Privacy: An Internet Society Membership Survey

November 2010

Internet Society
InternetSociety.org
info@isoc.org

Galerie Jean-Malbuisson, 15
CH-1204 Geneva
Switzerland

Tel: +41 22 807 1444
Fax: +41 22 807 1445

1775 Wiehle Ave.
Suite 201
Reston, VA 20190, USA

Tel: +1 703 439 2120
Fax: +1 703 326 9881

Introduction

Privacy and data protection issues have increasingly gained prominence in Internet governance discussions. Indeed, one of the five themes of the Internet Governance Forum 2010 is "Openness, Security and Privacy", and a number of workshops are devoted to these issues. Yet, the concept of privacy, opinions on what challenges are posed by the digital environment and approaches to protection of personal data vary from country to country, and within communities. Thus, it is important to understand these differences when developing Internet policy and laws concerning privacy.

The Survey

In May 2010, the Internet Society invited its members (Chapters, Organisational, and Global) to participate in a survey on privacy and data protection.

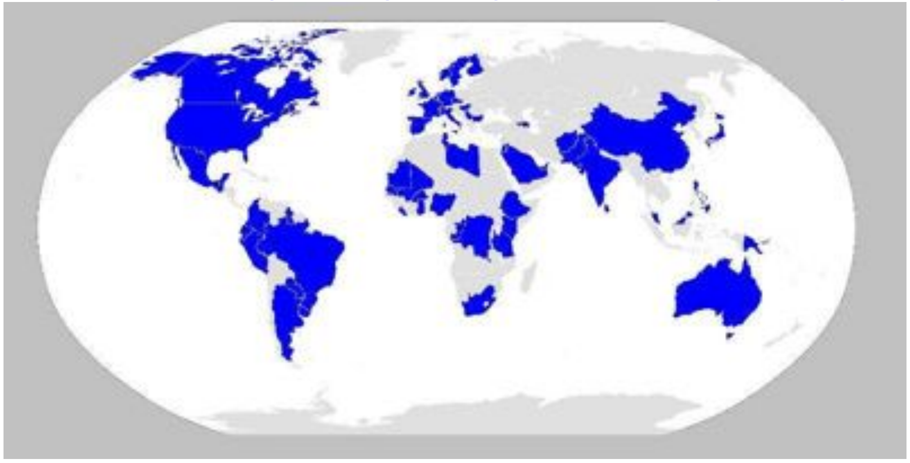
The objective of the survey was to gather information from across our broad membership around the world, specifically focusing on how issues of privacy and data protection are dealt with in their regulatory environment.

While our principal objective was to gather information to help guide the Internet Society's privacy efforts, we also hope that the information provided by our members will help inform international and regional dialogue on these issues.

The survey tool recorded 604 responses (from 100 countries), indicating broad global interest in privacy in the online environment, however only 153 responses (from 65 countries) contained actionable information. This was not unexpected as the questions were designed for people with particular interest or knowledge regarding privacy and data protection in their country. Further, in relation to many countries, information was only provided by one or a few respondents. Accordingly, we consider the sample too small to be representative: we do not seek to draw particular conclusions about issues concerning particular countries. Nonetheless, we note that even a single voice from a country can be informative.

We asked the respondents to identify the country for which their answers are applicable. The map below displays the countries of the 153 responses referred to above.[i]

Internet Society Privacy Survey: Responses by Country



The Report

This report is divided into five parts:

I: Definitions of Privacy, Personal Data and Personal Information

II: The Present

- Are privacy and data protection high priority issues?
- What are stakeholders doing to address these issues?
- What could/should they do?

III: The Future

- The top five emerging challenges in the digital environment
- Suggestions and principles to address the top five emerging challenges

IV: Laws, Regulations, Principles, Guidelines and other Resources

V: Internet Society Members' Activities

and has the following annexures:

- A: Legal definitions of "personal data" and "personal information"
- B: Privacy and data protection priority issues
- C: What stakeholders are doing to address these issues
- D: What stakeholders should/could be doing to address these issues
- E: The top five emerging challenges
- F: Laws, rules, principles or guidelines for the protection of personal data
- G: Places to look for guidance
- H: Internet Society member activities

I: Definitions: Privacy, Personal Data and Personal Information

The concept "privacy" underpins policies and laws concerning the protection of personal data/information, yet there appears to be limited international consensus on what privacy means. A lack of consensus on what privacy means in the online environment may hamper efforts to harmonize national data protection approaches to this issue.

