Communicating Online Confidentially

An Internet Society Survey

DECEMBER 2014

Communicating Online Confidentially

An Internet Society Survey

There are many legitimate reasons why Internet users might wish to remain anonymous and/or communicate confidentially online.

These reasons may include:

- to exercise their right or expectation of privacy;
- for personal security;
- concerns about unwarranted surveillance by governments or private companies;
- concerns about potential repercussions for statements made in social media and/or hosting blogs for “cyber-activists”;
- concerns about conclusions that may be drawn about them based on what they see and communicate on the Internet;

to name a few.

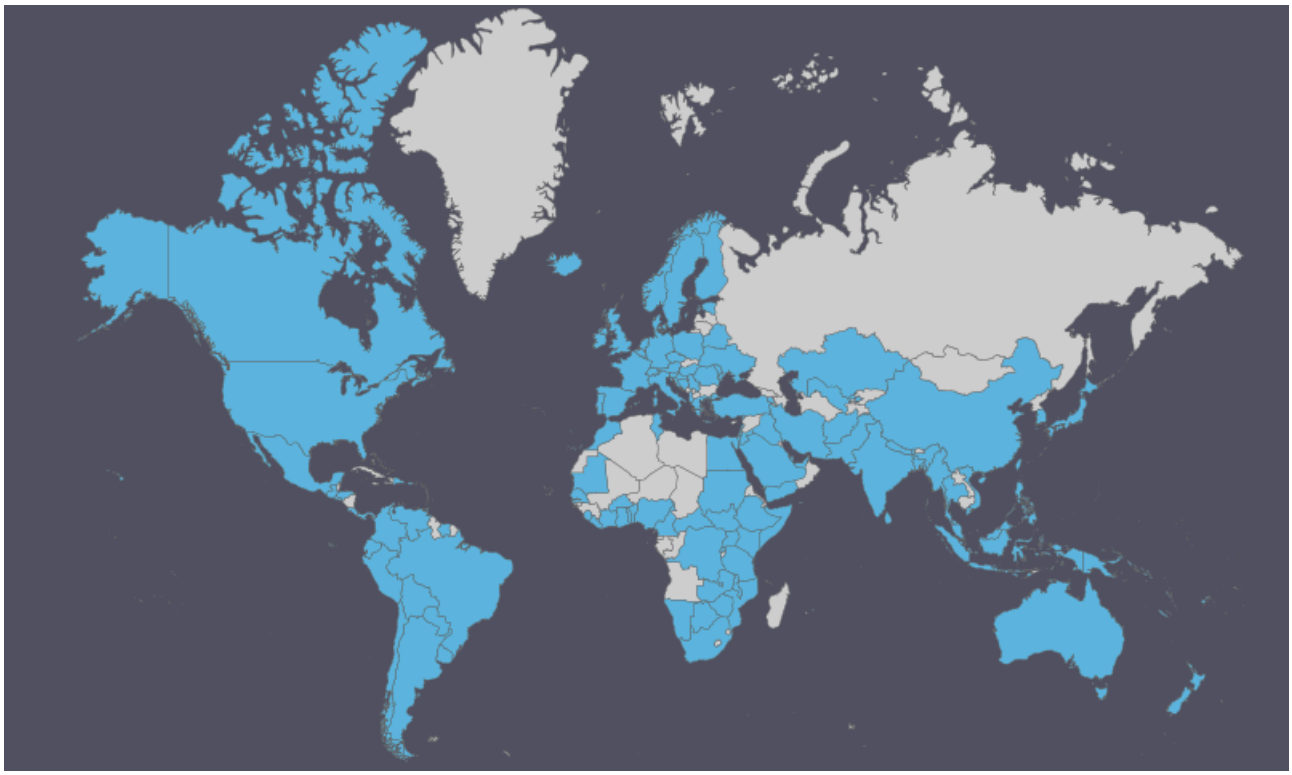
Each use case might require different tools and strategies.

The Survey

In 2014, the Internet Society invited its members and others to participate in an online survey regarding confidential communications on the Internet.

The objective of on privacy and surveillance.

The survey tool recorded 1347 responses (from many countries across the world), indicating global interest in this issue. However, we consider the sample to be too small to be representative. We do not seek to draw particular conclusions the survey was to gather information from across a broad spectrum of Internet users to help us gain a more complete understanding of their needs and expectations for confidential communications online. We also hope that the survey results will help inform international and regional dialogue about users’ needs and expectations in specific countries. Also, given the topic of the survey and the nature of the questions, it is likely that there is a self-selection bias towards individuals who have higher expectations of confidentiality; caring users. Nonetheless, the results are a useful window into the range of caring users’ needs and expectations.



Map: responses by country

Key Takeaways

We assume a self-selection bias to users that care about confidentiality.

The ability to communicate confidentially via the Internet is important to individuals. Those individuals use, and rely on, multiple tools and strategies for confidential communications just as they use multiple means to communicate via the Internet. Encryption is one of the tools they use for confidential communications.

Encrypted communications is not easy: there are a number of fundamental obstacles, including:

- insufficient information/guidance on how to use the tools;
- usability issues;
- dependency on other users using the same tools;
- incompatibility between tools/interoperability hurdles/poor tools.

Uncertainty as to whether an online communication would be confidential means that some individuals choose not to communicate via the Internet in some circumstances. For example, where:

- there is an unknown or suspicious “communicator”;
- there is a concern about surveillance;
- there is an untrusted device, application or access to the network;
- the user is unable to use encryption or other tools;
- the user is communicating certain types of information.

Online confidential communications may be exposed to others by:

(a) the Internet user himself or herself (usually by error);
(b) people they know (without their permission); or
(c) through monitoring, surveillance, hacking, insufficient security, etc.

Harm that individuals experienced from exposure of online communications that they thought were confidential could be wide-ranging – discomfort, embarrassment, financial harm, lost opportunity, loss of reputation, feeling that privacy has been violated, feeling of being observed, self-censoring, feeling powerless, feeling of insecurity, erosion of authority, reduced/loss of trust, etc.

The results also highlighted that there is a need for:

(a) greater transparency as to what happens to Internet users' communications data (including any surveillance that may or may not occur);
(b) better tools and guidance;
(c) neutral, trusted and respected sources of information;
(d) legal parameters.

