ANNEXURES PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

ANNEXURE A to PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

LEGAL DEFINITIONS OF "PERSONAL DATA" AND/OR "PERSONAL INFORMATION"

Armenia	Personal data: any data recorded on medium containing facts, events and circumstances about the person, in a form that allows or may allow to identify the person[1]
Burkino Faso	Constitue une donnée à caractère personnel, toute information qui permet, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques, notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques propres à leur identité physique, psychologique, psychique, économique, culturelle ou sociale. *Constitutes a personal data, information that can, in any form whatsoever, directly or indirectly, the identification of individuals, in particular by reference to an identification number or more factors specific to their physical identity , psychological, mental, economic, cultural or social.* (translated using Google Translate)
Germany	Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person *Personal information is information that of personal or material Circumstances of a specific or identifiable natural person* (translated using Google Translate)
Japan	"Personal information" means the information about a living individual, which contains the name, the date of birth and/or any other descriptions by which a specific individual can be identified (including information that can be easily collated with other information so that a specific individual can be identified)[2]
Lebanon	The draft law defines personal information as all data related to a physical person and which can be used to identify this person in a direct or indirect way including by comparing data from different sources or the intersection of such information
Mexico	Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual. Personal Data: Any information concerning an identified or identifiable individual Sensitive personal data: Those personal data involving the most intimate

[1] Unofficial translation of the *Law of the Republic of Armenia on Personal Data 2002* - http://www.parliament.am/law_docs/071102HO422eng.pdf

[2] *Act Concerning Protection of Personal Information* (Japan Law No. 57, 2003) – Article 2

	sphere of the data subject, or misuse of which can lead to discrimination or entails a serious risk to him. In particular, sensitive issues are those that may reveal racial or ethnic origin, health status, present and future, genetic information, religious, philosophical and moral beliefs, union membership, political views and sexual preference.
Pakistan	The law of personal data protection define personal data and sensitive data. The sensitive data is considered as a classification of personal data. Personal Data: Any kind of information refers to human beings or companies, which can be or would be indentified. Sensitive data: personal data which disclose racial or ethnic origin, political opinions, religious, moral or political thoughts, labour union affiliation or information regarding health and/or sexual aspects or behaviours
Senegal	Senegalese law 2008-12 Article 4: Personal Data is any information relating to a person identified or directly/indirectly identifiable by reference to an identification number or to one or more specific elements related to his physical, physiological, genetic, psychological, cultural, social or economic description.
Spain	Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. Personal information means any information concerning an identified or identifiable natural persons.
Sweden	Personal Data Act Section 3: Personal data = All kinds of information that directly or indirectly may be referable to a natural person who is alive. Section 13: Sensitive Personal Data is personal data that reveals a) race or ethnic origin, b) political opinions, c) religious or philosophical beliefs, or d) membership of a trade union e) such personal data as concerns health or sex life.
UK	Any information relating to an identified or identifiable natural person ('data subject') An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
USA	Definitions vary in detail In general, this is data/information (1) that identifies or is characteristic of an individual and (2) to which the individual has an interest in restricting or a legal right to restrict access to specific other persons. Examples: social security number, annual income, credit card numbers, academic "grades", medical information

ANNEXURE B to PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

ARE PRIVACY AND DATA PROTECTION PRIORITY TOPICS OF DISCUSSION?

Continent	Topics being discussed
Africa and the Middle East	• Possible amendment to the national data protection law • New draft data protection law • In the National ICT Policy • Internet Fraud (i.e. “Sakawa”)/Internet Security/Cybercrime/CERTs
Asia and the Pacific	• Social media • Need for privacy and data protection • Telemarketers • National digital identity • Security
Europe	• Social media • Social networking and privacy • Whether discussion forums should be moderated or not • Privacy on social network sites and online services such as Google • Abuse of personal information that people themselves place on the Internet in Facebook and the like • Business, Medical, Financial, Internet • Medical data/dossier; Medical records now being linked together centrally and with pharmacists' prescription sales • Storage of traveller data through national public transport pass. Storage of patient data through national "ERD" - medical dossier database • Government and industry data leaks (see www.speigel.de) • Wiretapping • Legal intercept of telecommunications • EU data retention law: files on medical status; fingerprints in passport and it’s storage; e-identity; public transport cards. • EU Data Protection Directive • Data Protection Law obligations • Data retention • Signals intelligence • StreetView • Personal threats via mail, blog comments etc. • Privacy in relation to IPR • How anonymity on the Internet is misused • ID cards and the associated database(s) • Identity theft and banking • Digital Economy Bill • Whois • Access to IP addresses as personal data
Latin America	• Federal Data Protection Act 2010 and Federal Institute of Access to Information and Data Protection • Project Digital Mercosur • Social Networks • Identity for Digital Certification
North America	• Social networking • Use of personal data by social media sites, specifically Facebook

Continent	Topics being discussed
	• Whether a definition of privacy rights and corporate responsibility to maintain the privacy of personal information should be codified • Facebook, Google • Homeland security/privacy • Security video cameras • Identity theft • Lost/stolen personal data • Encrypting stored data • See epic.org and EFF • State laws for handling PII • Cybercrime/privacy/Hacking • Privacy of data for websites

Country	Topics being discussed
Argentina	-
Belgium	• Social media and Whois
Burkina Faso	• Possible amendment to the national data protection law
Canada	-
China	• Social media
Ecuador	-
England	-
Finland	• Social networking and privacy • Whether discussion forums should be moderated or not
France	• Business, Medical, Financial, Internet
Germany	• Government and industry data leaks (see www.speigel.de)
Ghana	• Internet fraud (i.e. “Sakawa”)/Internet Security/Cybercrime/CERTs
India	• Need for privacy and data protection. • Telemarketers
Italy	• Wiretapping • Legal intercept of telecommunications
Jordan*	-
Kenya	• New draft data protection law
Mali**	• In the National ICT Policy
Mexico	• Federal Data Protection Act 2010 and Federal Institute of Access to Information and Data Protection
Netherlands	• Privacy in relation to IPR • EU data retention law: files on medical status; fingerprints in passport and it’s storage; e-identity; public transport cards. • Medical data/dossier; Medical records now being linked together centrally and with pharmacists' prescription sales • Storage of traveller data through national public transport pass. Storage of patient data through national "ERD" - medical dossier database
Norway	• EU Data Protection Directive
Pakistan	• National digital identity
Paraguay	• Project Digital Mercosur

Country	Topics being discussed
Philippines	• Security
Spain	• Data Protection Law obligations
Sweden	• Data retention • Signals intelligence • Privacy on social network sites and online services such as Google StreetView • Abuse of personal information that people themselves place on the Internet in Facebook and the like • Personal threats via mail, blog comments etc. • How anonymity on the Internet is misused
Switzerland	-
UK	• ID cards and the associated database(s) • Identity theft and banking • Digital Economy Bill • Access to IP addresses as personal data
Uruguay	• Social Networks • Identity for Digital Certification
USA	• Social networking • Use of personal data by social media sites, specifically Facebook • Whether a definition of privacy rights and corporate responsibility to maintain the privacy of personal information should be codified • Homeland security/privacy • Security video cameras • Identity theft • Facebook, Google • Lost/stolen personal data • Encrypting stored data • See epic.org and EFF • State laws for handling PII. • Cybercrime/privacy/Hacking • Privacy of data for websites

*Starting to become a topic of high priority
**Privacy is mentioned in the document, but no further developments in this area since 2005

ANNEXURE C to PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

WHAT ARE STAKEHOLDERS DOING?