To investigate country-level concepts of "privacy", we asked Internet Society members:

> *Does your government, or the government where your chapter or organisation is based, have a working definition for "privacy" (online or offline or both)?*

A respondent from Sweden said:

> *The Data Protection Authority states on its web site that: There is no commonly agreed definition, privacy is an inner characteristic different between individuals. A common interpretation is 'the right to be left in peace'. The 'right to have one's own personal individuality and inner sphere respected and not subjected to insulting treatment' is another.*[1]

A respondent from Ghana said:

> *Privacy is about the Security of your data, computers, network system which include the Internet. In securing the Internet, there will be the need to install firewalls to protect the organization's Internet (i.e. Intranet) against intruders.*

A respondent from the USA said:

> *… There is no overall definition accepted nationally. Some people define privacy as the right to control information about one's self.*

A respondent from Canada said:

> *Privacy may be defined as the right of the individual to determine when, how, and to what extent he or she will release personal information.*

A respondent from India said:

> *The Indian Cyber Laws defines privacy as follows: Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others.*

[1] http://www.datainspektionen.se/ordlista/#P

The terms “personal data” and “personal information” frequently occur in privacy and data protection laws, but the precise scope of those terms varies. Further, some countries have identified special categories of data which they term “sensitive data”.

To explore this issue further, we asked Internet Society members:

> *Do the laws in your country define "personal data" and/or "personal information"?*

A summary of selected legal definitions provided by the respondents is set out in **Annexure A**.

II: The Present

Are privacy and data protection priority topics of discussion?

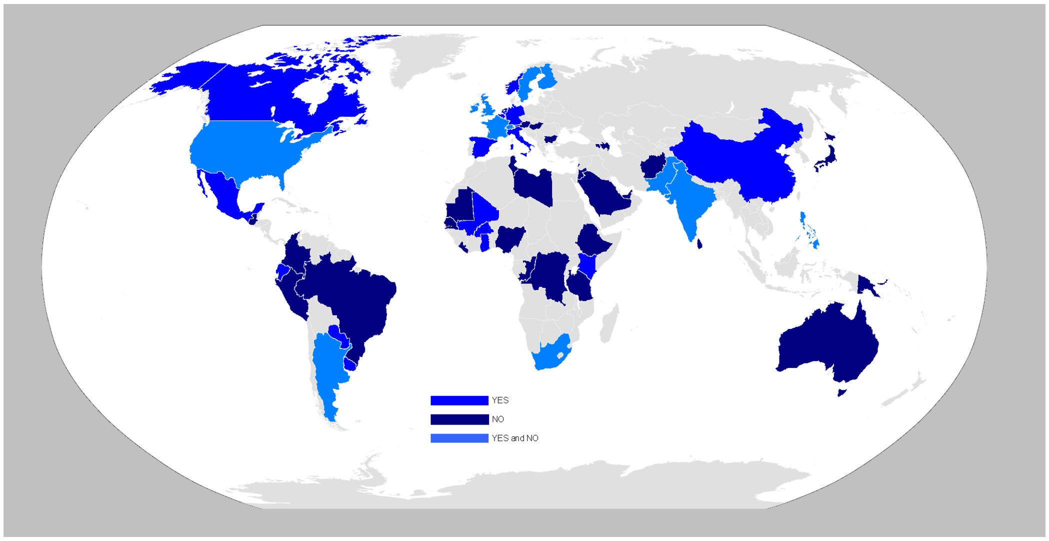
We asked Internet Society members:

> *Are “privacy” and/or the protection of “personal data” currently high priority topics of discussion in your country?*

153 respondents answered this question. 46.1% of those respondents (70) answered “yes”. The remainder answered “no” (67 - 44.1%) or “unknown” (16 - 9.1%).