The results

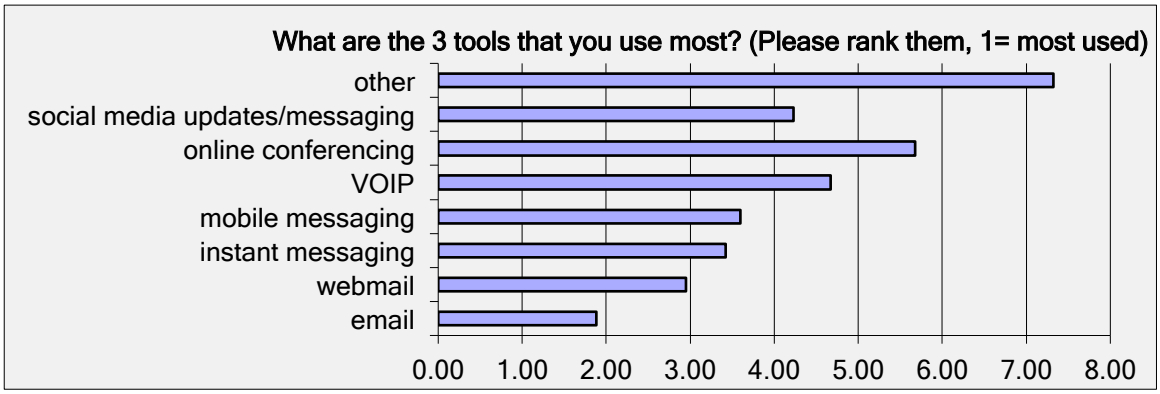
Below we provide the qualitative and quantitative feedback to each of the questions from the survey, together with our interpretation of the data.

Q: Which tools do you use to communicate online?

This question was divided into two parts:

- applications and services that are more obviously communication tools;
- applications and services that users may not immediately characterise as "communication tools", but which, nonetheless, are used to communicate.

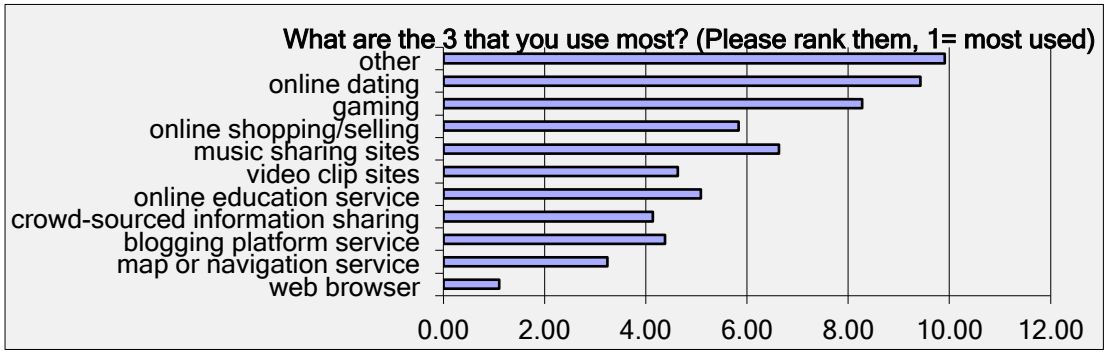
Which of these tools do you use to communicate online?		
Answer Options	**Response Percent**	**Response Count**
email	80.0%	1073
webmail	80.5%	1080
instant messaging	60.9%	817
mobile messaging	78.4%	1051
VOIP	73.9%	991
online conferencing	54.8%	735
social media updates/messaging	74.7%	1002
other		114
answered question		**1341**
skipped question		**6**



Among the respondents, *email*, *webmail* and *instant messages* are the 3 “communication” tools that are used most.

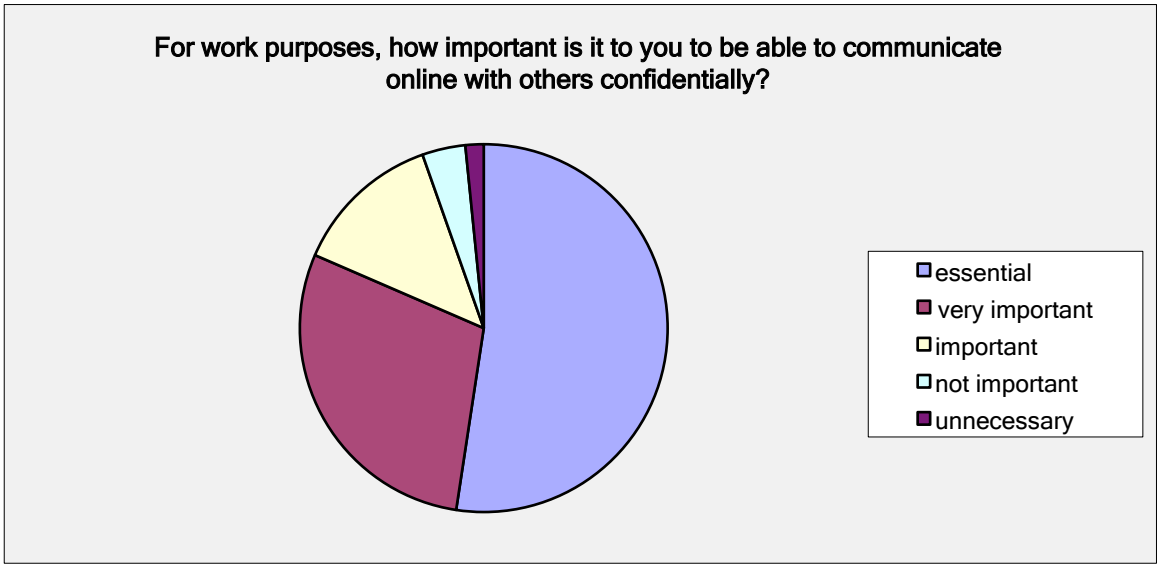
Which of these other online tools do you use?		
Answer Options	**Response Percent**	**Response Count**
web browser	98.5%	1312
map or navigation service	84.5%	1126
blogging platform service	43.0%	573
crowd-sourced information sharing platforms	76.0%	1012
online education service	49.0%	653
video clip sites	85.6%	1140
music sharing sites	27.5%	366
online shopping/selling	70.1%	934
gaming	12.2%	162
online dating	7.6%	101
other		57
answered question		**1332**
skipped question		**15**

Among the respondents, web browsers, maps or navigation services and crowd-sourced platforms are the 3 “other tools” that are used most.



