IESG, “IETF Policy on Wiretapping,” RFC 2804, May 2000 (TXT).

9.2. Informative References

TOC

[I-D.morris-privacy-considerations]	Aboba, B., Morris, J., Peterson, J., and H. Tschofenig, “Privacy Considerations for Internet Protocols,” draft-morris-privacy-considerations-00 (work in progress), October 2010 (TXT).
[CWSB02]	Clark, D., Wroslawski, J., Sollins, K., and R. Braden, “Tussle in Cyberspace: Defining Tomorrow's Internet,” In Proc. ACM SIGCOMM , http://www.acm.org/sigcomm/sigcomm2002/papers/tussle.html, 2002.
[OECD]	Organization for Economic Co-operation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” available at (September 2010) , http://www.oecd.org/EN/document/0,,EN-document-0-nodirectorate-no-24-10255-0,00.html, 1980.
[COE02]	Council of Europe, “Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems,” available at (October 2010) , http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/Racism_on_internet/PC-RX(2002)24E-1.pdf, November 2002.
[COE03]	

	Council of Europe, “Declaration on freedom of communication on the Internet,” available at (October 2010) , http://cm.coe.int/stat/E/Public/2003/adopted_texts/declarations/dec-28052003.htm, May 2003.

Authors' Addresses

TOC

	John B. Morris, Jr.
	Center for Democracy and Technology
	1634 I Street NW, Suite 1100
	Washington, DC 20006
	USA
Email:	jmorris@cdt.org
URI:	http://www.cdt.org
	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo 02600
	Finland
Phone:	+358 (50) 4871445
Email:	Hannes.Tschofenig@gmx.net
URI:	http://www.tschofenig.priv.at
	Bernard Aboba
	Microsoft Corporation
	One Microsoft Way
	Redmond, WA 98052
	US
Email:	bernarda@microsoft.com
	Jon Peterson
	NeuStar, Inc.
	1800 Sutter St Suite 570
	Concord, CA 94520
	US
Email:	jon.peterson@neustar.biz