Internet Society

English

Glossary of Internet Terms

91 Key Terms Explained — Making the Internet Everyone's Business

We're using the Internet all the time for various reasons, but how familiar are you with what's going on under the surface?

We believe that the Internet is for everyone and that it should be understandable for everyone. If you aren't familiar with the terminology used to discuss the Internet, it can be easy to gloss over conversations or news stories about Internet topics that could greatly impact your daily life.

This glossary provides terminological overviews of 91 key Internet-related terms that help you understand and make informed decisions about your daily online activities. Its brief explanations are organized alphabetically—in English, French, and Spanish—to help everyone understand and participate in Internet-related discussions.

As the Internet of tomorrow faces many challenges, now is the perfect time to understand it better. Being better informed means being equipped to make the right choices on how you use, experience, and influence the Internet of our future. The Internet is for everyone, and it is up to all of us to preserve and care for it.

A

Access

Internet access is the ability to connect to the Internet.

Alternative Access Solutions

Innovative and new ways to connect people to the Internet, thereby addressing the gap between those with and without Internet access.

Archiving

Storing electronic information that you no longer need to use regularly. Deleting online content often only removes it from public view, but it can be persistently archived forever. Even deleting your account isn't a guarantee that your content will be deleted as it may still be accessible through other means.

TERM	DEFINITION
Asymmetric Digital Subscriber Line (ADSL)	A type of access technology in which, as a user, you can download faster than you can upload.
Autonomous System (AS)	Autonomous Systems are the big networks that make up the Internet. As such, every computer or device that connects to the Internet is connected to an AS and each AS is operated by a single large organisation such as an Internet Service Provider.
Autonomous System Number (ASN)	A number that is used to identify networks within the routing system, which is the pathway that Internet Protocol (IP) packets of data use to travel from their origin to their destination. AS numbers are assigned by Regional Internet Registries known as RIRs.
Application Service Provider (ASP)	A business or organization that provides access to applications or services on the Internet.
Asynchronous Transfer Mode (ATM)	A technique used by telecommunication networks to transfer data at high speeds.

B

Backdoor Access	Any method that gives a third-party access to encrypted data thereby creating a major vulnerability that weakens the security of citizens and the Internet at large. "Backdoor access" can be possible because of a security flaw that has been unintentionally left in a system, or it can be deliberately designed (e.g., at the request of a government).
Bandwidth	The capacity of a network to transmit a certain amount of data within a fixed amount of time. Higher bandwidth means faster Internet speeds, allowing users to download, upload or access information online more quickly. Bandwidth is measured in terms of performance in bits per second (bps), kilobits per second (kbps), or megabits per second (Mbps).

TERM	DEFINITION
Big Data	Every online search made, webpage visited, e-mail or message sent, product or service purchased leaves hundreds of thousands of electronic tracks about an individual. This data is collected by corporations, or governments who then use these for specific intents and purposes to further their needs. This type of data collection is generally seen as negative unless we give our explicit and knowing consent. In some cases, the use of big data can increasingly be used for new insights by using machine learning but it can also represent a source for risk of criminal attacks. Big data can result from either active or passive collection of data such as CCTV, or scientific systems like oceanographic, environmental, and astronomy research.
Border Gateway Protocol (BGP)	Is used to direct traffic across the Internet. Networks use BGP to exchange "reachability information" – networks they know how to get to. Any network that is connected to the Internet eventually relies on BGP to select path and reach other networks.

C

Client-side Scanning (CSS)	Systems that scan message contents—i.e., text, images, videos, files—for matches against a database of inappropriate content before the message is sent to the intended recipient. Another example of CSS is anti-virus software, which may do this to find malware in files and messages you receive. As CSS happens on the user's own device, a key question is whether it is done with the knowledge and consent of the individual.
Community Networks	Communications infrastructure deployed and operated by citizens to meet their own communication needs. Community networks are about bringing affordable Internet to a community–by the people, for the people model.
Content Blocking	Worldwide and growing trend of governments blocking the Internet to prevent access to illegal content (e.g., for child protection or national security protection). However, apart from issues relating to child pornography, there is little international consensus on what constitutes appropriate content from a public policy perspective. The proportionality of content blocking can also depend heavily on the technical way it is done. For instance, an Internet shutdown, or preventing all access to a social media platform, are examples of content blocking, but highly likely to be considered disproportionate.