The results of these questions illustrate that Internet users use multiple applications or services to communicate online.

Q. For work purposes, how important is it to you to be able to communicate online with others confidentially?



There were 1320 responses to this question.

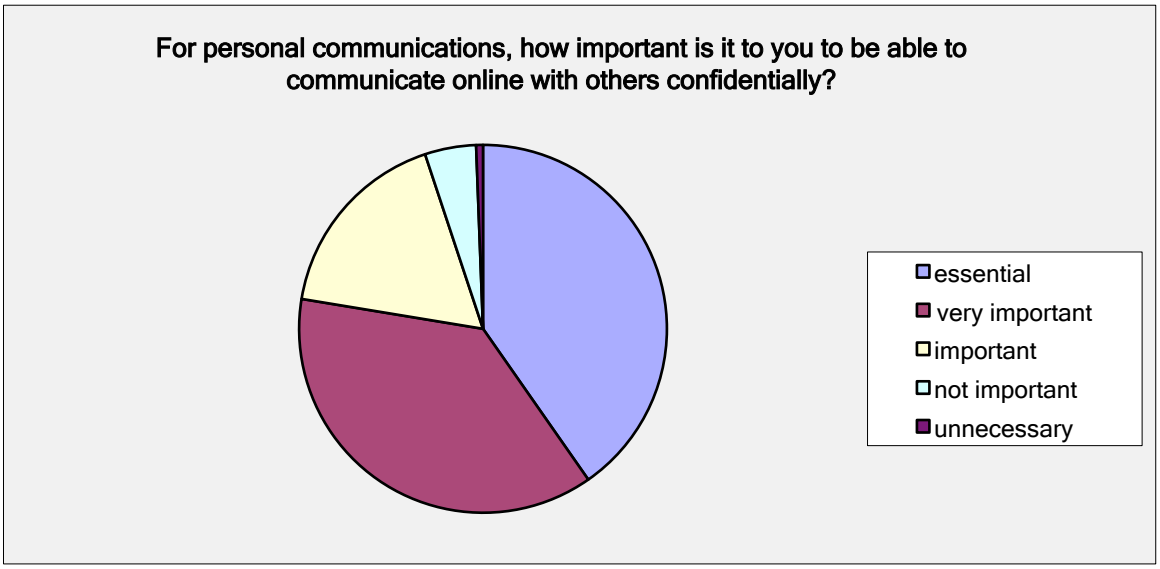
54% responded that it is *essential* for them to be able to communicate online with others confidentially for work purposes.

29.1% responded that it is *very important*.

13.1% responded that it is *important*.

Only 5.2% responded that it is not important or unnecessary.

Q. For personal communications, how important is it to you to be able to communicate online with others confidentially?



There were 1331 responses to this question.

40.3% responded that it is *essential* for them to be able to communicate online with others confidentially for personal communications.

37.3% responded that it is *very important*.

17.3% responded that it is *important*.

Only 5.1% responded that it is not important or necessary.

Q. What tools or strategies do you use for private communications with other users?

There were 1313 responses to this question.

The responses demonstrate that, among the pool of respondents, the top 4 tools that used are:

- encryption;
- privacy settings on social media;
- separate user accounts for different activities; and
- "Do Not Track" browser feature.

What tools or strategies do you use for private communications with other users? (select any that apply)		
Answer Options	**Response Percent**	**Response Count**
encryption	52.6%	691
Virtual Private Network	42.3%	555
proxy server	21.1%	277
Tor	15.2%	200
non-tracking search engine	16.0%	210
Do Not Track feature in Firefox, Chrome, Internet Explorer, Safari or other Web browser	49.0%	644
cookie blocking tools	28.3%	372
java script blocker	23.3%	306
private browsing mode	44.1%	579
privacy settings on social media	51.5%	676
pseudonym (a username that is not your real name)	30.8%	405
separate user accounts for different activities	50.3%	661

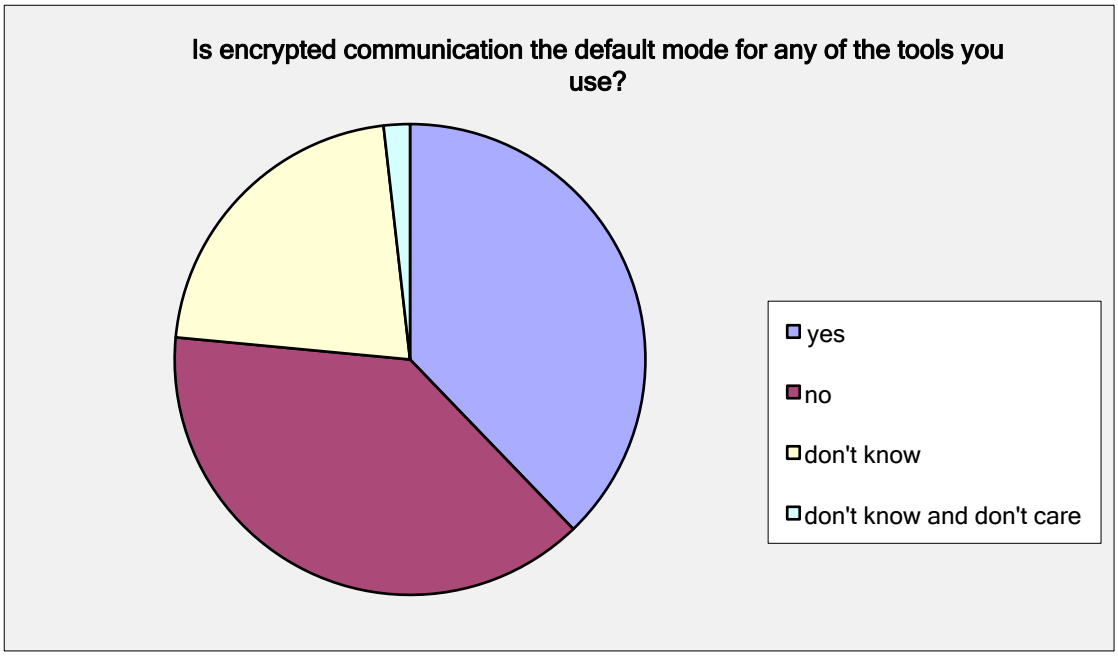
separate browsers for different activities	29.6%	388
separate devices for different activities	20.0%	263
separate payment methods for different activities	21.8%	286
none	7.3%	96
other		47

