The Free Internet Act
THE FREE INTERNET ACT

No seriously if you are not contributing or commenting/viewing; go away you 9gag/4chan trolls. <-9gaggers are not evil we opposed sopa <- Yet you troll facebook tributes pages of bullying victims. Your argument is as valid as Hitler going “But we opposed communism!”

v? - 29th February 2012

http://reddit.com/r/fia

I am the Shepard of the flock you guys need to do the work :P
If data gets deleted like b4, where could i back it up for you? like that.... Reverting document brb
Turned editing off

Public bulletin

Downing_Street_Cat Note:
Whoever thought it was a good idea to capitalise ‘data’, ‘upload’...etc. Should learn that IT IS NOT RUDDY NEEDED.
24/02/12 - Just another note: I have removed the child porn bit as if we can’t get it right then it WILL be used against us.

BeniwaAnon Qs:
24/02/12 - Should this be treated as an Act, Bill, Treaty, Agreement or even Protocol?
24/02/12 - Suggestion for definitions: P2P, Bittorrent, Magnet.

Anonymous:
Should we include specifically that data on any social websites (Facebook, Twitter, etc.) will not be monitored/deleted (or used in court) in very clear wording?

People need to make copies of this in case it “disappears” from Google Docs.

There needs to be a separate article describing the basic Internet rights of an individual or citizen.

Table of Contents

Title I – Definitions
Administrator – Any person who has:
1) The authority, permission, or right; and
2) The capability, including legitimate access to alter the hardware and/or software of an information system or service provider.
Unless:
(1) that person's authority, permission, right, or access are no greater than the majority of other users of the information system or service
or
(2) the greater authority, permission, right and access are functions of the information system or service.

Anonymous – Without reference to an true identity. Entirely without identification, or possibly pseudonymous if that pseudonym is not linkable to an Identity.

Anonymous Network - A network of computers whose sole purpose is to anonymize the traffic passing through it in order to hide the identity of a user. Including but not limited to; TOR, Darknet, Virtual Private Networks or Proxies.

Bandwidth - The breadth of data that can be successfully transported in a given period of time by means of network hardware without the occurrence of data loss; measured in bits per second.

Information System – Any system which may contain one or more of a person or persons, hardware, software and related infrastructure, that allow users, service providers or other information systems to receive, remove, process, store and distribute data.

Censorship – The restriction, method of restriction or acts that restrict the distribution, filter the content or modify any data whatsoever in an attempt to restrict the information from reaching

others who are eligible for its reception as per laws in place and the creators ideas and understanding of the propagation of data.

Child/Children – Any person under the age of majority for their country of residence, if not defined the universal franchise standard of 18 years of age shall be accepted.

Child Pornography – Any image or video that depicts a real human child or then the universal age of 18, in sexually suggestive nude photos or showing sexual acts between children or other adults nature as part of the content. For the purpose of this Act ‘real human’ refers to a person that has at some point been or is currently alive.
Exceptions to this rule, goes as follow:
Any form of digital or traditional artwork.
Traditional family memory photos, e.g. first bath or at the pool for the first time.
Materials that are used for education or scientific purposes, e.g. a documentary on an indigenous children under the age of majority for their country of residence, if not defined, (debating removing this section again)

Content – A work, a piece of information or data.

Creator – A person, group, or entity who creates or produces content or derives or modifies content from another creator or creators, as in but not limited to studios, artists, writers or programmers.

Data – A digital representation of information, including but not limited to video, audio or text, which may be readable by or transmissible between either a human or a machine or other information system such as a network of computers.

Download – The act of retrieving, transferring or copying data from an external or remote information system to a local storage medium or device including but not limited to mobile phones or other handsets, personal computers or other personal information systems.

Downloader – A user that has initiated a successful download of data. (?)

Educational use – The copying and distribution of data to a clearly defined group of people for the sole purpose of teaching, whereas none of the participants have a commercial interests in the use of data.