TERM DEFINITION

Content Delivery Network (CDN)

A network of servers that stores content near end-users, making it more readily available (sometimes also called a Content Distribution Network).

Content Provider

A person or organisation who provides information via the Internet. E.g. articles, videos, or podcasts.

Content Regulation

Limiting the user's freedom of access to information. This has recently been a matter of public concern and debate with the need to raise awareness amongst its users, and more widely, of the existence of national laws and measures which pose risks to human rights. Censorship being the number one concern.

Cookies

Internet cookies refer to the piece of data that is stored in your computer when you visit a website so that it later remembers your preferences making your browsing experience personalized and convenient.

However, the convenience comes at a high price for your privacy and security. Best practices show the need for always checking your privacy settings to manage your possibility to block third-party cookies.

Country Code Top-Level Domain (ccTLD)

Two letter code used to indicate countries in the Domain Name System (DNS) —e.g. .IN or .FR

Customer Provided Equipment (CPE)

The devices needed by customers to establish an Internet connection, typically a home router, or broadband modem.

Cybersecurity

The practice of protecting the security and privacy of networks and programs from digital attacks by using technical and technological solutions. Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users via ransomware, or interrupting normal business processes. Not every crime that occurs on the Internet is covered by the term cybersecurity.

D

Data Center

Refers to a large computing facility with dedicated data storage space, data communication lines, power supplies, and Internet backup systems.

TERM	DEFINITION
Data Privacy	Refers to the protection of an individual's personal information (online data) from unauthorized access, use, or disclosure. It involves ensuring that individuals control how their data is collected, stored, processed, and shared by organizations or entities. There are many helpful online privacy tools. Use them to protect your online privacy, and to keep track of what information you're sharing as you browse.
Data Security	Measures used to protect all types of personal and non-personal information online (data), so that it remains confidential and available. This involves using encryption and controlling access practices to secure and safeguard it. Find out more on Best Practices for Data and Information Security.
Digital Divide	The gap between those who have Internet access and those who don't. The digital divide is multifaceted so it includes many factors that contribute to lack of access, such as physical connectivity, affordability, quality of service, and relevance.
Digital Equity	The concept that every person should have equal opportunity to access digital technologies, including the Internet.
Digital Inclusion	A comprehensive approach to provide equitable access to digital services and technologies for everyone (e.g. youth, women, elders, minorities, and persons with disabilities)
Digital Footprint	A digital footprint refers to the trail of data that is left behind by an individual's online activity. It includes all the digital interactions and information associated with a person across various online platforms and services, including social media, online purchases, web browsing history, app usage and location data. Our digital footprints increasingly include data collected passively by systems like numberplate recognition, urban CCTV, fitness trackers, mobile phone networks, and so on.- Our digital footprint encompasses data that does not simply result from your own deliberate online activity. While it is not possible to have zero digital footprints, you can take simple steps toward reducing your digital footprint.
Digital Literacy	Is creating and deepening understanding, and knowledge on how the Internet and related technologies affect and benefit you as a user. It refers to the ability to effectively find, evaluate, create, and communicate information using digital technologies.

TERM	DEFINITION
Disinformation	Also known as fake news, it is information that is deliberately created to deceive people, which is different from misleading information, otherwise known as "misinformation."
Distributed Denial of Service (DDoS)	A specific type of cyber attack, often executed by sending unbearable amounts of traffic to the victim from many locations across the Internet.
Domain Name System (DNS)	A system that helps people navigate the web. The system turns domain names, such as example.com, into Internet protocol (IP) addresses, such as "192.0.2.1," allowing web browsers to get to websites and other Internet resources.
Domain Name System Security Extensions (DNSSEC)	Protocol extensions that introduced authenticity and integrity protections to the Domain Name System (DNS). The primary goal of DNSSEC is to address vulnerabilities in the traditional DNS system, which can lead to unauthorized redirection of internet traffic and compromise the accuracy and reliability of domain name resolution (the process of translating a web address to a numerical IP address).