The responses also identified the following additional categories of tools and strategies:

- password/pin
- separate virtual machines
- different operating systems
- carefully select recipients
- elliptic phrasing
- divided messages
- clean up browser cache and cookies
- security token (for two-factor authentication)
- authentication tools
- flash cookie removal tools
- anti-malware, spyware, antivirus and firewall
- certificate authority pinning and analysis
- generate fake but plausible Web traffic
- obfuscation tools
- private network
- virtual credit card
- hardware encryption

Q. Is encrypted communication the default mode for any of the tools you use?

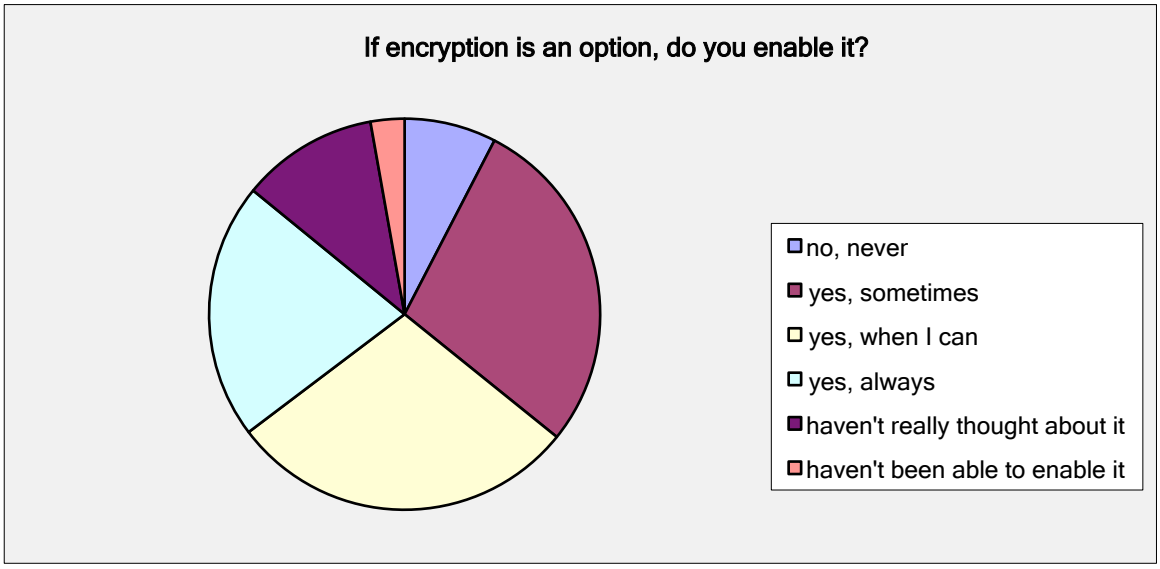
There were 1319 responses to this question.



The responses were fairly evenly divided between “yes” and “no”, 37.8% and 38.7% respectively.

21.7% responded “did not know” and 1.8% responded “don’t know and don’t care”.

Q. If encryption is an option, do you enable it?



There were 1296 responses to this question.

Only 7.8% responded that they never enable encryption. However, a further 11.3% responded “haven’t really thought about it”.

The majority responded that they enable encryption at least when they can (78.3%).

2.8% (36 respondents) responded that they haven’t been able to enable encryption.

Q. If you found it difficult or impossible to enable encryption, what obstacles did you encounter?

There were 393 responses to this question.

The reported obstacles include:

Insufficient information/guidance

- inadequate user manual for application
- not knowing how to install or use it
- lack of technical sophistication
- difficult to choose between encryption types and modes
- hard to understand the different types and options
- not knowing when or how to turn on encryption
- lack of encryption fluency

Usability

- usability
- user interface/user experience
- extra steps involved
- not user-friendly
- hard to configure
- too onerous
- time
- encrypted email is difficult to use
- application does not have built-in encryption
- absence of easy opt-in to enable encryption
- unsure if changing settings affects other aspects of the OS, etc.
- no method to detect if encryption is on or off
- using it across multiple devices
- problems with website usability
- managing public keys
- exchanging keys with other users
- key management
- key revoking and distribution
- fear of losing keys and not being able to access documents
- having to change passwords frequently
- misplacing usernames and passwords
- inconvenient long strings of letters and numbers that need to be read out
- confusing
- complex
- slow
- difficult to configure
- having to enable every time the device is connected to the Internet (e.g. VPN on iPhone)
- problems using a VPN
- unavailable for some systems

Dependency on other users

- lack of other people using it
- the other user (in the communication) does not use it
- not widely accepted or used
- lack of/slow adoption by other people
- convincing other users to install/enable secure communications tools or plugins
- having to encrypt with a third party
- the network effect

Incompatibility/interoperability hurdles/poor tools

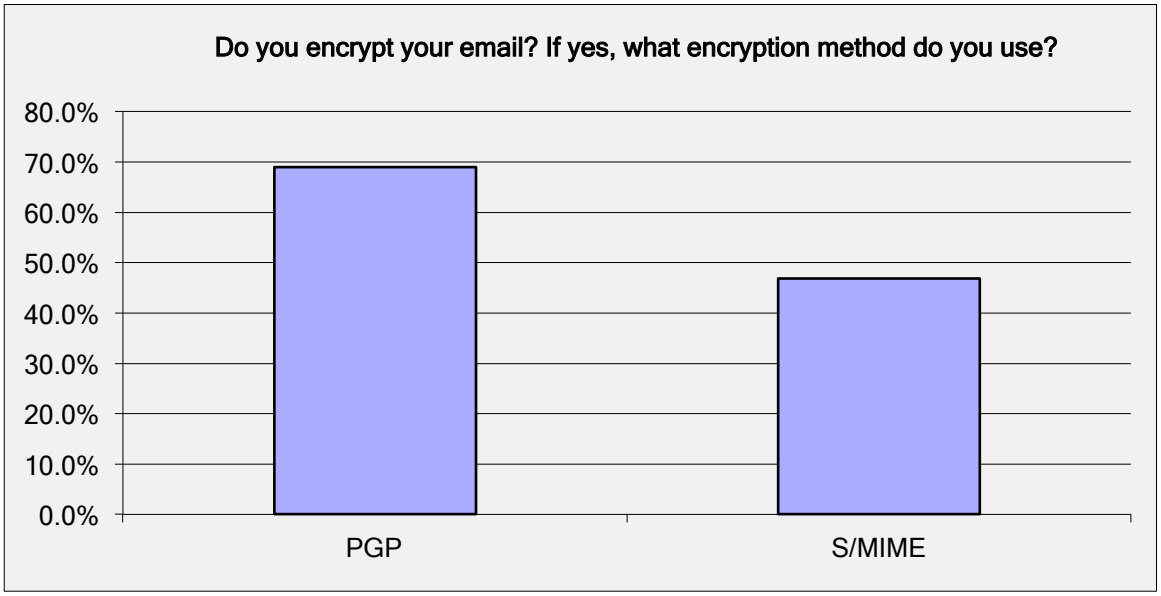
- too many incompatible tools
- incompatibility (e.g. between encryption and communications software)
- lack of interoperability with other users' platform choice
- other users need to have the same software for it to work
- cross client encryption is not available
- platform unavailability
- closed source/suspicious vendors
- lack of transparency