Country	Stakeholder	Action
Afghanistan	Government Policymakers	Ministry of Tele-Communication
Argentina	Enterprise	Acentuar desde las distintas Camaras las practicas y acciones para que este tema sea prioritario Make the issue a priority
Argentina	Government Policymakers	laws and regulations
Argentina	Government Policymakers	An annual seminar made by National Director of Personal Data Protection
Argentina	Media	CXO Community (an online and printed magazine) - news, opinions, seminars
Argentina	Users	Evangelizacion y concienciacion Advocacy and awareness raising
Armenia	Government Policymakers	Cooperation with CERT – police department, project
Australia	Civil society	Privacy advocates: attempts to bring privacy issues to policymakers attention
Azerbaijan	Government Policymakers	ICT Policy still not implemented as yet
Azerbaijan	Users	Very few people understand or are willing to use the Internet as they feel at risk with personal data
Belgium	Government Policymakers	http://www.privacyconference2009.org/home/index-iden-idweb.html
Belgium	Users	http://thepublicvoice.org/madrid-declaration
Burkina Faso	Government Policymakers	Le gouvernement et la Commission informatique et libertés
Canada	Enterprise	Varies from strict compliance to nothing
Canada	Government Policymakers	Active investigations and enforcement ministry
Canada	Users	Varies from proactive to apathetic
China	Enterprise	Follow the law and revert our opinions to the lawmakers and

Country	Stakeholder	Action
		government
China	Government Policymakers	Legislation and enforcement/review of the law
China	Users	Follow the law and revert our opinions to the lawmakers and government
Cook Islands	Enterprise	Improving
Cook Islands	Enterprise	There are no laws, but the private sector are more closed about information about other people and how it is used - mainly because business people here generally originate from countries where there are privacy laws
Cook Islands	Government Policymakers	Nothing
Cook Islands	Government Policymakers	Nothing that specifically addresses personal information or privacy - each government does their own thing
Cook Islands	Users	Stale
Czech Republic	Enterprise	Very rarely as a non-systematic approach
Czech Republic	Government Policymakers	From time to time raised media discussion
Czech Republic	Users	Individually differs very greatly
Ecuador	Government Policymakers	Laws
England	Enterprise	Varies from the tendentious but ineffective to the serious
England	Government Policymakers	Blithering
England	Users	From the naive to the cynical
Ethiopia	Government Policymakers	Trying to formulate policy
Finland	Enterprise	Quite active participation to workgroups, seminars and such
Finland	Government Policymakers	Implementing EU directives to national law, updating regulation, taking in various discussions actively
Finland	Users	Small very active groups exist but mainstream is expecting government to take care of it
France	Enterprise	AFCPD association

Country	Stakeholder	Action
France	Government Policymakers	CNIL
France	Users	Many blogs
Germany	“Internet Geeks”	They are saying "Windows bad, Linux good" and Linux solves all the problems and that is that.
Germany	Enterprise	They are trying to scare people in order to buy their privacy and protection of private data products
Germany	Enterprise	Every company which stores privacy data has to setup a review process and nominate a “data protection responsible person” which has to report directly to governmental data protection agencies
Germany	Government Policymakers	They leave all the statements to Mr Schaar. They don't really do anything else.
Germany	Government Policymakers	Proposal for 'Personal Data Letter' that informs users about the data that is stored about them (realisation unlikely)
Germany	Government Policymakers	Laws, discussions
Germany	Users	They are somewhat scared, and therefore, many refrain from using services like internet banking
Germany	Users	Waiting for help
Ghana	Enterprise	ghNOG, GhNIC and other organization are also partnering with ghCERT to create awareness on Internet Security issues and how some of the incidence can be prevented.
Ghana	Government Policymakers	Ghana Computer Emergency Response Teams (i.e. ghCERT) has been collaborating with the Government agencies and other organization to create awareness on Internet security issues and how some of the security incidences can be prevented
Ghana	ISOC Ghana	ISOC Ghana is partnering with ghCERT to create the necessary awareness on Internet Security issues and how they can be prevented
Ghana	Users	Normally users will ensure they are following the required Internet Security policies and regulations
Guyana	Enterprise	Not aware of any action
Guyana	Government Policymakers	Not aware of any action
Guyana	Users	Not aware of any action
Hungary	Enterprise	Taking into consideration the above laws

Country	Stakeholder	Action
Hungary	Government Policymakers	Awareness of due laws and organisational/personal conditions to enforce those laws
Hungary	Users	Taking into consideration the laws; approaching the due organisational entities (on highest level the ombudsman) in case of malfunctioning or problems with laws
India	Academia	Carry out research
India	Enterprise	Not much discussion
India	Enterprise	Protection of Internet and cyber safety
India	Enterprise	Seminar/ workshops are organised without any co-ordination
India	Enterprise	Guidelines are laid down but still to be implemented
India	Enterprise	Active
India	Enterprise	Implementing policy
India	Enterprise	Formulating policies and do's & don'ts
India	Government Policymakers	Some concern is being shown. Appear not to understand its implications.
India	Government Policymakers	Protection of Internet and cyber safety
India	Government Policymakers	Policies are still in the transformation stage
India	Government Policymakers	Not very active
India	Government Policymakers	Making IT laws
India	Government Policymakers	Nothing
India	Government Policymakers	Forming self-regulatory bodies such as DSCI - http://www.dsci.in
India	Users	Not aware of the issues involved
India	Users	Protection of Internet and cyber safety
India	Users	Are concerned
India	Users	Mostly unaware of the latest developments
India	Users	Very concerned and active
India	Users	Following Act and policy

Country	Stakeholder	Action
India	Users	Take steps to secure their data
India	Users	Following directives as best as they can
Italy	Enterprise	Protection of sensitive data if applicable
Italy	Government Policymakers	Public discussion of new wiretapping rules
Italy	Government Policymakers	Not too much besides proposing legislation to limit legal intercept The Italian authority for the protection of personal data is quite active
Italy	Users	Agreement or disagreement on personal data treatment (whether must be explicitly authorised or not)
Italy	Users	Not too much
Japan	Enterprise	Enforcement of corporate legal and ethical compliance
Japan	Government Policymakers	Enforcement of the applicable laws
Japan	Users	Discussion ongoing online, but not much on the non-online world
Jordan	Enterprise	Implementers
Jordan	Government Policymakers	Initiator
Jordan	Users	Provide feedback
Kenya	Government Policymakers	Drafting relevant legislation
Lebanon	Enterprise	Nothing
Lebanon	Enterprise	Nothing
Lebanon	Government Policymakers	Proposing a very restrictive law
Lebanon	Website hosts	Sometimes publish a privacy policy
Malaysia	Enterprise	Company policy
Malaysia	Government Policymakers	Drafting law/policy and enforcement
Malaysia	Users	Accept and respect the policies
Mali	Enterprise	Health centres are applying ethical measures, and they

Country	Stakeholder	Action
		mentioned some new measures to be applied
Mali	Government Policymakers	Government mentioned some measures on the subject but has done nothing as yet
Mauritania	Enterprise	is not applying the collective agreement
Mauritania	Government Policymakers	Little interest
Mauritania	Users	most affected and associations of trade unions are demanding but nothing happens is managed by businessmen
Mexico	Enterprise	Implementation phase
Mexico	Government Policymakers	Implementation phase
Mexico	Users	Implementation phase
Netherlands	Enterprise	Want access to everything when useful for their business case
Netherlands	Enterprise	Collect less sensitive personal information to optimize target marketing efforts
Netherlands	Enterprise	Comply to government requirements regarding the protection of privacy and personal data
Netherlands	Government Policymakers	Want control of course
Netherlands	Government Policymakers	Maximize the collection of personal data to allow for tighter control of taxes, medical expenses, etc.
Netherlands	Government Policymakers	They implement EU-directives and do not design privacy into big ICT-projects. Some things go well, many things are going the wrong way because of ignorance.
Netherlands	Government Policymakers	For patient dossier, include an opt-out
Netherlands	Users	Do not care that much apart from some active groups
Netherlands	Users	Scattered objections to excessive personal data collection
Netherlands	Users	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.
Nigeria	Enterprise	Seminars
Nigeria	Government Policymakers	Lip service
Pakistan	Enterprise	Planning over paper formatted

Country	Stakeholder	Action
Pakistan	Enterprise	Silent
Pakistan	Enterprise	Nothing
Pakistan	Enterprise	Do their own
Pakistan	Government Policymakers	Planning for better and trustworthy solution of identity threads
Pakistan	Government Policymakers	Some policy making
Pakistan	Government Policymakers	Nothing
Pakistan	Government Policymakers	E-crime law has been prepared but suspended by the government because of several loopholes and lack of clarifications
Pakistan	Government Policymakers	Do nothing for privacy and protection
Pakistan	Users	Unaware which is best
Pakistan	Users	Worried
Pakistan	Users	Most users do not have any interest
Pakistan	Users	Nothing
Papua New Guinea	Enterprise	Adopting their own policies
Papua New Guinea	Government Policymakers	Some discussions
Papua New Guinea	Government Policymakers	Not much
Papua New Guinea	Users	Starting to have some awareness
Paraguay	Enterprise	Banks Association are studying and working on a draft law
Paraguay	Government Policymakers	Working on a draft law
Paraguay	Mercosur Digital	Mercosur Digital is making a case analysis to adapt EU model as well as Mercosur in the working group SGT13
Peru	Enterprise	Not active
Peru	Government Policymakers	Developing law