Electronic Communication – The method of transferring data between multiple information systems by means of electronic method to which information system has access and right of use.

Fair Use – The copying or distribution of any data under copyright in a manner that is for non-profit use, non-commercial use, transformative use (such as parodies and derived creations

inspired or based on original content), referential use (such as citation, commentary, or criticism), non-distributive educational use, or as a personal backup of data that has been legally obtained.

File – A self contained piece of data including but not limited to an image, segment of audio or video, text or other work, typically stored on a hard drive, disk or other storage medium or information system, which may be copied, distributed, uploaded, downloaded or otherwise transmitted or received over a network or physically via a physical storage medium.

File Sharing – The upload of data or the action of making data available for the purpose of allowing other parties to download and/or redistribute that data.

Identity -

Illegal Content – Content that is explicitly forbidden by applicable law.

Internet - A global system of interconnected networks and nodes that use the standard Internet protocol suite (e.g., TCP/IP) to transmit and share information or data.

Internet Service Provider (ISP) – Any organization or person that provides access to the Internet as a service.

Intellectual Property - A common reference to the three state-granted intellectual monopolies Copyright, Patent or Trademark. Such monopolies may be held by legal or natural persons.

Internet Protocol - The set of rules which Internet connected devices use to send data to each other.

Link – Any data on a website or that contains the location and a connection to other websites.

MAC ID / MAC Address - Acronym for Media Access Control ID/Address. A unique twelve character address assigned to a network interface or device. Though addresses are uniquely assigned (typically at time of manufacture), new or different addresses can be assigned through software. Valid addresses may contain both letters and numbers ranging from zero through nine and the letters A through F often written with colons or hyphens used as pair separators (See examples). Example addresses: 00:00:00:00:00:00 or FF-FF-FF-FF-FF-FF.

Media – Digital and non-digital methods of retaining various amounts of information or data. (eg. compact disks, flash drives, or even vinyl records)

Private Data – Either of the following:
1) Data that positively identifies a user or any of a user’s property,
2) Data that might cause harm to a user if it were to become public data,

Exception: Data that the user in 1) or 2) has explicitly agreed to make public data is not private data.

Public Data – Any data legally accessible to an user.

Transmission – The process of sending and/or receiving data via propagating a point-to-point or point-to-multi-point signal.

Upload – The act of sending, transferring or copying data from a local storage medium or device including but not limited to mobile phones or other handsets, personal computers or other personal information systems to an external or remote information system.

Uploader – A user that has completed or contributed to an upload to an online storage, site or service, or to another user.

User – An individual that is utilizing or interacts with a service, tool, program, or information system; eg. an uploader or a downloader.

Title II – The Freedom of Internet Act
Article I. Censorship
A) No Federal or State Governments shall pass any law, nor ratify any treaty, which imposes or administers any kind of censorship on the Internet, except in the situations detailed in Section C.

B) Censorship may only be enforced after illegal material has been found, and no steps can be taken to monitor data being uploaded. Censorship is to be limited to the illegal content and no steps shall be taken to censor legal content uploaded by the party.

C) Censorship is only allowed if content is found to be illegal content in accordance with this act.

1) All false information in an attempt to misguide, scam, cause damage, trap users financially, or mutilate collateral are considered illegal content .

Article II. Culpability
A) Only the creator or uploader of data is responsible for whether that data is legal to upload, possess or make available to other users or information services.
1) A creator or uploader of illegal data is subject to judicial proceedings as laid out in Article V.
2) Punishment may be acted on with the procedures from Article VI or punishment determined by his/her country of current residence.

B) If the content under considerations is a work that was partially or fully derived from another content under copyright, it is required that the derived should,
contain a minimum of 40% of the original content,
be wholly comprised of sections of the original,
not be a subtitled parody video,
to be illegal content.