- not integrated with communication tools (e.g. Web mail)
- insecure encryption algorithms
- trusting certificates (particularly self-signed certificates) and for which uses/applications
- lack of standards
- service is not offered in an encrypted form
- missing features
- decryption tools/could be decrypted
- firewalls
- proprietary software
- passphrase timeout
- no open encryption
- poor key/certificate management tools
- not supported by vendor
- many websites do not offer encryption
- not supported by the application or service

Other

- expired or invalid SSL certificates (for websites)
- hash-based message authentication code (HMAC) issues
- trust
- reliability
- not wanting to store a private key on a device connected to the Internet
- cost
- policy restricted
- mobile network carrier
- port filtering
- VPN blocking

Q. Do you encrypt your email? If yes, what encryption method do you use?



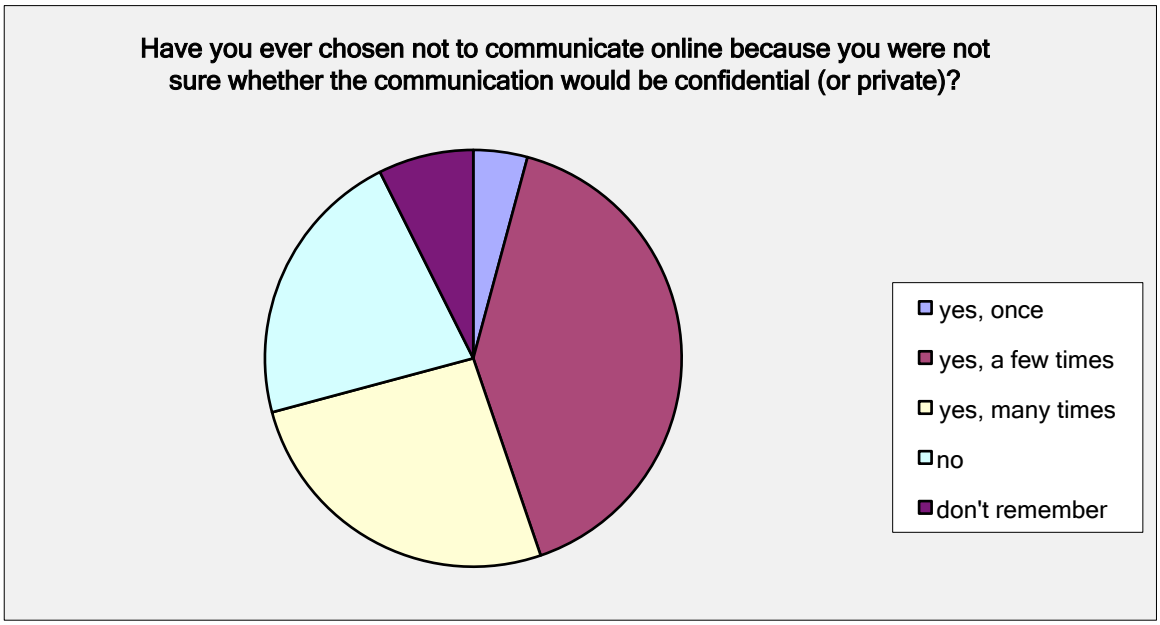
There were 525 responses to this question.

Other reported tools included:

- GPG/GnuPG
- own mailer server with VPN tunnels
- transport encrypted by HTTPS or VPN (but not message)
- STARTTLS
- server-based solutions like TLS between Message Transfer Agents (MTAs)
- Kerberos
- Exchange plug-in
- Protonmail
- Stenography
- Web mail (using SSL/TLS)
- HUT GNOS-V
- Virtru

Q. Have you ever chosen not to communicate online because you were not sure whether the communication would be confidential (or private)?

There were 1319 responses to this question.



70.9% responded that they have at least once and for many, on more than one occasion, chosen not to communicate online because they were not sure whether the communication would be confidential (or private). 7.4% responded that they did not remember.

These are some of circumstances where respondents reported they chose not to communicate online:

Unknown or suspicious "communicator"

- sender unknown or hosting server unknown/uncertain
- suspicious/untrustworthy website or email
- messages soliciting money

- “any time something looks the least bit dodgy”
- when the browser reports that a certificate is untrusted
- intrusive source
- spam

Surveillance

- during Arab Spring revolutions
- countries that engage in censorship/surveillance
- employer monitoring/surveillance

Untrusted device, application or access to the network

- when using a public computer (e.g. in kiosk) or public WiFi
- discovered email had been compromised
- suspected hacked account (e.g. email, Skype)
- tool claiming to encrypt the communication, when, in reality, it wasn't the case
- website that requests personal information without using HTTPS
- website that swaps between HTTPS and HTTP during purchase steps
- insecure connection
- sites that ask for a password, but don’t provide encryption
- travelling in a foreign country

Unable to use encryption or other tools

- if a recipient refuses to set up email encryption
- unable to use VPN
- if a merchant website did not offer encryption
- if a website requests information without offering HTTPS