E

Encryption	Encryption protects data from unauthorized viewing, by making it unintelligible to anyone who does not have the key to decrypt it. An unauthorized person can still access the encrypted data, but it will be indistinguishable from random data. Encryption can be used to protect both stored and transmitted data, and plays a critical role in protecting day-to-day digital activities like online banking, and shopping, and making sure private messages stay private.
End-to-end Encryption (E2EE)	E2EE is the process of encrypting data at the point of transmission, and decrypting it only at the point of receipt. The aim of E2EE is to ensure that no intermediaries (such as email or messaging servers) can access the contents of communication, even if they play a legitimate part in relaying the data from sender to recipient.

F

Fragmentation

Internet fragmentation is the division of the unified, open, global Internet into smaller, isolated networks subject to different rules, regulations, and technical standards—which may not be able to interconnect or interoperate seamlessly. This is a big deal as it results in blocked sites affecting your online experience, so here is why you should pay attention to this issue.

Freemium

A business model in which a company offers basic or limited features to users at no cost and then charges a premium for supplemental or advanced features. When it comes to the Internet, "Free" doesn't mean "free": it usually means you pay through the data about you being sold to a third party.

File Transfer Protocol (FTP)

One of the first protocols used to exchange files over the Internet.

G

"Ghost Protocol" Proposal

Claims by governments that a third party can be added to listen in to conversations for law enforcement or national security purposes without weakening the encryption used to protect the messages. This amounts to having a "silent listener" in the room, for what you thought were confidential conversations. It negatively impacts the trust relationship between users and service providers.

H

Hypertext Transfer Protocol Secure (HTTPS)

Secure communication channels to codify the exchange of files over the web (e.g. text, sound, images, video) between the user's computer device and the server. Before entering any website make it a habit to check if it is secure making sure it begins with "https" rather than "http."

I

Innovative Access Solutions

New ways of providing successful connectivity—e.g. fiber broadband networks and 5G mobile networks that are developed to address the problem of unequal access to the Internet.

TERM	DEFINITION
Internet	It is a "network of networks," made up of almost 70,000 independent networks that use the same technical protocols and choose to collaborate and interconnect.
Internet Engineering Task Force (IETF)	Founded in 1986, it is the body that develops standards and protocols for the Internet.
Internet Ecosystem	The different players who make Internet work via an open, transparent, and collaborative model that relies on processes that are local, bottom-up and accessible to users around the world.
Internet Exchange Point (IXP)	A physical and usually neutral location where different networks meet to exchange local traffic. IXPs make the Internet faster and affordable.
Internet Governance	The multi-stakeholder approach that is widely accepted and used as the optimal way to make Internet policy decisions for a globally distributed network.
Internet Service Provider (ISP)	A company that is paid to provide a high speed Internet access and other related services such as tech support, equipment rental or email services to individuals and industries. They serve as the gateway for users to access online content, services, and applications.
Internet Shutdown	An intentional disruption of Internet-based communications within a specific geographic area, rendering online services inaccessible or effectively unavailable, for a specific population. Examples include attempts by governments to control the flow of information during elections or national exams.
Internet Society (ISOC)	A global charity with the mission of promoting and developing an open, secure, and trustworthy Internet for everyone. The Internet Society also provides the legal and financial framework for the IETF.
Internet Standards Organization	Refers to the Internet Engineering Task Force (IETF), which is the premier standards development organization (SDO) for the Internet. Founded in 1986, it makes voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet. But as stated on its site, in no way does it control, or even patrol, the Internet.