1) If the data is similar in look, feel, presentation or idea but of different origin and is a original work other than for the similarity, it is not culpable. (Trademarks, registered names...etc are exempted from this.)
2) If the new products are released as a series of parts then combined content poster, fan art etc are not culpable. The content is to be considered to evaluate culpability.
3) An imitation, parody or data derived from real world presence of a copyrighted content as in but not limited to the name, photograph of a
[The above clause was added to prevent people from abusing copyright other than for fair use by inserting a small fraction of extra content or by dividing the content, this additionally protects users from copyright when creating derived content or in any other likely case.]

C) Any website includient is only subject to process in accordance with Article IV.

D) Internet Service Providers shall not be liable for damages caused by any illegal upload or download initiated by a user of their service.
1) ISPs shall not monitor the content of data being uploaded or downloaded by their users, except as allowed in Article V.
2) ISPs shall not filter, restrict or distort any data being uploaded or downloaded in any way that is based upon the content of that Data.
3) ISPs shall not be required to alter their service in any way due to the illegal actions of a user of their service.

E) No user shall be held liable for the upload of data unless it can be proven that the User has certain knowledge that the data was not legal to upload in the country or countries where the upload was initiated and/or completed.
1) A user is liable for the illegal upload of data if they upload illegal content, and is subject to the judicial proceedings found in Article IV.
2) A user shall bear no liability for the download of data that was made available by an illegal act of upload. It must be assumed that a user does not have certain knowledge that the data in question was uploaded illegally.
3) A user may bear liability for failure to report to an authority the download of any public data that would in no case be legal to upload as public data. Such data includes but may not be limited to child pornography or obvious private data.

F) No User shall be held liable for the upload of any copyrighted material that the user can reasonably assume falls under the definition of Fair Use of copyrighted data.
Article III. Restrictions on the Internet
A) No federal union, sovereign state or transnational or supranational entity or organisation may pass unilateral restrictions on the Internet.
B) Bandwidth-throttling shall not be used as a means of Penalty for any alleged illegal activity. (It was here before, it is judge to debate again)

Article IV. Content Removal
A) The removal of illegal data from any service or information system must follow the guidelines found in this article.

B) Notice must be given to an administrator of the information system and to the uploader of the content within at least 30 days in advance of any deletion of data from any information system or service, or within 24 hours of the transfer of the data in question from publicly accessible storage to privately accessible storage.
1) Verified electronic means of communication as in a email signed with a digital signature (or pin #?) can be used for issuing the notice.
2) Only the data in question may be so deleted or transferred. Related data including but not limited to data that describes the content or location of the Data in question, any of the uploader’s private data, or any data that is part of the function of an information system or service provider shall not be required to be removed.
3) Within the allowed 30 days, the uploader of the data in question may respond to the information system administrator with a request to stop or reverse the removal of the data in question. If the user verifies their identity and additionally offers a reasonable assertion of fair use or other reasonable defense to the claim that the data in question is illegal, the service provider may at their discretion forward such identity and claim to the complainant and reverse the removal without liability until a judicial authority has determined whether the claim is valid.

C) Information systems and administrators must provide notice to the uploader regarding any removal when and why data will be removed under this article, and who has ordered such a removal.

D) Orders to remove data based on willful false claims or by entities that do not represent or possess the rights to object to the Upload of the content in question will be considered acts of censoring, and defamation of the character of the uploader in the form of wrongful accusation of criminal activity.
1) Willful false claims of copyright infringement shall be treated and tried as equivalent to copyright infringement, and will only be diminishable on the sole condition of proof provided and accepted by a ruling court that supports the defendant's reason for claiming infringement. No law or act shall diminish the liability wrongful claims of infringement shall carry as set forth by this act.

Article V. Judicial Proceedings
A) Anyone undergoing judicial proceedings based on this document must be judged in the nation's courts wherein the alleged offense activities.
1) If an individual resided in more than one country when committing violation(s) of this document, they must be judged in the country in which they committed the offense.
2) The individual in question may demand extradition to his country of residence or citizenship, where he must then be tried for the listed offences. The court proceeding shall judge the offense as if the offence had been committed in his country of residence or citizenship during the event of the crime.
3) No person is to be extradited, deported or forced to leave, or forcibly taken from a country for the need of legal proceedings. Any legal proceeding must be conducted in the country of which the offense was committed.