When communicating certain types of information

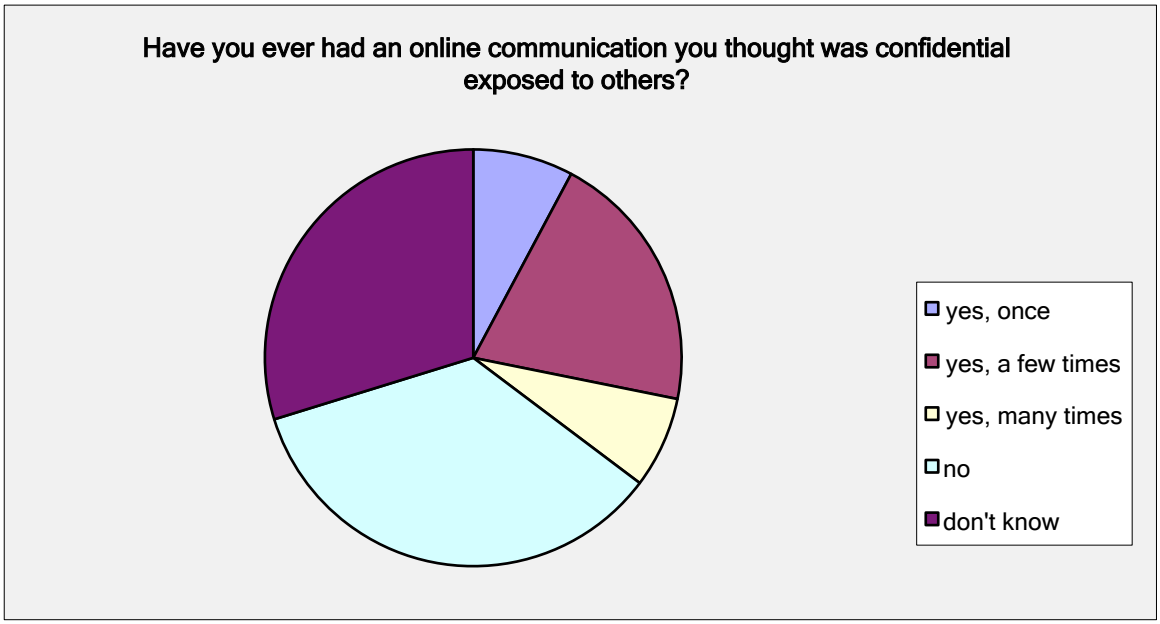
- to avoid sending passwords and other personal/confidential/sensitive information
- for sharing of cryptographic material (e.g. key exchange)
- to communicate login information when an encrypted solution is not available
- to communicate passport, drivers license, credit card details (not via email)
- sharing bank account information/financial information
- sharing a business idea/developing a business proposal
- sharing a password or pin with family
- sharing personal information/private matters
- communicating medical matters
- commercial confidential information (e.g. that would disclose intellectual property)
- communicating about government sensitive/official information
- legal professional privilege
- job interviews
- information that could incriminate me

Other

- concerns about the recipient's security
- "personal information that I don't want databased"
- to have no accessible digital record
- if a forum requests more information than the individual wants to provide
- information that the individual would not want recorded in writing
- "anything that I would not put on a postcard … I do not put into an email"
- in the context of undertaking social science research (gathering information in contexts where topics are sensitive and confidentiality is essential)
- "sharing documents/information that we felt ought not to get into the wrong hands"
- multiple modes for portions of a communication

Q. Have you ever had an online communication you thought was confidential exposed to others?

1,312 respondents answered this question.



35.3% of respondents reported that they had an online communication they thought was confidential exposed to others on at least one occasion. 29.8% reported that they did not know whether this had occurred. 35.0% responded "no", however, it is possible that they also experienced unauthorised disclosure of a confidential communication without their knowledge. One of the respondents summarised this well:

> *"This is the problem. I'm sure some of my communications have been exposed to others, but I have no way of knowing".*

The respondents who answered “yes” were invited to provide details of the circumstances in which their confidential communications were exposed to others. These are some of the reported circumstances:

Monitoring/surveillance/hacking/insufficient security

- ads based on search history and/or email content
- posts on social media to “friends” exposed to social media monitoring tools
- communications exposed using WiFi provided by hotels
- operating system leaked real and user names while connecting to public WiFi
- personal email hacked or recipient’s email hacked
- social media account hacked
- website hacked – username/password obtained
- communication with professor viewed by third parties
- government agency surveillance
- employer monitoring of employees’ email, messaging
- telecommunications authority’s notification platform hacked and passwords stolen
- targeted by a military virus
- “man in the middle” attacks
- contents of mail server dumped to public site in Scandinavia
- stolen credit card number

Action taken by others

- work colleagues forwarding emails or including others in reply
- email messages forwarded without permission
- “… emails to me have been blind copied to others”
- recipient intentionally or carelessly reveals content
- incorrect handling by recipients
- private emails being quoted on blog
- someone “outed one of my [anonymous] profiles”
- people replying to an encrypted message unencrypted, or sharing confidential information via insecure channels
- whiteboard pictures of Skype meeting published on a blog
- dating site photos

Action taken by the user

- mistakenly sent confidential email to wrong recipient or distribution list
- accidental posting on Facebook
- accidentally sending a “reply all” message
- accidentally submitting the password in the wrong GUI (Graphic User Interface)
- accidentally used “the wrong browser” when ordering a product
- posting on forums which can be found and viewed using Google Search
- unaware that a person was on a VoIP call
- unaware that a mailing list was public
- told to create an account for sharing in the context of a conference, which turned out to a social media platform