In some cases, respondents from the same country gave different answers. For example: one or more respondents in the USA responded “yes” while one or more other respondents responded “no”. The responses are illustrated in the map below.

Are privacy and data protection high priority topics of discussion?



For those respondents who answered "yes", we asked those persons to identify the particular topics under discussion. A summary of their responses appears in **Annexure B**. The three most common issues identified by respondents were:

- social media (mentioned by respondents from all regions except Africa and the Middle East);
- particular categories of personal data (e.g. medical and financial data); and
- privacy and data protection laws (i.e. existing laws, new laws etc.).

The responses generally appear to point to the need for more or stronger laws for privacy and data protection.

What are stakeholders doing to address these issues?

As a follow-up question, we asked Internet Society members to describe what stakeholders are doing in their country to address those issues. 110 respondents answered this question. Details of their responses are set out in **Annexure C**.

A number of respondents consider that relevant stakeholders in their countries are not doing anything or are not doing enough to address privacy issues, particularly government and policymakers.

Interestingly, a respondent from a country without privacy and data protection laws observed that the private sector is more careful about the use of personal information and attributed those practices to the prevalence of business people that come from countries with such laws.

Another respondent expressed the view that businesses in their country engaged in supplying data protection products were "trying to scare people" so that they would buy their products.

Although it was our intention to elicit information regarding activities being undertaken by stakeholders to address particular local issues concerning privacy and data protection, we also received some interesting opinions regarding the attitudes and approaches taken by Internet users. Opinions varied, even within countries. For example, in India, opinions regarding Internet users' attitudes to privacy ranged from: they are not aware; mostly unaware; concerned; to very concerned.

We have extracted some of the responses below:

Azerbaijan	• Very few people understand or are willing to use the Internet as they feel at risk with personal data
Canada	• Varies from proactive to apathetic
Finland	• Small very active groups exist but mainstream is expecting government to take care of it
Germany	• They are somewhat scared, and therefore, many refrain from using services like internet banking • Waiting for help

Ghana	• Normally users will ensure they are following the required Internet Security policies and regulations
India	• Not aware of the issues involved • Mostly unaware of the latest developments • Are concerned • Very concerned and active
Italy	• Agreement or disagreement on personal data treatment (whether must be explicitly authorised or not)
Japan	• Discussion ongoing online, but not much on the non-online world
Netherlands	• Do not care that much apart from some active groups • Scattered objections to excessive personal data collection • They do not care if there is some financial benefit, discount or whatever. “I have nothing to hide” is often said. But awareness is growing.
Pakistan	• Most users do not have any interest • Worried
Papua New Guinea	• Starting to have some awareness
Philippines	• Some concern, but little discussion • Average computer users rarely know about privacy, its implication to them and other things
Saudi Arabia	• Most users do not know that their data is insecure inside and outside the Kingdom
Senegal	• Take care of their personal data and warn the Administration about any violation or abuse
South Africa	• Tend to trust organisations with their data
Spain	• Not organised to defend their interests • Education and awareness campaigns on the right to protect privacy
Sri Lanka	• Most users are still not very aware of the importance of their privacy and personal data
Sweden	• Concerned about privacy while publishing private intimate personal details on blogs and social media sites
Switzerland	• Should inform themselves how their data is being used and processed
Tanzania	• Many users may have abstract idea

The Gambia	• Are concerned
UK	• Despairing • Participating in civil society organisations which care about their privacy
USA	• Ambivalence • Users are becoming more and more aware (thanks to Google, Facebook, et. al.) that their data is being collected, aggregated, and mined more than they had known • Are poorly informed about choices and many have no idea where to look for guidance • Deleting information from Facebook • Willingly surrendering personal data in exchange for "special" offers, generally worthless in nature • Efforts to understand how the confluence of threat and behaviour of others affects the individual user, and what to do about it • Clueless • Putting too much information on the Internet • Worried about the privacy of their data and personal info

What should stakeholders be doing to address these issues?

We also asked Internet Society members whether they have any suggestions as to what stakeholders should be doing to address these issues. 131 respondents answered this question. 67.2% of those respondents (88) answered "yes".