Country	Stakeholder	Action
Peru	Users	Not active
Philippines	Enterprise	Only data held/used by outsourcing companies
Philippines	Enterprise	Resort to laws and other international standards such as ISO/IEC and others
Philippines	Government Policymakers	Becoming more intrusive, only intends to protect (foreign) data held by outsourcing companies
Philippines	Government Policymakers	They are doing fine though they appear to have been left out especially with Western counterparts
Philippines	Users	Some concern, but little discussion
Philippines	Users	Particularly average computer users rarely knows about privacy, its implication to them and other things
Republic of Congo	Enterprise	Protection of their customers and themselves data
Republic of Congo	Government Policymakers	Promotion of the E Governance and all its implications
Republic of Nauru	Government Policymakers	Nauru Security Development Services Government Office
Saudi Arabia	Government Policymakers	Government only interested in prosecuting cybercrime and ensuring its ability to intercept all email traffic for internal security purposes
Saudi Arabia	Users	Most users do not know that their data is insecure inside and outside the Kingdom
Senegal	Enterprise	Apply decrees and guarantee the privacy of any personal data and sensitive data - advertise the government of any violation
Senegal	Government Policymakers	Define laws and rules and control their application and inform people about their right to have their personal data protected
Senegal	Users	Take care of their personal data and warn the Administration about any violation or abuse
South Africa	Enterprise	Tend to focus on US implementation leads
South Africa	Government Policymakers	Not much
South Africa	Users	Tend to trust organisations with their data
Spain	Enterprise	Not interested in privacy because of the commercial effect
Spain	Government Policymakers	Not much, the public entity in charge the data protection policy has no mean to verify the accomplishment of the law

Country	Stakeholder	Action
Spain	Government Policymakers	APD: Agencia Española de Protección de datos
Spain	Government Policymakers	They have organized workshops and national consultations
Spain	Government Policymakers	Approved a law called LOPD (Ley Organica de Proteccion de Datos)
Spain	Users	Not organised to defend their interests
Spain	Users	Education and awareness campaigns on the right to protect privacy
Sri Lanka	Academia	Universities are working on some supporting roles
Sri Lanka	Enterprise	Different companies have different policies
Sri Lanka	Government Policymakers	Still policy making regarding privacy and personal data is in progress
Sri Lanka	Users	Most users are still not very aware of the importance of their privacy and personal data
Sweden	Enterprise	Trying to comply with vague legislation
Sweden	Enterprise	Supervision of use
Sweden	Government Policymakers	Deferring new legislation until after national election in September 2010
Sweden	Government Policymakers	Overseeing laws, Information
Sweden	Users	Concerned about privacy while publishing private intimate personal details on blogs and social media sites
Sweden	Users	Discussing
Switzerland	Civil society	Pressing for better protection of personal data
Switzerland	Enterprise	Some, like banks, have strict rules, others should to do more to protect personal data
Switzerland	Government Policymakers	Following EC recommendations
Switzerland	Users	Should inform themselves how their data is being used and processed
Tanzania	Enterprise	IT-driven service industry may be at forefront of addressing private information
Tanzania	Government Policymakers	Until now, no known law, policy or regulation

Country	Stakeholder	Action
Tanzania	Users	Many users may have abstract idea
The Gambia	Enterprise	Guess they think about it
The Gambia	Government Policymakers	They are not doing anything
The Gambia	Users	Are concerned
UK	Enterprise	Breaching the Data Protection Act
UK	Enterprise	Registering with the Data Protection Register
UK	EuroDIG	Cross-European dialogue about these issues: http://www.eurodig.org/eurodig-2010/programme/plenary/plenary-2
UK	Government Policymakers	Government seems not to recognise the dangers of a unified electronic database. Nor do they understand the dangers of a single point of failure “brittle” identity database/passport.
UK	Government Policymakers	Assuming that the Data Protection Act is being enforced
UK	Government Policymakers	Implementing and amending the various laws which are already in place
UK	Users	Despairing
UK	Users	Participating in civil society organisations which care about their privacy
Uruguay	Enterprise	Generating internal processes
Uruguay	Government Policymakers	Adapting all laws and regulations to the digital world
Uruguay	Users	Being more conscious
USA	Academia	Privacy advocates in academia are discussing these issues, in classrooms and seminars
USA	Enterprise	Business making misuse of private information
USA	Enterprise	Trying to intrude as much as possible into personal data/information of everyone
USA	Enterprise	Eroding
USA	Enterprise	Most enterprises in the US have a "privacy policy", which is generally posted on their web site. However, corporations keep data much longer than consumers realize. Often, when a user deletes information from a social networking site, the information is not disposed of, merely hidden from the public.

Country	Stakeholder	Action
USA	Enterprise	Very little
USA	Enterprise	Industry coalitions for privacy
USA	Enterprise	Will garner any info to be used for financial gain
USA	Enterprise	A [social media provider] seems to believe they can do whatever they want
USA	Enterprise	Large corporations and industry show support in their own security and definition of public versus private information and data
USA	Enterprise	Aggregating, trading and “losing” as much personal data as possible as fast as possible
USA	Enterprise	Protection mechanisms being developed for telecommunication standards, that is, transmission protection but not data protection standards
USA	Enterprise	Generation of policy to comply with laws
USA	Enterprise	Legal minimum
USA	Enterprise	Developing working solutions
USA	Government Policymakers	Government making it easier to obtain private information - often to protect trademark interests and blind support for “law enforcement”
USA	Government Policymakers	Some trying to enhance protection, some doing the opposite
USA	Government Policymakers	Varied
USA	Government Policymakers	US Congress has begun to investigate the handling of personal information by both Google and Facebook
USA	Government Policymakers	Plenty
USA	Government Policymakers	Draft bills on more comprehensive privacy definitions and protections
USA	Government Policymakers	“Day-lighting” past abuses of individuals info
USA	Government Policymakers	Listening to complaints
USA	Government Policymakers	Regulating industries as to what they can and cannot share
USA	Government Policymakers	New legislation and regulation targeting the inappropriate use or possession of sensitive data

Country	Stakeholder	Action
USA	Government Policymakers	Aggregating and losing citizen data at exponential rates, poor law-making, no real protections
USA	Government Policymakers	Legislation passed
USA	Government Policymakers	Generation of laws and social engineering policies
USA	Government Policymakers	Nothing
USA	Government Policymakers	Talking
USA	Government Policymakers	Discussing regulation and new laws
USA	Users	Users' privacy rights are shrinking - and ISOC should help to educate users and policy makers on how to protect privacy online
USA	Users	Ambivalent
USA	Users	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.
USA	Users	Somewhat little
USA	Users	Are poorly informed about choices and many have no idea where to look for guidance
USA	Users	Deleting information from Facebook
USA	Users	Not as much as they probably should
USA	Users	Willingly surrendering personal data in exchange for "special" offers, generally worthless in nature
USA	Users	Ambivalence
USA	Users	Efforts to understand how the confluence of threat and behaviour of others affects the individual user, and what to do about it
USA	Users	Clueless
USA	Users	Putting too much information on the Internet
USA	Users	Worried about the privacy of their data and personal info

ANNEXURE D to PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

WHAT SHOULD STAKEHOLDERS BE DOING TO ADDRESS THESE ISSUES?

Region	Suggestion

Africa and the Middle East	**Education and awareness raising**
	• Provide people with more information on privacy and data protection
	• Raise awareness by providing training
	• Educate Internet users
	• They should teach privacy in schools and at religious congregations
	• Raise awareness of these issues, by conducting seminars and workshops at different universities/colleges etc.
	• Organise seminars and workshops
	• Stakeholders should familiarise themselves with issues related to protection of personal data
	• The main focus should be on the community since this service is intended for their use and need
	
	Formulate policies, laws and guidelines
	• The government should formulate policy and broadcast it to the people
	• Information Security standards/procedures need to be put in place
	  ○ These should include: i) Development of Information Security Policies ii) Appointment of an officer responsible for Information Security to implement the policies/standards and procedures iii) Information Security Audits
	• Distribute guidelines/templates for data protection that everyone can use
	• Formalise a standard regarding the definition of personal information
	• Laws that address this should be placed under discussion at our parliament.
	  ○ However, the bill regarding this should be raised by someone/organization that is knowledgeable in that area. This is because the parliament may not have the full knowledge as to the details of the issue. Thus, that education should come from a professional in that field of discipline.
	• Adopt guidelines on this issue
	
	Other
	• People should be able to choose whether their data should be public of private
	• Business should encourage the application of the collective agreement structure
	• Start by forming an ISOC chapter

Asia and the Pacific	**Education and awareness raising** • More awareness is needed • More emphasis and education • Engage in public debate. Articles in media. Discussion on TV. • Create awareness among the public at large, particularly youth • More awareness and concern regarding privacy and private data • The government should conduct an awareness workshop so the people are aware of the importance of privacy/data protection • Raise awareness and impose policy with enforcement • Raise awareness among Internet users • Make cyber security a required course for all graduates and computer degree holders