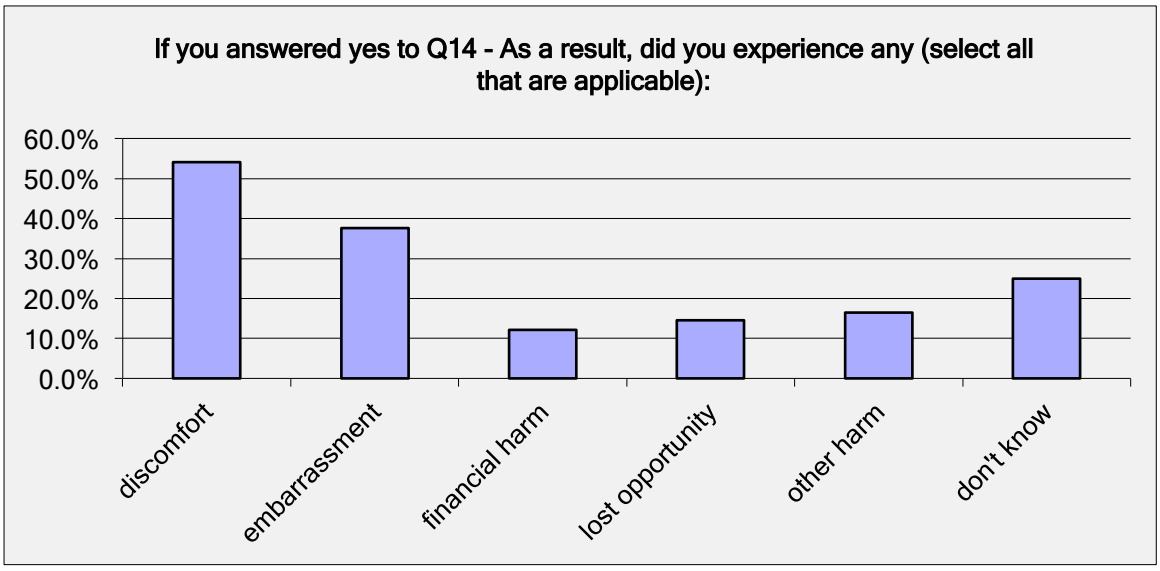
Other

- using iMessage - sent passwords as SMS, but iMessage sent via IP and stored them on the server
- domain names for internal use observed by external robots
- messages stored on service provider server

Q. As a result did you experience any discomfort, embarrassment, financial harm, lost opportunity, other harm, or don't you know?

556 respondents answered this question.

Here are the results:



One of the respondents commented:

> *"I believe I must have had confidential information exposed to the US and UK security services at least as a result of the mass surveillance activities that Snowden exposed. My reaction was a sense of anger, violation and increased wariness about what thoughts I committed to those platforms. Services like Google are so pervasive and difficult to substitute that (after a brief period of trying to switch to others) I am back with Google, Skype, Facebook, etc. - I just don't like it."*

Another said:

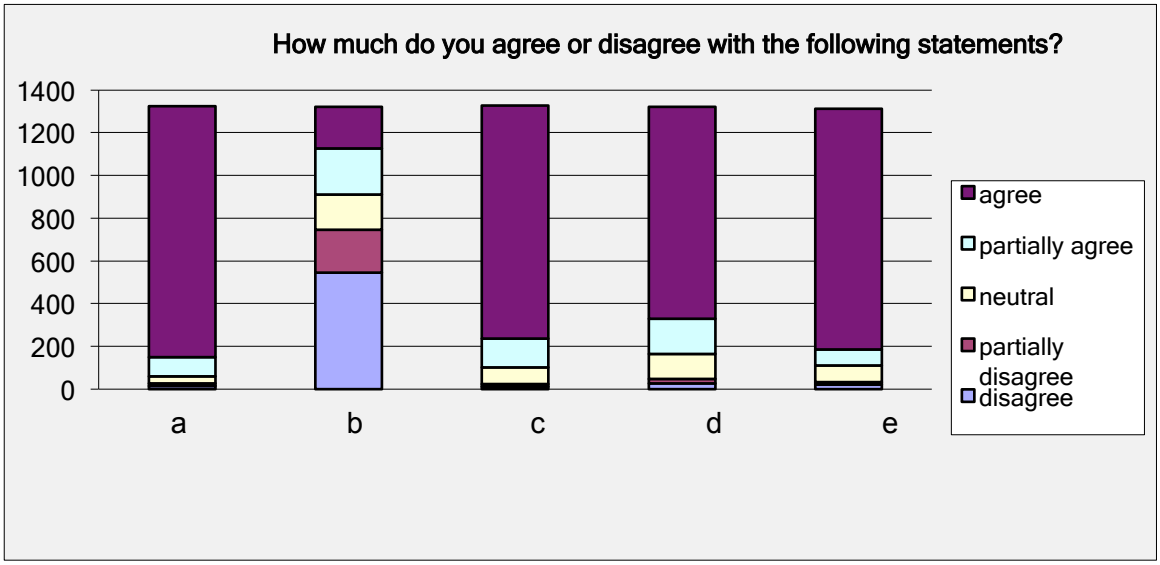
> *"Often I can't tell what the impact is until much later, and then it is too late and too complex to resolve adequately. I have had my credit card stolen apparently through online theft, passwords compromised, and had to start using very complicated passwords and two-factor [authentication], which is inconvenient."*

Other types of reported harm include:

- loss of reputation
- feeling that privacy has been violated
- feeling of being observed
- self-censoring
- feeling powerless
- feeling of insecurity
- reprimand from supervisor
- others' experienced hurt feelings
- exposed bargaining position led to withdrawal from negotiations
- having to engage credit report monitoring due to compromised accounts
- reduced/loss of trust
- erosion of authority
- spam
- subject of an investigation

However, one individual proudly reported the successful prosecution of the perpetrator of an intrusion into his or her "personal system".

Q. How much do you agree or disagree with the following statements?



a = When I communicate, only the intended recipient should see the content

b = Confidential communication is a great idea, but it is just not worth the extra inconvenience

c = I don't want intermediaries to see the contents of my communications (ISPs, email service providers, carriers, social network service providers)

d = I don't want my government to see the contents of my communications

e = I don't want other governments to see the contents of my communications

Most respondents agreed or at least partially agreed with all the statements except b.