Respondents from a number of countries suggested that stakeholders should do more to raise awareness about privacy and data protection. For some countries, where there are no privacy or data protection laws, respondents suggested that such laws should be developed.

Some respondents provided suggestions to improve compliance with existing laws (e.g. through sanctions or compliance measurement criteria). Others proposed a more global approach to data protection or an approach modelled on laws in another region (e.g. the European Union).

Some of the more specific suggestions included:

- Opt-in by default
- Define what is public and what is private
- Build privacy features into the design of new systems
- Remove cost barriers for access to information under Freedom of Information law
- Tailored user-managed privacy settings for data
- Require the private sector to meet the same minimum standards as government
- Limit collection and access to data

- Uniform adoption of last-login timestamp for services accessed via online login

Looking at the responses from a regional perspective, we observed that *education and awareness raising* was mentioned in all regions. Respondents from all regions except Europe made suggestions which could be characterised as *formulation of policies, laws and guidelines*. In Europe, the suggestions regarding polices, laws and guidelines seemed to be principally focused on *implementation and enforcement*. These are the four main categories of suggestions we identified from the responses for each region:

	Africa and the Middle East	**Asia and the Pacific**	**Europe**	**Latin America**	**North America**
Education and awareness raising	✓	✓	✓	✓	✓
Formulate policies, laws and guidelines	✓	✓		✓	✓
Implementation and enforcement			✓		✓
Consultation and dialogue	✓		✓	✓	

A summary of the responses (by region and country) is set out in **Annexure D**.

III: The Future

The top five emerging challenges relating to "privacy" and the protection of "personal data" in the digital environment

The respondents to the survey were asked to identity what they consider to be the top five emerging challenges relating to “privacy” and the protection of “personal data” in the digital environment. 152 respondents identified at least one emerging challenge. These are summarised in detail in **Annexure E**.

It is difficult to succinctly and comprehensively express the multitude of emerging challenges identified by the respondents in a few paragraphs. However, we have attempted to do this by category (below). The breadth of identified challenges is itself indicative of the complexity of issues associated with privacy and data protection in the digital environment.

Not unexpectedly, the identified issues are not the same in all regions. For example:

- there was generally more granularity in the responses provided from countries where there are already well-established privacy and data protection laws.
- there appears to be more emphasis in Asia on "security" as an emerging challenge.
- in Africa, increased connectivity was identified as an emerging challenge.

From the responses, we identified the following categories of challenges (listed alphabetically). Note: These categories are simply a subset of the topics raised and do not reflect a consensus view:

- **Competing issues:** privacy vs. convenience; privacy vs. access to public services; privacy vs. security; privacy vs. law enforcement (e.g. of IPR rights); privacy vs. identification; anonymity vs. access to information regarding interests and proximity information
- **Connectivity:** increased connectivity; increased online transactions; increased devices
- **Culture:** developing and having a culture of personal data protection
- **Data durability:** difficulty correcting false accusations on websites; information online is there "forever"; getting personal information removed
- **Digital Identity:** identity fraud and theft; validating identity without compromising personal data; lack of anonymity; protection of integrity of identity
- **Economics of privacy:** value of privacy to individuals; value of personal data to businesses; impact on trade where countries are perceived as unsafe destinations for data; high profit margins for illicit use of personal data
- **Ownership, control and responsibility:** exchanging data without informing the individual and/or not seeking their permission or consent; personal responsibility for own data
- **Regulatory:** lack of a legal framework; enacting laws; complexities of regulating online privacy settings for individuals; inadequate focus on auditable procedures for data retention; global availability of data but national laws; insufficient government interest and/or expertise; potential legislation to ban encryption; lack of resources
- **Scope:** determining what is "personal data"
- **Surveillance:** e.g. by government; Deep Packet Inspection; data collected by search engines being used by government and enterprise to profile users
- **Technology:** implementing technology to support privacy; data aggregation, correlation and analysis tools; tools for speed of transmission; cloud computing; no standard data format; IP addresses; lack of a cohesive set of tools to ensure privacy; lack of encryption