Region	Suggestion
	Consultation, dialogue, research • Government bodies, civil society and relevant industry representatives should conduct a dialog and define the policy for privacy and data protection. In order to define this, a collection of definitions is needed to reach consensus and integrate all the relevant areas as perceived by different stakeholders. • Undertake a more detailed and in-depth analysis of the subject • National level consultations - government and private sector leading to legislation • Study the approaches in other countries, especially North America and Europe • Need to discuss, introduce basic rules and work on evolving a complete solution **Global approach** • There needs to be a global approach to global organisations that pose threats to privacy (e.g. social media) • Full international cooperation to stop abuse of the Internet **Formulate policies, laws and guidelines** • The government should pass a law regarding privacy and data protection • 1. Define the issues 2. Define the basic right to privacy 3. Table regulations 4. Protect privacy with laws 5. Enforce laws with strong penalties • Enact a privacy/data protection law • Legislation on privacy should be enacted • There should be a comprehensive set of policies with international standards. This should be undertaken by the government, regulatory bodies and academia collaboratively. • The government needs to establish a privacy law so that when information of a private nature is divulged then there is some recourse that can be taken to protect the interests of the person concerned • The government should have a unified law and a simple set of rules to help people have a deeper understanding of privacy issues **Other** • Encourage government action through public pressure • Force application of Freedom of Information, at no cost. Finding out information can cost thousands of dollars. • Do something at least • Improve • A one-cent charge on every mail would penalize salvo-spam, and thus indirectly leave no motive for the surreptitious cross-referencing of people's age, interests, politics, liquidity, sexuality, religion, philosophy and skills.
Europe	**Education and awareness raising** • Learn and understand how the Internet works • Help people understand what privacy is and that your personal data should be a highly valued good • Better education at all levels of service provider • Educate children about general privacy issues, without trying to make them buy any single piece of software • More accessible information should be provided • Exchange information with each other as to how it should and can be done; inform customers better

Region	Suggestion
	• Improve understanding that better security is not an “off the shelf” service or a product, rather a process **Implementation and enforcement** • Enforce the law, punish the data abusers • Much higher penalties for government bodies which "lose" electronic data • Promote methodology and compliance measurement criteria • The private sector should develop codes of conduct for publishing and marketing companies using personal information of users that could help complement legislation and offer trust to end users • Provide clear security guidelines for data entry and retrieval • Differentiate policy from implementation • Lapses in privacy protection in social media should be corrected urgently • Put clear limits as to what data can be collected, and who has access to such data • Extend data protection laws to Web 2.0 • Applying laws and guidelines that are not based on old-world economy structures **Consultation** • Governing authorities must discuss with stakeholders **Users** • Empower users to maintain their own privacy settings for their data (different privacy requirements for different users) • Never tell the truth over the Internet unless there is a good reason for doing so • Lock data physically to the person that is described (i.e. through key); free availability is second here: authorization approval by owners only (or under strict conditions as an exception to this rule) **Technology** • Design systems with privacy as a requirement **Other** • Rethink the value of privacy, its history in various cultures, and its relevance to non-globalisation • Be more organised
Latin America	**Education and awareness raising** • Educate themselves and be reasonable **Formulate policies, laws and guidelines** • Discussing and creating laws • Personal data protection **Consultation and dialogue** • Work together to try to develop the best draft law and involve every interested party **Other** • Do not use privacy/data protection as an excuse to reduce freedoms • See the case exposed by Robert Pitofsky in 1998 in the US Congress regarding the minimal considerations for privacy online
North America	**Education and awareness raising**

Region	Suggestion
	• Education via modern media • Provide more information on data theft and an inexpensive means of protection against theft of account numbers and identity **Formulate policies, laws and guidelines** • Create similar laws that require private companies to protect data, at a minimum, to the level the government protects information • Formulate laws that address the sharing of personal information • Establish the same data protection laws as in the European Union • Enact a standard for what is private and what is public • The government should develop an list of minimum and maximum expected protections • Develop a standard for all types of data, maybe something similar to the rules for health records • Follow the approach being taken in the European Union **Implementation and enforcement** • Digital law enforcement should scrutinize everyone in the Internet Service Provider industry who has access to a user's data • When private information is misused for marketing/harassment, a criminal penalty should be applied • There should be financial punishments for data leaks • Establish an independent Privacy Officer **Community action** • The people of the US should demand a definition of "privacy", and a codified "right to privacy" • Consumers must demand that companies be held responsible for data breaches, and punished in a meaningful way • Interest groups, like ISOC/ACM/IEEE should mobilize to support this effort • Get informed, take protective cautionary steps to mitigate the effects of any side effects from loss of personal data • Get involved • ISOC could/should take the lead in publishing white papers on the subject, for the purpose of informing users and governments, directing policy, and establishing clear guidance for use of the Internet **Specific solutions** • All information sources, sharing etc. should be strictly opt-in, and opt-in by default • For online accounts users login - a uniform adoption of last-login timestamp

Country	Suggestion
Afghanistan	The government should pass a law regarding privacy and data protection
Australia	1. Define the issues 2. Define the basic right to privacy 3. Table regulations 4. Protect privacy with laws 5. Enforce laws with strong penalties

Country	Suggestion
Australia	1. Force application of Freedom of Information, at no cost. Finding out information can cost thousands of dollars. 2. A one-cent charge on every mail would penalize salvo-spam, and thus indirectly leave no motive for the surreptitious cross-referencing of people's age, interests, politics, liquidity, sexuality, religion, philosophy and skills.
Australia	There needs to be a global approach to global organisations that pose threats to privacy (e.g. social media)
Belgium	Lapses in privacy protection in social media should be corrected urgently
Brazil	Discussing and creating laws
Canada	All information sources, sharing etc. should be strictly opt-in, and opt-in by default
China	More awareness is needed
Colombia	See the case exposed by Robert Pitofsky in 1998 in the US Congress regarding the minimal considerations for privacy online
Congo Democratic Republic	Provide people with more information on privacy and data protection
Cook Islands	Improve
Cook Islands	The government needs to establish a privacy law so that when information of a private nature is divulged then there is some recourse that can be taken to protect the interests of the person concerned
Ecuador	Personal data protection
England	Never tell the truth over the Internet unless there is a good reason for doing so
Ethiopia	The government should formulate policy and broadcast it to the people. Raise awareness by providing training.
France	Promote methodology and compliance measurement criteria
Germany	Educate children about general privacy issues, without trying to make them buy any single piece of software
Germany	Differentiate policy from implementation Improve understanding that better security is not an "off the shelf" service or a product, rather a process Better education at all levels of service provider
Germany	Empower users to maintain their own privacy settings for their data (different privacy requirements for different users)
Germany	Help people understand what privacy is and that your personal data should be a highly valued good
Ghana	Information Security standards/procedures need to be put in place.

Country	Suggestion
	These should include: i) Development of Information Security Policies ii) Appointment of an officer responsible for Information Security to implement the policies/standards and procedures iii) Information Security Audits
Guyana	Educate Internet users
India	Engage in public debate. Articles in media. Discussion on TV.
India	More emphasis and education
India	Undertake a more detailed and in-depth analysis of the subject
India	Need to discuss, introduce basic rules and work on evolving a complete solution
India	Study the approaches in other countries, especially North America and Europe Create awareness among the public at large, particularly youth Encourage government action through public pressure
India	Make cyber security a required course for all graduates and computer degree holders
Ireland	More accessible information should be provided
Italy	Governing authorities must discuss with stakeholders
Italy	Be more organised
Japan	The government should have a unified law and a simple set of rules to help people have a deeper understanding of privacy issues
Jordan	The main focus should be on the community since this service is intended for their use and need
Kenya	Stakeholders should familiarise themselves with issues related to protection of personal data
Lebanon	Distribute guidelines/templates for data protection that everyone can use
Liberia	Laws that address this should be placed under discussion at our parliament. However, the bill regarding this should be raised by someone/organization that is knowledgeable in that area. This is because the parliament may not have the full knowledge as to the details of the issue. Thus, that education should come from a professional in that field of discipline.
Liberia	They should teach privacy in schools and at religious congregations
Malaysia	Raise awareness and impose policy with enforcement
Mali	Adopt guidelines on this issue
Mauritania	Business should encourage the application of the collective agreement structure
Netherlands	Put clear limits as to what data can be collected, and who has access to such data
Netherlands	Design systems with privacy as a requirement.