TERM	DEFINITION
Internet of Things (IoT)	Internet connected everyday objects that have a powerful data analytic capabilities that promise to transform the way we work, live, and play. IoT is widely debated as it raises surveillance concerns and privacy fears (E.g. smart home appliances and electronic devices).
Internet Protocol (IP)	Like the physical world, one needs an address to get around in the online world. As such, this is a set of rules consisting of sequences of numbers that governs the communication and exchange of data online. Both the sender and receiver should follow the same protocol in order to communicate the data.
Internet Way of Networking (IWN)	The foundation of a strong and successful Internet that works the way it does thanks to the Five Critical Properties which, when combined, drive how it operates and evolves.
IP Address Spoofing	Also known as Internet Protocol (IP) spoofing. It is a fraudulent activity of fabricating a source IP address field in IP packets with the purpose of hiding the identity of the sender or pretending to be another computing system.

L

TERM	DEFINITION
Latency	The time it takes for data to travel between sender and receiver. Network latency is a significant Internet connectivity issue measured in milliseconds and affecting end-users' online experience.
Low Earth Orbit (LEO) Satellites	These satellite systems are recent solutions used to provide reliable communication services that solve the end-to-end delay also known as communications latency.
Local Content	Content that is locally generated, relevant and adapted to the local realities of a particular country. Such contents drive the growth of local, regional, or national Internet as they are relevant to the communities, and economies of that specific country.
Local Internet Registry (LIR)	A Local Internet Registry (LIR) is an organization or entity that is responsible for distributing and managing Internet Protocol (IP) address space and Autonomous System (AS) numbers within a specific geographic region or service area. LIRs play a critical role in the allocation and administration of IP addresses and AS numbers, helping to ensure the efficient and effective functioning of the Internet.

M

Machine-in-the-Middle Attacks (MITM)

A threat to data confidentiality, in which a third party intercepts a communication between users (or machines). In such an attack, Alice and Bob think they are talking to each other, but in fact Mallory (in the middle) is masquerading as both of them, and therefore reading, and potentially tampering with, their messages.

Malware

Malicious software that infects computers for various reasons, including to extract data from them, or to control them remotely – for instance as part of a DDoS attack. But malware doesn't only affect Internet-connected computers. For instance, one way of spreading it is to leave infected USB keys around.

(Mandatory) Data Localization

Refers to government requirements that control the storage and flow of data to keep it within a particular jurisdiction.

Mass Surveillance

Untargeted or "blanket" surveillance of individuals' behaviour or communications. In the Internet context, this is the goal of some government policies, particularly in repressive or authoritarian societies. Regardless of the stated justification (which may be for national security, or to counter terrorism or child abuse), mass surveillance is, by definition, disproportionate in a democratic society. This practice threatens online freedom of expression, and the safety, privacy and autonomy of the citizen.

Measuring the Internet

Provision of accurate data and analysis to understand how the Internet is evolving to protect it from the forces that threaten it, like Internet shutdowns.

Misinformation

False or inaccurate information which results from simply getting the facts wrong.

Multi-Stakeholder Approach

A model of governance that involves the participation and collaboration of various stakeholders from different sectors of society in decision-making processes related to the governance and management of the Internet. Unlike traditional models of governance that are characterized by top-down, hierarchical structures and centralized control, the multi-stakeholder approach emphasizes inclusivity, transparency, and collaboration among diverse stakeholder groups.

Mutually Agreed Norms for Routing Security (MANRS)

A global initiative to protect the Internet by improving the security of the Internet's global routing system through agreed norms.

O

Open Source

A decentralized software development model that encourages open collaboration by making the source code freely available for any peer modification/improvement.

Open Systems Interconnection (OSI)

The Open Systems Interconnection (OSI) model is a conceptual framework that standardizes the functions of a communication system into seven distinct layers. The model provides a systematic approach to understanding and designing network protocols and communication systems.

P

Peering

Internet peering is a process through which Internet service providers (ISPs), content delivery networks (CDNs), and other network operators establish direct connections between their networks to exchange traffic and facilitate the efficient routing of data between their respective customers and networks. Peering allows networks to exchange traffic without the need to pay transit fees to third-party network providers.