Here are some of the comments accompanying the answers:

Regarding convenience

- *"I chose "partially disagree" for (b) because often it isn't worth the extra inconvenience. For example, when the recipient doesn't care about the confidentiality of the communication enough to use a secure mode of communication—I would prefer to communicate with the person, because they are a friend and will sacrifice the confidentiality of that communication for them. But I won't say things that I might via different modes of communication."*

- *"often confidential communication is a "nice to have". In other words, I would often prefer confidential communication, but because it's not always a requirement, I frequently choose unsecure communication methods due to convenience."*

- *"For personal email, at times i agree it is not worth the inconvenience. However for work, whatever perceived inconvenience there is, is worth it. …"*

- *"Confidential communication is a great idea, but it is just not worth the extra inconvenience - It needs to be made easier."*

- *"I think confidential communication is worth the extra inconvenience! If I knew of a way to send encrypted mail, I would be more comfortable putting sensitive information in it."*

- *"I partially disagreed with (b) because it depends on the communication. For many personal communications, even though I don't believe the government or service providers has any right to invade my communication without warrant, encrypting seems a gratuitous step and isn't worth it. However, there are many communications for which it is crucial and accordingly "worth it."."*

- *"it IS worth the extra inconvenience, but sometimes it's just not an option at all"*

Regarding types of communications

- *"c) For me this depends a lot on what I'm communicating. Some communications I expect will be semi-public (Social Media for one thing) and other communications should definitely remain confidential."*

- *"A lot of my communications are in the context of organizational transparency, So that part needs to be public. On the other hand, a lot of my personal communications would rather be private… ."*

Regarding government access

- *"lawful interception with a court order for severe criminal offense, assuming that there is a strong parliamentary oversight, are OK."*

- *"I recognize the need for governments to protect their citizens in certain circumstances"*

- *"Democratically-sanctioned due process with strong transparency is key for govt. access to private communications for law enforcement"*

- *"Other governments do not have any right to intrude my privacy. And reg mine, I have nothing to hide."*

- *"I have nothing to hide from GCHQ or the NSA. If they want to store terabytes of useless information, I can't stop them, and encrypting my conversations and downloads will only draw attention to them."*

- *"The arguments for and against governments viewing private communications are nuanced. I believe there is a balance to be struck between privacy of communication and maintenance of social order. I also believe the current balance, as it seems to be, is wrong. The problem is international, given governments spy on each other and everyone else, so the solution has to be international too. …"*

Regarding trust

- *"I trust .. Google and Facebook and I do not trust any government, especially post-Soviet"*

- *"In order to uphold my integrity, meaning that I stay true to myself, others and consistent in my actions and thoughts; I need to be able to trust that the tools I use to form my opinion about myself and others aren't compromised"*

Regarding theory and reality

- *"In theory, I totally agree/disagree, but in practice I have compromised my own desire for privacy because there are too many people I wish to communicate with who do not care enough about privacy to be troubled with encryption."*

Q. What information or guidance regarding protecting the confidentiality of your communications would you find useful?

There were just over 500 responses to this question. They included:

Better tools

- better and easier to use tools
- confidentiality by default
- simpler encryption software
- easier implementation of PGP
- alternatives to services that do not offer encryption
- privacy by design approach
- encryption by default; user choice to remove
- encryption that runs in the background
- standardisation of privacy settings
- opportunistic encryption
- fix certificate warnings so they are useful

Guides

- "how-to-guides"; e-guides; tutorials; best practices; scenarios; ways to implement tools; learning circles; short movies with case studies; education through media and schools; worldwide campaign
- how to activate and use privacy settings
- information about confidential communications, including how and when to use them
- more information on how to secure online communications
- how to use encrypted communications and not draw attention to yourself (e.g. Tor)
- step-by-step instructions for encryption and updated modules with newer encryption standards
- simple explanation of how to use encryption keys
- how to detect and turn off "geolocator" apps
- clearer understanding of the engineering limitations of different technologies vis-à-vis confidentiality
- browser guidelines; how to browse anonymously
- updates about new tools
- how to convince others to set up encrypted email
- how to prevent identity theft, how emails and buying patterns are used by telemarketers and search engines
- how to use social media securely
- Tor tutorials
- the implications of loss of encryption keys
- internal policies; company guidance

Information sources/services

- dedicated website with information on encryption technologies (and quick start guide)
- better analysis of the relative effectiveness of encryption technologies
- a security efficacy index
- a list/map of countries that ban or limit the use of encryption
- threat model "walk-through" tool
- centralised authoritative resource
- comprehensive list of vendor tools/platforms which have encryption or other means to protect privacy
- guidance that is not provided by big enterprises, guidance that is provides by sites that care for the rights of Internet users
- information on standards
- information on source code and mathematics; likelihood of backdoor and/or government involvement

Transparency

- ability to tag information as confidential
- icon that is as ubiquitous as the SSL lock icon
- prominently displayed (large, brightly colored) uniform and simple icons across all sites and platforms that act as a green-yellow-red instant recognition mode for site safety and privacy
- highlighted options for confidentiality for each service
- publicise and rank companies and applications by their level of privacy implementation
- warning that the confidentiality/security is not sufficient for the transaction
- to be warned when a service has no encryption and gives a pop-up option for encryption
- data integrity checksums published at the bottom of all web pages

- information about whether a communication is confidential/encrypted/authenticated or not
- requiring websites and apps to be clear about what they are using your information for
- clear and easy accessible end user agreements and statements of confidentiality from all service and solution providers
- mechanisms to indicate which parts of communications are protected
- software to provide notifications of privacy violation
- services purporting to be secure must publish external security review results
- indications of who is accessing your communications
- information about communication information passed to third parties (e.g. advertisers and intelligence agencies)
- services purporting to be secure must publish external security review results
- services must disclose security breaches to customers
- Information regarding assurance of the confidentiality should be given prior to engaging

Surveillance

- exposing online surveillance
- full public disclosure of government and private tracking and surveillance activities
- transparency on the role of government intelligence agencies
- warrant data canaries
- legally mandated disclosure of who has access to messages that a user sends through a platform
- legal requirement that the user be informed when there is packet-sniffing or the use transparent proxies
- detailed information on government ability to require service providers to supply users' information
- services should make clear whether they can obtain clear version of data they hold or data that transits through them

Legal environment

- local and international privacy laws
- a solid judicial base to expedite prosecution of privacy infringements
- clear charter on limitations of power (enforcement, national security etc.)
- guidance in laws, rules and regulations
- class actions against companies that don't implement effective security for confidential information
- fee payable to the user for use of personal information

Other

- methods for finding weaknesses in confidential communication (e.g. allowing encryption to be defeated)
- verified functionality backed by non-severable liability
- a way to assess the trust that one can place in encryption tools
- a way to avoid having data stored in, or routed through the US
- access should be auditable
- privacy should be free and not a service for which you would pay more to enable
- replace username and password with electronic digital signatures

Concluding Remarks

We would like to thank everyone who participated in this survey. The responses to this survey are helpful in identifying Internet users' needs and expectations with respect to confidential communications, 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.

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave.
Suite 201
Reston, VA 20190
USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881
Email: info@isoc.org