Country	Suggestion
Netherlands	Provide clear security guidelines for data entry and retrieval Lock data physically to the person that is described (i.e. through key); free availability is second here: authorization approval by owners only (or under strict conditions as an exception to this rule)
Nigeria	Organise seminars and workshops
Pakistan	Raise awareness among Internet users
Pakistan	Government bodies, civil society and relevant industry representatives should conduct a dialog and define the policy for privacy and data protection. In order to define this, a collection of definitions is needed to reach consensus and integrate all the relevant areas as perceived by different stakeholders.
Pakistan	Do something at least
Papua New Guinea	National level consultations - government and private sector leading to legislation
Paraguay	Work together to try to develop the best draft law and involve every interested party
Philippines	More awareness and concern regarding privacy and private data
Philippines	Enact a privacy/data protection law
Philippines	Legislation on privacy should be enacted
Republic of Congo	People should be able to choose whether their data should be public of private
Republic of Nauru	The government should conduct an awareness workshop so the people are aware of the importance of privacy/data protection
South Africa	Formalise a standard regarding the definition of personal information
Spain	Extend data protection laws to Web 2.0
Spain	The private sector should develop codes of conduct for publishing and marketing companies using personal information of users that could help complement legislation and offer trust to end users
Sri Lanka	There should be a comprehensive set of policies with international standards. This should be undertaken by the government, regulatory bodies and academia collaboratively.
Sweden	Privacy is dead. Get over it.
Sweden	Full international cooperation to stop abuse of the Internet
Switzerland	Exchange information with each other as to how it should and can be done; inform customers better
Switzerland	Rethink the value of privacy, its history in various cultures, and its relevance to non-globalisation

Country	Suggestion
The Gambia	Start by forming an ISOC Chapter
UAE	Raise awareness of these issues, by conducting seminars and workshops at different Universities/colleges etc.
UK	Much higher penalties for government bodies which "lose" electronic data
UK	Rethink the value of privacy, its history in various cultures, and its relevance to non-globalisation
UK	Learn and understand how the Internet works Applying laws and guidelines that are not based on old-world economy structures
UK	Enforce the law, punish the data abusers
Uruguay	Educate themselves and be reasonable Do not use privacy/data protection as an excuse to reduce freedoms
USA	Get involved
USA	Provide more information on data theft and an inexpensive means of protection against theft of account numbers and identity
USA	The people of the US should demand a definition of "privacy", and a codified "right to privacy" Interest groups, like ISOC/ACM/IEEE should mobilize to support this effort Additionally, consumers must demand that companies be held responsible for data breaches, and punished in a meaningful way
USA	For online accounts users login - a uniform adoption of last-login timestamp Digital law enforcement should scrutinize everyone in the Internet Service Provider industry who has access to a user's data When private information is misused for marketing/harassment, a criminal penalty should be applied
USA	Create similar laws that require private companies to protect data, at a minimum, to the level the government protects information
USA	Formulate laws that address the sharing of personal information
USA	Establish the same data protection laws as in the European Union
USA	There should be financial punishments for data leaks The government should develop an list of minimum and maximum expected protections
USA	Education via modern media
USA	Enact a standard for what is private and what is public
USA	Some should be arrested, some deported, others simply fired
USA	Get informed, take protective cautionary steps to mitigate the effects of any side effects from loss of personal data

Country	Suggestion
USA	ISOC could/should take the lead in publishing white papers on the subject, for the purpose of informing users and governments, directing policy, and establishing clear guidance for use of the Internet
USA	Establish an independent Privacy Officer
USA	Develop a standard for all types of data, maybe something similar to the rules for health records
USA	Follow the approach being taken in the European Union

ANNEXURE E to PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

THE TOP FIVE EMERGING CHALLENGES BY REGION

EUROPE

The top emerging challenge

- Cross-border data protection
- Ensuring individuals understand the value of privacy
- Social engineering (e.g. phishing)
- Spam distribution and botnet activity
- Lack of an international secure user-ID pass (or similar)
- The collection and storage of traffic data (e.g. geo-location data)
- Implementing privacy by design in complex systems
- Providing public Internet services without intrusion on the user's privacy
- Widespread poor understanding of privacy options
- Complexities of regulating online privacy settings for individuals
- The trade-off between convenience and data protection
- Collapse of trust in anyone and anything online
- Obstacles to connecting old and archaic data protection systems
- Unauthorised access to personal data
- Preventing unauthorized use
- Medical data
- Medical records digitisation usability versus protection
- Collection of medical data by insurance companies
- Data mining made really easy
- Data can be transmitted quickly
- Mining personal data is becoming a huge industry
- Cloud computing/storage/networking (x2)
- Recognising privacy as an unchallenged (assumed) 'good'
- Educating people, children and customers about privacy and data protection
- Data protection law enforcement is not easy for users
- Insufficient government knowledge regarding protection of personal data
- Security being an excuse for tighter control
- Identity theft
- IP security
- Digital Economy Act (x2)
- Copyright laws
- Robot commercial communication through telephone

The second emerging challenge

- Digital identity – including the faking of digital identity by a third party
- Stopping unknown data collections and collectors
- Worms and botnets
- Security systems leaking (like databases and such)
- Traffic monitoring, with logging
- Data visibility – where is "my data" stored
- IP information providing conditions
- Awareness among general population
- Protecting illegal access and use by criminals
- Medical records (Doctors, dentist, hospitals, pharmacies) being centralised
- Surveillance laws
- Class actions against major players

- Definition of personal ID without any meaning
- Limitation to legal intercept of private communication
- Government “snooping”
- Control of use collected data is impossible
- Unclear definition as to what is wiretapping - there is a definition in constitutional law but it is scarcely applied
- Financial data
- Search engines (x2)
- Use of child pornography as an excuse for more control
- Using data contrary to purpose
- Tendency to use a single cross-agency identifier
- Public companies misusing data
- Accessing and abusing individuals' health information
- Data on communication and transportation should be regulated
- Misdirected privacy concerns by Government impeding new services
- Hadopi law

The third emerging challenge

- The balance between identification and privacy on the Internet
- Hacking of databases with personal information
- Make hidden data collections visible to the public
- Malware and such
- Surveillance camera
- Encryption and the lack thereof
- Restricting profiling by businesses, employers, authorities
- Class actions against ICANN
- Electronic personal ID cards
- Large scale education about issues of data collection, profiling and privacy
- Corporate “snooping”
- Correlation of data is becoming easier than ever (search engine, location info,...)
- The policies of data retention are paying scarce attention to a standard for auditable procedures in data retention
- Personal data
- It is easy to copy, edit and link information
- IPR (copyright) as a base for control
- Personal certificates
- Collecting data for no specific reasons
- Awareness of issues among professionals
- Over-reliance on electronic data e.g. in banking and in personal dealings
- Constraining access to otherwise public information
- Individuals wanting their cake (privacy) while eating it too (dislikes targeted adverts)
- Amendment 138 to the Telecoms Package

The fourth emerging challenge

- Privacy in non-democratic countries (abuse by governments)
- Non-cooperating countries
- Education is not properly focused on these issues
- Poor data handling, losing control over collected data
- Indicating unauthorised use (afterwards)
- Global availability versus national legislations
- Class actions against specific registrars
- Consistency with foreign approaches
- Deep Packet Inspection (DPI)
- Expansion of CCTV
- Personal data trail is becoming ever more dense
- No standard formats of the records

- Communications data
- Anyone can be a content provider
- Use of data for other reasons then for what it got collected
- DNS
- Education about privacy, security, and technical measures
- Awareness of issues among public
- Undue usage of IPR (Intellectual Property Rights)
- All-knowing search engines means publish once equals publish always and everywhere
- Interoperability and open standards

The fifth emerging challenge

- Developed countries need to downgrade systems to be inline with not-so-developed countries
- Privacy as tool for disruption (abuse by anarchists)
- Maintaining anonymity while providing individuals with interests and proximity information
- Define and implement legal venues for quick protection of personal data and against profiling
- It is becoming for the individual very difficult to maintain control
- Standards, standards, and even more standards
- Security
- Absence of global laws and understanding
- Large scale data mining
- Email
- Loss or theft of data
- Spamming
- Information online gets cached and is not purged
- Geo-location
- Global availability of personal data through lax privacy policies of social media

ASIA AND THE PACIFIC

The top emerging challenge

- Information misuse
- Social media sharing personal data by default without authorisation
- Making a law and getting it passed by the parliament
- Development of privacy policy
- Privacy laws
- Policy
- Lack of a clear policy
- Adequate protection for children
- Privacy in social media
- Smart phone
- Government not taking privacy issues seriously
- Internet access
- Pervasive computing
- Facebook policies
- Protection of personal details
- Political pressure
- Lack of a code of conduct for local/municipal government workers
- Government exceeding its mandate and eroding citizen rights
- Government mandated surveillance and censorship
- Internet/Digital Censorship
- Government and law enforcement agencies not taking the issues seriously enough
- Government with insufficient knowledge and understanding of the issues
- Security of data
- Email safety
- Hackers and spyware (x3)
- Awareness