B) Before judicial action can begin, substantial evidence of culpability must be provided.
1) Data that identifies locations or devices, including but not limited to Internet Protocol addresses or MAC IDs are not proof of the identity of a user and can not therefore be used to positively identify a user.
2) Collection of any personal information or private data of any individual other than that which can be used as evidence is prohibited. Any Data absorbed during the search for evidence must be returned to its owner within 15 business days. Any copies of data not used as evidence must be permanently deleted and removed from any kind of storage.
3) Any hardware withheld should be returned if the person is cleared of charge or if he completes his sentence as required by the legal proceedings. If damage occurs to evidence, the withholding officer incurs all expenses on seized property.
4) Accessing, copying, transmitting or storing any data that belong to the convicted person other than that can be used as evidence is prohibited and the offender is liable for it.

Article VI. Appropriate Punishments

A) In case of copyright infringement a settlement will be considered in monetary form as defined in Article IX.

1) The Uploader of infringed Data shall have no other financial liability other than the one defined in Article IX for settlement.

Article VII. Rights of the user

A) Every user has a right to appear as anonymous and/or under pseudonym.

1) No data collected by an Information System under claim that it is collected to help the user to use the service (for example mobile numbers to aid password recovery) may be demanded,

used or shared in a way that may lead to the user losing their anonymity.
2) Information systems have to explicitly specify the data that they may use and share to help in identifying the user, the IP address is excepted from this and is bound by condition in Article V [B.1].

B) Everything the user does with his/her computer is considered private. This privacy may only be breached while the set criteria of section C is fulfilled.

C) A user's privacy can only be breached while
1) User is suspected of illegal acts in the user's residing country.
2) Adequate evidence, as defined in Article V Section B has been obtained
3) The international authority as defined in Article VII should be informed, and authorization collected in advance if at all a breach if privacy is to be initiated.

D) The use of anonymizing networks (Proxies) is protected.
1) The service providers or users in general of these services are not required to provide any information that may lead to the identification of an anonymous user.
2) Monitoring of traffic in, out of inside of an anonymizing network is prohibited

E) No discrimination or suspicion may be based on the methods employed by a user to ensure their security and privacy on the Internet.

F) Encrypted data is considered private. No user may be forced to release the password to encrypted data even if their privacy has been breached.

Article VIII. Liability and Settlement of Copyright Infringement Claim
A) The liability of a copyright infringement will be strictly limited to the damage it caused as described here.
1) All calculations related to this are to be carried out in a consumer, retail, individual level pricing upon which the production cost, marketing cost will not influence.
2) The maximum liability of the user who has committed infringement can be 200% of the calculated damage.

B) The user may only be held liable for the data that he/she infringed. The user may not be held responsible for any data not directly handled/accessed by the user in question.

C) The damages and and its extent is to be calculated by considering the number of receivers of the shared file.
1) If the data was shared with a single individual the retail price of that data as marketed by the creator is to be considered as damage and maximum liability cap is applicable.

2) For number of receivers is between 2 and 75, the multiple of the marketed value of product for personal use will be considered as damage, maximum liability cap is applicable.
3) For numbers greater than 75 but less than 1000 the amount payable by a distributor for as many copies will apply as the damage. A maximum liability cap of 150% is applicable.
4) For anything greater than 1000 receivers a nominal charge for mass distribution may be collected with a liability cap of 150%.

D) All fair use and educational use activities will be considered as non-damage causing and liability free.

Article IX. (This may or not be the final article)
A) This act may not be interpreted as implying for any collection of people or any individual to perform an act with the intent to maim or destroy the rights and freedoms set forth herein.

B) Any intent to harm a physical location or resource through the co-option of the Internet may be recorded and openly distributed for public knowledge and resolution.

C) The right to access the Internet shall not be denied by any federal or state government.