- **Transborder:** providing data protection across national borders; lack of international cooperation; inconsistent standards across countries (particularly developed vs. developing); lack of global approaches
- **Transparency, knowledge and understanding:** insufficient or inadequate understanding of privacy, personal data, data visibility (i.e. knowing where data is stored); default settings; insufficient proactive examination of usage terms before sign-up
- **Unauthorised access and use:** illegal and/or unauthorised access to personal data (e.g. via phishing, hacking, malware, botnets, spam, spyware, careless installation of file-sharing software etc. and/or insufficient security)
- **Users:** Inappropriate use of social media; need for adequate protection of children

and classes of personal data that were considered particularly challenging:

- Geo-location data
- Medical data
- Financial data
- Credit card data
- National ID cards
- Biometric data

Note: The list of categories is not exhaustive. Please refer to **Annexure E** for further details of the emerging challenges identified by respondents (by region).

Suggestions or principles to address the top five emerging challenges

We also invited Internet Society members to provide suggestions or principles to address the top five emerging challenges they identified regarding "privacy" and the protection of "personal data" in the digital environment. Almost all of the responses proposed actions or principles to strengthen the protection of personal data and/or increase individuals' awareness of the importance of protecting their personal data. However, one respondent expressed the view that society should place less emphasis on individual privacy.

A summary of the responses is set out below, separated into various categories (listed alphabetically):

Business online

- The right to keep personal details private should be a basic human right that cannot be signed away by a waiver or "click-thru" agreement
- Assign the burden of protection of personal data to the organisation not the consumer
- Companies should be required to justify the intended use of personal data, in a regular review process
- When personal data is collected, the online service provider should provide a "statement of intended use" describing how the details will be used, selected from a list of approved statements
- Any privacy arrangement (right to use data) between a customer and a goods or services provider should expire within a specified period (e.g.

6 months) or require renewal when there are material changes to the provider

- Encourage business to protect data

Certification and insurance

- Establish a widely publicised “trust mark” awarded by an independent body to websites and social media that:
  - satisfies some defined minimum privacy protection standards
  - provides good and secure default privacy settings
  - clearly explains the effect of the privacy policy and privacy settings
- Establishment of a privacy mark system
- Creation of “Privacy Insurance”

Cloud computing and ISPs

- Keep private data out of the cloud behind protective electronically protected firewalls that should be provided by ISPs
- ISPs should not communicate their customers’ personal data to collecting societies

Educate and raise awareness

- Build a targeted program to sensitise individuals in developing countries regarding the risks of disclosure of identity information online
- Help stakeholders and ordinary individuals to understand the dangers involved and how best to defend themselves
- Provide seminars and education in rural areas
- Educate users and the general public on the importance of privacy and personal data
- Launch a global campaign highlighting online privacy issues
- More workshops
- Raise individual awareness generally and regarding precautionary steps needed to self-protect

General principles

- Opt-in rather than Opt-out privacy settings
- The default for new applications using personal data should be “opt in”
- Privacy online is no different than privacy online
- Users should protect their personal data
- Users should be responsible for their disclosure of personal data
- Privacy protection must not conflict with principles of net neutrality
- Users must control collection and use of personal data
- The data owner must always authorise data access and use (in advance)
- Online service providers should not make the sharing of personal data a prerequisite for access to their services
- "Sensitive" personal data should not be available
- The default for new applications using personal data should be “opt in”

Institutional

- An international organisation dedicated to personal data protection should be created
- Work together in a multistakeholder environment
- Seek input from the International Association of Privacy Professionals (IAPP)
- Create regional and global committees for privacy and protection of personal data
- The views of users and the general public should be taken into account when developing policies on privacy
- Local governments should remind their citizens of the risks of disclosing personal information online and provide them with information regarding services which allow users to block access to particular websites
- Software and hardware “back doors” should not be available to governments

International and local

- Develop international requirements for the handling of personal data
- Strive for local or continent-based solutions as international solutions may not be politically achievable
- Global harmonisation of essential privacy principles in relation to social media and "cloud" computing