- Social networking sites
- Online shopping using credit cards
- Corruption
- Secret identity in terms of digital currency

The second emerging challenge

- Law Enforcement
- Businesses using unfair practices in the absence of specific regulations
- IP address as “personal data”
- People use social networking tools inappropriately and include a lot of personal data about themselves inappropriately
- Online security
- Adoption of data protection legislation to protect privacy
- Protection
- The concept of social media sites owning personal data entered by users
- Saving details
- Bureaucratic conformity
- Information leakage through careless installation of file-sharing software
- Theft and misuse - cyber crimes due to inadequate measures against
- Enterprise has no financial reason to care
- Piracy
- Online shopping
- Products automatically profiling data and collecting Personally Identifiable information
- Policy required
- Transmission of sensitive information
- Lack of implementation agencies understanding of the severity of issue
- Establishment of a privacy mark system
- Government survey
- Spying on Privacy
- Unawareness of users
- Data transfer
- Enhancing the capacity of the government authorities regarding the data protection and privacy
- Identity fraud
- Identity theft
- Budget
- Use of personal data by large corporations (Telcos) for business advantage (i.e. marketing)
- Authorized use. Avoiding misuse
- Ease with which data can be lost and found

The third emerging challenge

- Identity theft as then theft of wealth and property
- Breach notification
- Information about others is usually passed on even when it is of a confidential nature and often without permission
- Internet filtering
- Personal digital data protection in personal digital devices
- Accessibility
- The impossibility of users removing false accusations about themselves on other websites
- Family details
- Income-bracket discrimination
- Questionable conduct of online retailers allegedly reselling the personal information of customers
- Impact on foreign trade, particularly in services
- There is no official body to regulate privacy
- Hacking within firewall
- Online banking
- Use of search engines to profile individual users and target that user by government, business and criminals

- Government interest
- Unethical exchange of information
- Lack of user awareness about the significance of privacy
- Chain mail campaigns
- Hacking
- Enterprises and service providers exploit the unawareness of users
- Cybercrime
- Implementation of law to enhance data protection
- Scammers
- Social mischief
- Availability of experts
- Lack of public awareness/concern over privacy issues
- Exchange of data without informing concerned individual
- Not breakable and easily formatted

The fourth emerging challenge

- Country being seen as an unsafe destination for data – impact on BPO industry
- Definition and enforcement for “sensitive personal data”
- People use the “reply all” feature inappropriately in emails
- Computer fraud and scam
- Definition of the right to share and protect personal data
- Storage
- Lack of global approaches
- Transparency and conduct
- Religious intolerance
- Lack of social education on what might happen using computers and networks
- Unauthorized, unethical research - particularly in health sector
- Existing regulations have no "teeth"
- Emails
- Social network programs not distinguishing between "friends" , "family" and "strangers" and sharing personal data with everyone
- Stakeholder association meetings
- Leakage of defence data
- Registration with web sites
- Spam/Junk/Advertisement mails/Calls
- Protection of the Internet
- Keeping the stakeholders and organization working with personal data accountable
- Data used for gain or profit without the end user knowing
- Political liberty
- Low level of security
- Mobile phone companies
- Have to be multipurpose use

The fifth emerging challenge

- Data processors and subcontracting issues
- Once information is online it is there forever and one never knows how someone can or will use that information
- Internet and mobile communication
- Prevention from misuse of personal data for commercial purpose
- Good governance
- Deprivation of access to public services
- Harassment
- Companies with good lawyers can do what they like with people's private data
- Combination of mobile internet and social networking to track individual users by location
- Funds required for activity
- Access of business competitors
- Personal blogs
- Phishing
- Education on Internet Safety
- Public awareness regarding this issue
- Lack of controls or knowledge about privacy
- Harassment
- Infrastructure
- Banking and e-commerce

NORTH AMERICA

The top emerging challenge

- Third party use of personal data for targeted advertising and unknown uses
- Correlation across various data collections enables significant data mining of individuals personal data
- Personal data required for necessary/desired services and then unnecessarily preserved by the recipients
- Ubiquity of data
- Deletion of personal data, particularly from archives
- Validating identity without compromising personal data
- Security at the expense of privacy
- Data ownership – i.e. who owns the data?
- Defining terms
- Access
- Are the right stakeholders involved?
- Appropriate use of personal data
- Increased crime relating to loss of privacy (e.g. identity theft)
- Automatic renewal via charge card on websites
- Overcoming the lack of legislative gumption to fix what is not working
- Wireless communication networks offer no privacy
- Finding a balance between individual rights under the 4th amendment and community rights to know information needed for just society etc.
- Protecting economic personal information
- Human stupidity
- Individuals' lack of awareness as to what organisations can do with their data
- Ensuring privacy policy is enforced
- Concentration of corporate influence on government privacy policies
- Misunderstanding by end users as to what things actually mean
- Deeper integration of business into our personal lives
- Prevention of the fraudulent use of illegally obtained personal data
- Cracking into computers to steal identity information
- Cloud computing
- Identity theft
- Banking online

- Data protection
- Security video cameras
- Protection from hackers/security
- Monitoring data transmissions without court approval
- Lack of anonymity on the Internet due to government and corporate tracking
- Making more people aware of how to protect their personal data
- Privacy rights that only apply with respect to government not business

The second emerging challenge

- Leakage of personal data to third parties that are misusing information to support ID theft
- Correlation of data from multiple sources
- Rights when your data is used inappropriately
- Ownership of personal data
- Security of the data
- Security
- Increasing government intrusion into private communications
- Phishing
- Wired communications networks: no privacy
- Defence, intelligence and law enforcement information compromises and hacks
- Fraudulent websites
- Lack of awareness of what organisations actually do with their data
- Make sure data breaches are appropriately handled
- Present governments' policies where security trumps privacy
- Making money is more important than creating trust
- Lack of legislation to assure privacy
- Prevention of hacking of online personal data from storage systems
- Government abuse of private databases
- Keeping up with all the changing regulations for international companies
- Identity being used illegally
- Re-defining privacy laws in a meaningful way in the digital environment
- Employers using posting against potential employees
- Some international forced use of fingerprints contributing to types of data collections available for correlation and data mining
- Mandatory reporting of breaches from private companies
- Social media
- Personal responsibility for people's own data, especially younger people
- Default settings for web sites / social networks' privacy settings
- Increase in the size of data breaches due to larger aggregation of data
- Data standards
- Records of searches preserved by "search engines"
- Getting personal info removed

The third emerging challenge

- Determining what is and what is not personal data in the digital age
- Rights when you have the data
- Services related to the collection and distribution of personal data
- User knowledge
- Data sharing
- Lack of clear ethical goals and standards regarding privacy of data
- Person to person: no privacy in presence of wireless and wired communications networks
- Information surrounding how to build weapons
- Phishing type scams
- Insufficient proactive examination of usage terms before signups
- Lax security attitude of online social media sites
- Young, inexperienced CEOs [of social media sites] think they know more than they really do
- Lack of adequate coverage of genuine issues in the news media
- Prevention of posting personal data online into databases with weak security

- Abuse of centralised medical records
- Data de-identification
- Layman's lack of understanding of the loss of privacy on the Internet
- Opt-ins rather than Opt-outs
- GPS
- Protocols for sharing data
- ubiquitous, real-time, government video surveillance in the name of "protection"
- Corporate data control
- Cookies and "tokens"
- Too much sharing of data without consumer consent

The fourth emerging challenge

- Determining reasonable best practices for the use of personal data and sharing of such data with third parties
- Opt-in versus opt-out
- Identity theft
- Social network virus
- Personal control
- Lack of agreement within and between any groups about goals, policy, actions
- US mail: limited privacy
- Compromises to power grids and other infrastructure elements
- Technologies as yet unknown
- Getting tougher laws in the face of corporate lobbying
- Government needs to stay out of the way of business
- The general populations lack of understanding of the enormity of the issue
- Preserving the Neutrality of the Internet
- Increased disregard for individual privacy in the corporate economy
- Updates in law that reflect new technology
- Cellphones: microphone eavesdropping
- Misuse of information gained by government and businesses
- Collapse of consumer credit system due to universal theft of all credit card data
- IP/copyright
- Lackadaisical protection of repositories of personal data/information, permitting "hacking" of same
- Need more legal protections for personal privacy rights

The fifth emerging challenge

- Explaining to end users what benefits come with sharing personal data and precisely what sharing is undertaken
- Unwanted marketing
- Redress and accountability
- Government denial of benefits of knowledge and use of best cryptographic protections to most users
- Policy statements to protect MY privacy: like mortgage backed derivatives
- Compromised information from health care institutions
- Direct hacking attacks
- Actually enforcing effectively laws on privacy, especially mandatory deletion on request
- Lack of a cohesive set of tools to ensure privacy
- Preserving an individual's right to privacy
- Education of the public
- Credit/Debit Cards
- Ability for people to control their data "in the wild"
- Denial of insurance and employment due to unauthorised release of private medical data
- New technology
- Social networking privacy issues