Peer-to-Peer

Protocols where entities share information and resources directly, without relying on a centralized server. Typically seen in file sharing and blockchain networks.

Personal Data

Any information that when pieced together can be used to identify a particular person.

Phishing

An attack that attempts to steal your money, or your identity, by getting you to reveal your personal information, such as credit card numbers, bank information, or passwords, on websites that pretend to be legitimate.

Point of Presence (POP)

A location, facility or access point where networks connect with each other.

Public-Key Infrastructure (PKI)

A structure of encryption keys, certificates, and trusted third parties, used to operate public-key (or asymmetric) encryption. This is a form of encryption in which the key used to encrypt data is not only different from the key used to decrypt, but can also be safely published without compromising the confidentiality of the encrypted data.

TERM	DEFINITION
Pulse	The Internet Society Pulse is a central website that aggregates reliable and accurate Internet data from many sources giving insight into such matters as the impact of Internet shutdowns, and the resiliency of a country's Internet. This offers background information and context to journalists covering Internet issues around the globe.

R

Ransomware	A type of malware attack whereby hackers can infiltrate your data. Here are 6 tips for protecting yourself against it.
Right To Be Forgotten	The legal right of an individual to request that specific information about them should be dissociated from their name, as an obstacle to searching for it online. (For instance, searching for "John Smith fraud scandal" would not retrieve the information in question.)
Router	A device that receives and sends data between computers connecting the devices to the Internet and enabling them to communicate with each other.

S

Satellite Internet	The use of satellites called low Earth orbit (LEO) satellites to provide Internet access to the unconnected, particularly in rural regions. These systems at times introduce new security and privacy concerns.
Spam	Any kind of unwanted, and annoying e-mail, text message, phone call, or message that you receive in bulk from people or companies who want to advertise their products or broadcast their political or social views.
Surfing	The activity of exploring various websites and webpages on the Internet by using a web browser.

T

Top-Level Domains (TLDs)

Examples of these are .com or .org. The Internet regulation organization known as ICANN (Internet Corporation for Assigned Names and Numbers) is entrusted by the global Internet community with the responsibility to ensure the stable and secure operation of this Internet's root zone directory making them accessible on the Internet.

Transport Layer Security (TLS)

A widely used protocol that authenticates and encrypts data sent between applications over the Internet. E.g. used to secure web traffic.

U

Universal Access

Is part of the universal right of freedom of expression for people to have an inclusive, equitable and affordable Internet regardless of where they live or their origin.

Universal Acceptance

A principle of internationalization and accessibility related to achieving a multilingual Internet. The use of Latin-based alphabets should not be a precondition of using the Internet.

V

Voice Over Internet Protocol (VoIP)

VoIP allows the cheaper use of broadband Internet service lines to place and receive voice calls.

Virtual Private Network (VPN)

A VPN is a mechanism for creating a secure (virtual) network via what may be an insecure or untrusted intermediary service, such as the public Internet. It can be used to protect confidentiality and privacy.

W

Wireless Local Area Network (WLAN)

Common name for network technologies that connect two or more devices wirelessly, forming a Local Area Network (LAN) within a limited area Wi-Fi network.

World Wide Web Consortium (W3C)

An organization that establishes standards for web technologies.

Wireless Personal Area Network (WPAN)

An access point set up for a person (e.g. Wi-Fi sharing on a mobile phone).

The Internet is for Everyone

Founded in 1992, the Internet Society is a global charitable organization that believes the Internet is for everyone. Through our community of members, special interest groups, and 120+ chapters worldwide, we defend and promote Internet policies, standards, and protocols that keep the Internet open, globally connected, and secure.

Learn more at InternetSociety.org

Internet Society

Platinum Transparency 2024 Candid.

Charity Navigator ✦✦✦✦ FOUR-STAR

The Internet Society is a U.S. 501(c)(3) charity (EIN 54-1650477) with a multi-year top 4-star ranking from Charity Navigator.