Laws, guidelines and principles

- Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data
- European Data Protection laws
- Facebook Users’ Bill of Rights
- Fair Information Practice Principles
- Generally Accepted Privacy Principles
- Good Data Protection Acts (e.g. UK) and principles like confidentiality, integrity and availability
- International Standards on the Protection of Personal Data and Privacy (the Madrid resolution)
- Madrid Privacy Declaration
- OECD Guidelines on Privacy and Transborder Data Flows
- Safe Harbor Privacy Framework (US-EU) and (US-Switzerland)

Laws, implementation and enforcement

- Promote and develop methodology and compliance measurement criteria
- Stricter rules, regulations and penalties
- Provide strong personal data protection
- Introduce laws covering privacy and data protection
- Laws should not allow automatic opt-in or automatic renewal of services
- Enforcement agencies should examine the practices of the ISP with access to users’ data
- Criminal penalties for misuse of personal data for marketing or harassment

- Encourage policymakers to formulate policy on privacy and leave implementation to the relevant actors
- Improve enforcement legislation and in courts
- Give people channels to denounce abuse
- Mandatory reporting of breaches from private companies
- Update law to reflect new technology
- Educate politicians so they are able to pass appropriate laws

Other

- Consider alternatives for transmission of personal data (e.g. post rather than email)

Scope of privacy

- Develop differentials in privacy
- Corporate/Commercial privacy
- Personal privacy

Spyware, malware and hacking

- Ban spyware and hacking (through laws)
- Involve the companies offering security solutions to stop spread of spyware and hacking

Technical solutions

- The IETF should develop protocols for the verification, sharing and securing of personal data which are independent of local definitions
- Develop systems which allow individuals to tag personal data with a privacy policy that can be enforced by an automatic enforcement scheme (example provided: www.springerlink.com/content/l2u4488247134753)
- Privacy by design should not be optional
- Uniform adoption of last-login time-stamp for online accounts users login
- Fully customize MS Windows to avoid unattended use of the account system and related accounts of the operating system
- Restrict RFID applications to the Internet of Things. No embedded RFID in personal user applications

Understand the issues

- Conduct a field study
- Set up a taskforce to address the issues
- Case studies on the damage caused by invasion/violation of privacy

WHOIS

- Restrict access to Whois data to law enforcement and to authorised registries and registrars for the purposes of network management

IV: Laws, Regulations, Principles, Guidelines and Other Resources

Laws, regulations, principles and guidelines

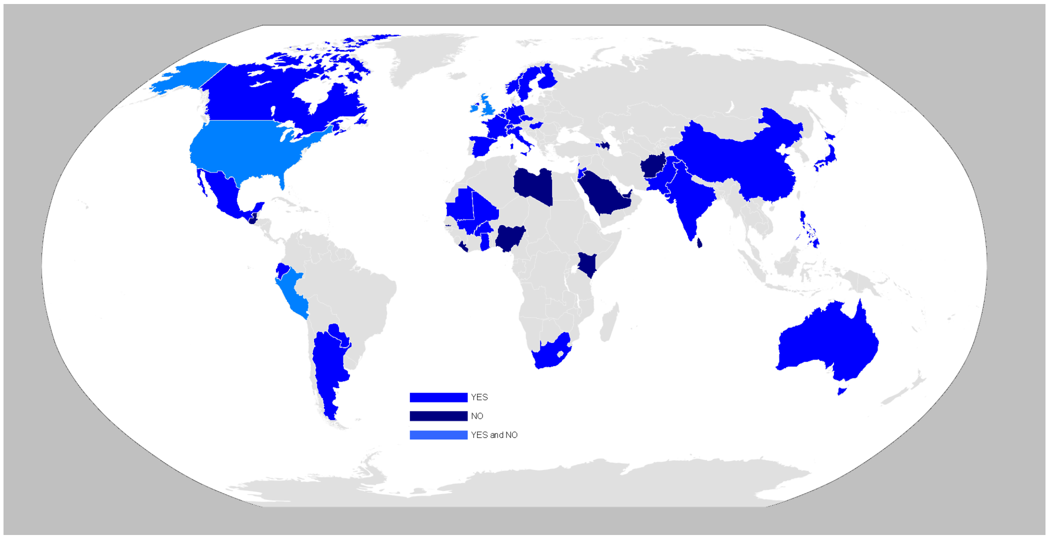
We asked our Internet Society members:

> *Does your country have any specific laws, rules, principles, guidelines, or other regulations that apply to the protection of "personal data" and/or "personal information"?*

to help us to compile a list of relevant laws, regulations etc. and identify those countries which do not have privacy and/or data protection laws. 153 respondents answered this question. 61.2% of those respondents (94) answered "yes". The remainder answered "no" (16.4%) or "unknown" (22.4%).