AFRICA AND THE MIDDLE EAST

The top emerging challenge

- Lack of understanding of the concept of privacy
- Development of local laws and rules that are acceptable/consistent with international principles
- International treatment of personal data
- Developing laws and agreements
- Sufficient “know-how”, and understanding of the issues by decision makers
- Corporations underhandedly changing T&C principles
- Separating public and private data
- Availability of broadband
- Increased connectivity
- Social networks
- Password management
- Data encryption based on fingerprints
- The possibility that the data may not reach the person it was intended for
- Sharing of third party personal data/information over bluetooth, especially mobile phones
- Freedom is mandatory before any privacy and knowledge on what is "personal data"
- Non-democratic governmental approach to the privacy of the individual
- Insecurity
- Personal protection
- The conflict between the inherent right of the individual to privacy and government desire to monitor traffic
- Spyware
- E-Commerce
- Discrimination/retaliation

The second emerging challenge

- Let all individuals be aware of the different uses of his personal data
- Terms and conditions
- Tension between state and commercial interests against privacy interests
- Lack of government understanding of technology
- Potential legislation against use of encryption software in emails or on laptops
- Corporations feeding data to advertisers even when you opt out
- Understanding
- Distribution of Private data to others
- Increasing online transactions
- Increased electronic gadgets (phones that record sound and take pictures, for example)
- Social networking
- Unable to find easy tools for any ordinary users to back-up, secure, and use personal data while using removable storage medium
- Regulating privacy
- Processing of personal data for collateral purposes and security
- Protection of private information
- Regulation accepted by all parties: Government, Users and ISP
- Understanding of the issues by private sector
- Commercial use for advertising
- Encouraging governments to create laws for privacy and protection of personal data
- Viruses and anti-virus software
- War
- Hotspot
- The wrong person might receive it

The third emerging challenge

- Determine links between personal data/privacy and human rights
- Protection and Security
- Low priority for government/police
- Increased exposure as the first world tighten their security

- Lack of respect for individual rights
- Corporations associating online activities with you because you are logged in to their service and it can pick up what you're doing from where you browse
- Acceptance
- Different norms for personal data in different countries
- Mobile telephone communications
- High-capacity storage media, making data “snatching” easy
- Email privacy
- Software that extracts data from formatted disks
- Give a value to the worker
- Determining how private data should be handled
- The problem of information security
- The appropriate technology able to guarantee privacy
- Understanding of the issues by users
- Fraud
- Mobility and Security of Data exchange
- Internet Fraud, and the need to install firewalls in organisation’s intranet
- The collapse of human dignity
- Whois
- Maybe by eavesdropping, the wrong person may receive it

The fourth emerging challenge

- Personal data and information
- Big profit margins possible in illicit use of personal data
- Lack of resources on the ground to address the problem
- Too much information being gathered by one corporation, even indirectly without your involvement, that can easily be collated
- Awareness among users
- Low income of officers tempting them to part with private information for pay
- Hardware failure
- Encourage research and studies and the discovery
- The rights of the holder of personal data
- Are people understanding the importance of the matter?
- Understanding of the issues by educators
- User access management, which includes user registration, review user access right and unattended
- Industrious espionage
- The content might be changed before arrival, perhaps by someone or data loss

The fifth emerging challenge

- Ease of interception of communications and identity theft
- Lack of a legal framework or capability to enforce the law
- Privacy concerns not being taken seriously by corporations
- Ease of publishing on web may be abused
- Limited knowledge of users regarding privacy and protection of personal data
- Hear and understand the workers
- Consulting on action needed
- Data back-up Solutions
- Misunderstanding
- E-commerce data
- It might not arrive on time due to routing issues

LATIN AMERICA

The top emerging challenge

- Educating customers about the digital environment and security

- Information
- Developing/having a culture of personal data protection
- Privacy versus security (x2)
- Bank security
- Enactment of data protection laws
- Punishment of digital crimes
- Regulation of targeted online advertising
- Protection of personal data, particularly of children
- Management of personal data on the Internet
- Social networks
- Recognising that privacy is grounded in human rights

The second emerging challenge

- Digital signatures
- Establishment of an Agency
- Sale of personal data
- VPN links
- Mobile
- Typical authentication and authorisation issues
- Protection of personal data for criminal investigations
- Use of other personal data for unmoral or illegal purposes
- Paedophilia and Identity Theft
- Data Protection law
- Knowledge
- Control in the context of government is exercised collectively rather than individually

The third emerging challenge

- Data encryption
- Well prepared public clerks
- Disclosure of personal data in TV, radio, newspapers
- Security through proxies
- E-mail
- Trust is not “transitionable” property
- Protection of privacy by cloud service providers and ISPs (cloud computing)
- Sale of illegal data bases
- Use of information for Call Centres
- Protection of minors
- Protection of identity integrity

The fourth emerging challenge

- Capacity building
- Personal data protection
- Security certificates
- E-government
- Education, particularly of youth
- Protection of privacy in social networks
- International Transfer of Data
- Legal reforms

The fifth emerging challenge

- Database of personal data security
- Phishing
- E-learning
- Disposal of private information
- National identity cards and biometrics

- Medical data
- International agreements

ANNEXURE F to PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

LAWS, REGULATIONS, PRINCIPLES AND GUIDELINES

Country	Laws, regulations, principles and guidelines
Argentina	Law 25326 (data protection national law) Law 1846 (data protection law for City of Buenos Aires Code of conducts for email marketing practices Do not call registry (for the City of Buenos Aires)
Argentina	La ley mencionada y la de Habeas Data
Armenia	The Law of the Republic of Armenia on Personal Data http://www.parliament.am/legislation.php?sel=show&ID=1331&lang=eng
Belgium	The EU directives and their implementation by the Member States
Burkina Faso	Loi du 20 avril 2004 portant protection des données à caractère personnel Le décret 2007-283/PRES/PM/MPDH du 18 mai 2007 portant organisation et fonctionnement de la Commission de l'Informatique et des libertés (CIL) article 35 à 40 de la Loi du 27 novembre 2008 portant réglementation générale des réseaux services de communications électroniques au Burkina Faso
Canada	Personal Information Protection and Electronic Documents Act http://laws.justice.gc.ca/eng/P-8.6/index.html
Czech Republic	Personal data protection law: Act no101/2000 Sb. CZ
Ecuador	The Constitution of Ecuador and in the law of the national system for public data storage
Finland	http://www.finlex.fi/fi/laki/alkup/2004/20040759 (Finnish version) Many laws and telecoms regulation apply to protection of personal data and such. They all are in-line with EU directives.
France	Protection des données personnelles
Germany	A list of the laws (35) can be found here: http://www.bfdi.bund.de/cln_136/DE/GesetzeUndRechtsprechung/Spezialgesetze/Spezialgesetze_node.html
Germany	http://bundesrecht.juris.de/bdsg_1990
Hong Kong	Personal Data (Privacy) Ordinance http://www.pcpd.org.hk/english/ordinance/ordfull.html
Hungary	There are several laws, codes, rules, and guidelines applying in different situations and circumstances with respect to different kinds of public and/or private activities
India	Information Technology Act 2000
India	Information Technology Act Right to Information Act More recently, Unique Identification (UID) project (now called Aadhar) has

Country	Laws, regulations, principles and guidelines
	been initiated by the government to give UID number to each citizen.
Italy	Code on the protection of personal data
Japan	Three laws (all in Japanese romaji) 1) Kojin jouhou hogo hou (for private corporations) 2) Dokuritsu gyousei houjin tou kojin jouhou hogo hou (for national government and government organisations) 3) Jichitai tou kojin jouhou hogo hou (for local government and the organisations)
Japan	Personal Information Protection law
Lebanon	Draft law indicates that all entities gathering personal data must apply for a permit
Mali	National Ethic Committee located at the Ministry of Health giving advice on all research programmes dealing with human beings. This Committee has some rules on personal data and information
Mexico	The Federal law of Transparency and Access to Public Government Information (LFTAIPG) contains a chapter on data protection obligations for government entities and agencies at the federal level. There is also a regulation of the LFTAIPG, the purpose of which is to guarantee the protection of the privacy rights of individuals and guidelines for access and modification of their personal data in possession of government entities.
Mexico	Federal Data Protection Act (2010) Data Protection Guidelines (2005)
Netherlands	Law on Telecommunikation, article 11
Netherlands	www.cbpweb.nl
Norway	Personopplysningsloven (lit. person information law) http://www.lovdata.no/all/nl-20000414-031.html
Pakistan	Recently an e-crime law was composed by a government committee but was suspended because of lack of definitions and clarifications
Pakistan	Data Protection Act 2005
Paraguay	National Constitution (Habeas Data), Laws Nº1682/2001 and its modification by law 1969/02. Law 1682/01 - Article 4 defines sensible data. Article 3 and 4 talk about public data
Philippines	1. Philippine Ecommerce Law 2000 or Republic Act 8792 2. General Banking Law 2000 or Republic Act 8754 3. Their implementing rules
Philippines	Pending - Privacy Bill draft only covers data retention and security by private companies (primarily targeted at outsourcing firms)

