xnet-x.net

Basic how-to guide for preserving fundamental rights on the Internet | Xnet

19-25 minutes

21 septiembre, 2017

Xnet publishes a Basic How-to guide for preserveing fundamental rights on the Internet

#Democracy – Rights and freedoms protected by the people: recent events in Catalonia as a case study

How-to guide: https://xnet-x.net/en/how-to-for-preserving-fundamental-rights-internet/

What is happening in Spain these days in relation with the situation in Catalonia is **a very significant milestone in the**

defence of freedoms and rights around the world in the digital age.

The reaction of the Spanish government has clearly shown that the entire population – not only those living in Catalonia – needs to have tools to guarantee their **fundamental rights (natural rights guaranteed per se which do not depend on any government**) independently of any unjustified or arbitrary tutelage [1] [2] [3].

Many international institutions like the United Nations [4], recommend this after the Snowden revelations, emphasizing that knowledge and use of digital tools by everyone to ensure their privacy, freedom of expression and access to information are essential and the only way to guarantee fundamental rights in the face of increasing state-approved mass surveillance.

The acceleration of events in Catalonia has finally made the whole Spanish population aware of this situation and many citizens are now ready to begin use these tools. But, these days, unlike situations such as those experienced in Turkey, for example, even the Catalan institutions are publicising the necessary tools. They have finally agreed to **assign, distribute and share responsibility for protection of freedoms** [5], thus beginning to endorse what we see as the embryo of what has to be **a democracy that is up to the requirements of the digital age**.

Xnet fights to empower people because we believe that a real democracy resides in thye fact of making it possible for each and every person to access the necessary tools to monitor their institutions and to be autonomous in their judgments and, consequently, in protecting their rights and freedoms.

We have worked tirelessly to teach people how to use these tools and to deactivate the gross attempts to criminalise them by powers that need people to be at their mercy.

From this point of view, what is happening these days is of historic significance and hopeful. This acceleration towards a greater degree of democracy and strength for civil society is taking place spontaneously, but lack of knowledge about some aspects of the digital milieu is exposing people to risks [6] [7].

Accordingly, and in order to facilitate this process of co-responsibility wherever necessary, Xnet has summarized the most important information in a basic How-to guide.

Our How-to guide is also been associated with the indispensable work in defence of rights and legal freedoms carried out by several organisations in the campaign #SomDefensores.

[1] Legal analysis by the Electronic Founder Foundation on the illegality of the attack by the Spanish Government on the top-level domain PuntCat and the Internet: “The content removed is essentially political speech, which the European Court of Human Rights has considered deserving of a higher level of protection than other forms of expression. Even though the speech concerns a referendum that has been ruled illegal, the speech does not in itself pose any imminent threat to life or limb. The […] seizure took place with only 10 days remaining until the scheduled referendum, making it unlikely that the legality of the domains’ seizures could be judicially reviewed before the referendum is scheduled to take place. The fact that such mechanisms of legal review would

not be timely accessible to the Catalan independence movement, and that the censorship of speech would therefore be de facto unreviewable[…]. Whether it's allegations of sedition or any other form of unlawful or controversial speech, domain name intermediaries should not be held responsible for the content of websites that utilize their domains.
https://www.eff.org/es/deeplinks/2017/09/cat-domain-casualty-catalonian-independence-crackdown
[2] Internet Society statement on Internet blocking measures in Catalonia, Spain "The court's ruling vis-à-vis .CAT has a disproportionate chilling effect on free expression, and an unjust impact on the ability of Catalan-speaking persons to create, share, and access content on the Internet."
https://www.internetsociety.org/news/statements/2017/internet-society-statement-internet-blocking-measures-catalonia-spain/
The Spanish government has been blocking websites containing information on the Catalan referendum to be held on 1 October.
https://twitter.com/OpenObservatory/status/912306031329529856
[3] Right to Privacy and Encryption : "European Parliament Science and Technology Options Assessment (STOA) on Mass Surveillance" and the "United Nations report on the promotion and protection of the right to freedom of opinion and expression"
https://xnet-x.net/en/right-to-privacy-and-encryption/
[4] The Catalan government is using cypherpunk techniques with voters data
https://medium.com/@josepot/is-sensitive-voter-data-being-

exposed-by-the-catalan-government-af9d8a909482

[5] On September 25, 13 young people testify before the National Police in relation to the “mirrors” of the referendum website https://twitter.com/mvilaredon/status/912231920540487680