In some cases, respondents from the same country gave different answers. For example: one or more respondents in the USA responded "yes" while one or more other respondents responded "no". The responses are illustrated in the map below.

Does your country have any specific laws, rules, principles or guidelines for the protection of personal data?



A summary of the responses provided by the respondents who answered "yes" is set out in **Annexure F**.

We also asked Internet Society members:

> *Does your organisation have any specific guidelines or codes of conduct that apply to the protection of "personal data"?*

152 respondents answered this question. 42.1% of those respondents (64) answered "yes". The remainder answered "no", "not applicable" or "unknown". Of those respondents that answered "yes", some said they:

- have internal guidelines or policies;
- were in the process of developing them;
- had adopted external guidelines or policies; or
- followed the relevant laws.

Places to look for guidance on these issues

We asked Internet Society members:

> *Where would you look for guidance in addressing these issues in an online context?*

97 respondents answered this question, identifying a fairly wide range of resources. A summary list of these resources is set out is set out in **Annexure G**.

V: Internet Society member activities in the area of privacy and data protection

Discussions

We asked Internet Society members:

> *Has your chapter or organisation devoted time to the discussion of "privacy" as it relates to "personal data" in the past year?*

152 respondents answered this question. 23.7% of those respondents (36) answered “yes”. The remainder answered “no”, “not applicable” or “unknown”.

One respondent from Asia said:

> *We have conducted an awareness program on child security where we discussed privacy and personal data. As expected, most people in the audience did [not place] any importance to (sic) privacy, except in the most loosely defined manner, i.e. do not peep into my bedroom or bathroom. The concept of personal data was alien to them.*

This statement illustrates that the concept of privacy is not the same all over the world. The privacy topics identified by the respondents included:

- Development of data protection laws and regulations
- Implementation of new data protection laws
- Review of existing data protection laws
- Balancing privacy and free speech
- Whois
- Social media
- Internet security
- Monitoring and surveillance by ISPs and telecommunication providers
- Privacy awareness raising
- Internet safety and standards
- Privacy issues with new web applications and other products

- Data protection and privacy on the Internet
- Trust
- Identity
- Privacy issues associated with school examinations
- Authentication
- Privacy in public institutions
- Privacy defaults in social media
- Business rules
- Legal consequences
- Smart Grid
- Global Climate Situation Room Collective Intelligence Platform
- Child security
- Shared/not shared information

Current and future activities

We asked Internet Society members:

> *Are you, your chapter or your organisation involved in current work undertaken by international (e.g. OECD), regional (e.g. European Commission) or national forums (e.g. US FTC) on the review of privacy laws or guidelines?*
>
> *Do you, your chapter or your organisation have any activities planned that relate to "privacy" and/or the protection of "personal data" this year?*

A summary of activities identified by the respondents is set out in **Annexure H**. The identified activities are being, or will be. undertaken by Internet Society members through their local chapter, individually or through their organisation.

Concluding Remarks

We would like to thank all our members who participated in this survey. The responses to this survey are helpful in identifying the wide-ranging views on privacy and will be useful in guiding the Internet Society's future work in this area.

Comments, views or ideas reported in this document are not necessarily held or endorsed by the Internet Society.

Questions regarding this report may be directed to isoc@isoc.org. Please include the words "Privacy Survey" in the subject of field of your email.

About the Internet Society

The Internet Society is a non-profit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. With offices near Washington, D.C., and in Geneva, Switzerland, it is dedicated to ensuring the open development, evolution, and use of the Internet for the benefit of people throughout the world. More information is available at: http://InternetSociety.org

[i] Also included in the maps in this report, but not visible, are the Cook Islands and the Republic of Nauru.