Country	Laws, regulations, principles and guidelines
Senegal	Law 2008-08 on electronic communication and exchange Law 2008-41 on data encryption Presidential Decrees about application laws of privacy and personal data protection and electronic exchange and data encryption and Decree about the creation of data protection commission
South Africa	ECT Act http://www.internet.org.za/ect_act.html
Spain	See LOPD in http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=1999/23750
Sweden	Personuppgiftlag Sekretesslag
Sweden	www.datainspektionen.se
Sweden	Data Protection Act (1998:204) and Personal Data Ordinance (1998:1191)
Switzerland	Telecommunications Law, 30.4.1997, Art. 13a, para. 2: “They shall take the technical and organisational measures necessary for data protection and security during processing, in particular during transmission.”
UK	Data Protection Act Privacy and Electronic Communications Regulations Freedom of Information Act Environmental Information Regulations
UK	Data Protection Acts and EU directives, Human Rights Act
USA	Privacy Act (1974) Freedom of Information Act (FOIA) (1974) E-Government Act (2002), Section 208 Health Insurance Portability and Accountability Act (HIPAA) (1996) Children’s Online Privacy Protection Act (1998) Financial Services Modernization Act (Gramm-Leach Bliley Act or GLBA) (1999) Consolidated Appropriations Act of 2005 Implementing Recommendations of the 9/11 Commission Act of 2007, Section 803 (addresses Privacy and Civil Liberties Officers) Federal Agency Data Mining Reporting Act of 2007 (Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007)
USA	http://www.dhs.gov/files/publications/gc_1271701587683.shtm
USA	http://www.justice.gov/criminal/fraud/websites/idtheft.html
USA	Privacy Act of 1974 and Patriot Act

ANNEXURE G to PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

WHERE WOULD YOU LOOK FOR GUIDANCE ON THESE ISSUES?

Source	Details
Academia/research	Harvard's Berkman Center for Internet and Society DiploFoundation courses www.scholar.google.com
Blogs/websites	www.michaelgeist.ca www.rogerclarke.com http://www.schneier.com http://www.protecciondedatos.org.mx
CERTs	
Civil society	Privacy International Electronic Frontier Foundation (EFF) Center for Democracy and Technology (CDT) Center for Digital Democracy (CDD) Open Rights Group Electronic Privacy Information Center (EPIC) The Public Voice Creative Commons Privacy Activism American Civil Liberties Union (ACLU) Privacy Rights Clearinghouse
Conferences and meetings	e.g. International Conference of Privacy and Data Protection Commissioners
Cryptography suppliers	
Industry bodies	BITKOM - Federal Association for Information Technology, Telecommunications and New Media IEEE - Computer Society
Internet governance discussions	IGF and EuroDIG
Internet technical community	Internet Society, Internet Society Chapters IETF ICANN W3C
Laws and regulations	
Legal and professional associations	e.g. International Association of Privacy Professionals (IAPP)
Media and other privacy news sources	e.g. www.privacy.org; www.wired.com

Source	Details
National and regional government agencies, networks and websites	e.g. European Network and Security Information Agency (ENISA) Economic Community Of West African States (ECOWAS) West African Economic and Monetary Union (WAEMU) Federal Trade Commission (FTC) Asia-Pacific Economic Cooperation (APEC) Data Protection and Information agencies Organisation for Economic Co-operation and Development (OECD) International Telecommunication Union (ITU) European Commission Ibero-American Network of Data Protection (RIPD)
Other	eLAC 2010 www.secureroot.com Packetderm, LLC (cotse.net) David Brin "The Transparent Society" Nicklas Lundblad "Privacy in a Notice Society" ACM guides
Private companies	e.g. Google, Microsoft, CISCO, Sophos
Standards/guidelines	ISO Good Information Security Standards/Procedures materials Privacy education guidelines and/or templates for campaigns Information Technology Infrastructure Library (ITIL) Madrid Declaration

ANNEXURE H to PRIVACY: AN INTERNET SOCIETY MEMBERSHIP SURVEY

ACTIVITIES THAT INTERNET SOCIETY CHAPTERS OR ORGANISATIONS ARE CURRENTLY INV0LVED IN REGARDING PRIVACY

Country	Details
Argentina	ISOC Argentina Chapter - participating in meetings and collaborating with relevant associations
China	ISOC Hong Kong Chapter – signed the Madrid Declaration
Czech Republic	Education system reform
England	Participation in IGF and EURIM ("an independent UK based Parliament-Industry group funded by its members")
Germany	Employed by a relevant organisation
Mali	ISOC Mali Chapter - in ECOWAS and WAEMU frameworks
Mexico	[Organisation] - European Commission decision on the adequacy of the protection of personal data in third countries
Netherlands	Advisor to various (governmental) parties; pleading for careful use of data
Norway	"Hobby politician", and member of the anti-DRD organization
Paraguay	[Organisation] - Mercosur working group SGT13 and Digital Mercosur Project
Peru	[Organisation] - eLAC 2010
Philippines	ISOC Philippines Chapter - drafted Philippine and 5 country monitoring and censorship report for FMA (ONI-funded)
Spain	OECD (Member of CSISAC) Council of Europe (Individual expert) IGF (Individual expert)
Sweden	Participation (as an individual) in Sweden's Trade Association for Digital and Interactive Marketing (see www.iabsverige.se) in discussions concerning self-regulation of targeted advertising
Sweden	National and European Commission
UK	Following EuroDIG discussions

ACTIVITIES THAT INTERNET SOCIETY CHAPTERS OR ORGANISATIONS ARE PROPOSING TO UNDERTAKE REGARDING PRIVACY

Country	Details
Argentina	ISOC Argentina Chapter - meetings and seminars on the topic
China	ISOC Hong Kong Chapter events
Cook Islands	PICISOC Chapter - perhaps PacINET conference in Vanuatu (September)
Czech Republic	Within centrally controlled secondary school leaving exams, which are being prepared
Ecuador	ISOC Ecuador Chapter - training young people not to disclosure sensitive or personal information in social networks
England	EURIM studies on Information and Identity Governance
Ethiopia	Formulating policy and conducting cyber education for staff
Finland	[Organisation] - product development to offer network based security, encryption and such to our clients and users
France	Customers aiming for “compliance”
Germany	ISOC Germany Chapter - educate children
Germany	[Organisation] - implementation of a Location Privacy Scheme in an Assisted Living Scenario: http://www.cs.uni-potsdam.de/pali
Germany	ISOC Germany Chapter - will try to setup workshop on privacy in autumn
Ghana	ISOC Ghana Chapter - organising training/education program in Information Security including “Privacy” and/or the protection of “personal data”
India	ISOC IKOL Chapter - proposal for Internet education in India
India	[Organisation] - discussion in progress
India	ISOC IKOL Chapter - works closely with law enforcement agencies and the general public on these issues
Italy	Frequently discussed within ISOC Italy Chapter and related forums
Japan	Regularly monitoring questionable online traffics; issuing campus-wide warnings and guidelines on privacy to the students, teachers, and administrative staff members
Mexico	The Federal Institute for Access to Public Information in Mexico will be hosting the VIII Meeting of the Iberoamerican Network on Data Protection in September-October 2010
Mexico	Will follow up: The work of the OECD on the 30th anniversary of the Privacy and Data Protection Guidelines. The 32nd International Conference of Data Protection and Privacy Commissioners to

Country	Details
	be held in Israel in November. The work of the Council of Europe in the revision of Convention 108. Participate in the activities for the data protection day on January 28, 2011
Norway	Information stands, demonstrations, political activity towards the parliament
Pakistan	ISOC Pakistan Chapter - we are trying to do some programmes in this area
Peru	[Organisation] - Conference prev. to III Ministerial Meeting of Information Society in LAC
USA	[Organisation] - we have yearly Standards of Business Conduct reviews
USA	San Francisco Bay ISOC Chapter - San Francisco INET
USA	Become more aware of threats and mitigations, deploy mitigations and defences
USA	Privacy Awareness Week
USA	Continuing focus