[6] List of irregularities during the search and arrest of a young man of 21 years for “cloning the web http://referendum.cat” https://twitter.com/mvilaredon/status/911285093142016001

Basic how-to guide for preserving fundamental rights on the Internet

Xnet has prepared this technical guide with tips and tools addressed to activists, journalists and citizens whose fundamental freedoms and rights on the Internet are being restricted by state powers or authoritarian governments.

It is important to read the recommendations, download and learn to use these tools beforea possible arbitrary block of the Internet, or attempt to access private data of citizens, etc. because, once it starts, it will be too late.te.

[***This guide is to be improved collectively; if you have any corrections write to: info[at]xnet-x.net /****Clave pública PGP*]

Arbitrary website and application blocking

Arbitrary Internet blockages occur primarily – but not only – when a government intentionally disrupts access to websites, mobile applications or electronic communication services to censor or control what people say or do.

Internet access is essential for the exercise of our freedoms and should be considered in itself a fundamental right [#KeepItOn]. Partially or totally blocking Internet access is a common practice in countries with authoritarian regimes, for example, to avoid access to certain types of content (in opposition to the regime, LGTBI, etc.) and to exercise control over conversations and the flow of information.

How to access websites that are arbitrarily censored or blocked in a particular connection/location: Tor and VPN

Both the Tor network and a VPN allow access to websites and applications that have been improperly blocked in a region or country, surfing the Internet as if it was being done from another geographical location.

For example, if a country blocks access to Twitter, people can use the Tor network or a VPN to access the social network as if their connection was coming from another point or country where these arbitrary restrictions on freedom of expression and access to information are not happening. Moreover, navigation in both cases is encrypted – in a “closed envelope”, so that it can only be read by the sender and

receiver.

- Tor for #Android | #iPhone | #PC
- #VPN

Tor for Android: Orbot

How to use Orbot:

Tor for iPhone: Onion Browser

There is no iPhone application that allows use of the Tor network for any application installed on the device. However, with Onion Browser you can access websites and the web version of arbitrarily blocked applications.

Tor for PC: Tor Browser

Download Tor browser for Linux / MacOS / Windows.

How to install and use Tor in Linux / MacOS / Windows.

Video: How to use Tor in PCs created for the launching of the Whistleblowing Platform against corruption of the City Hall of Barcelona (CAT):

VPN

A VPN (Virtual Private Network) allows your data to travel through an encrypted connection, or a kind of tunnel,before heading out to the open Internet, and connect to the Web from another location.
The easiest and fastest application to install in order to activate a VPN connection is Bitmask, which is also free. At the moment it is only available for Android phones and Linux PCs although its version for the MacOs iPhone is about to be released and, in the not too distant future, its Windows version. However, there are many very low-cost payment services that offer VPN connection for all types of devices – see below for information on Internet services that ensure the preservation of privacy and information.
It is advisable to have both Tor and VPN options. Iftraffic is blocked through Tor, you can then use the VPN, and vice versa.

For a correct configuration of the VPN connection, it is important to ensure that you are not suffering ‘DNS leakage’. Otherwise you will not be able to overcome the blockade and will reveal your connection data. In the page DNS Leak test you can find out how to test it and how to solve it,.

Mobile Device Encryption

Encrypting devices, especially mobile phones, is essential to maintain the privacy of personal data should they be lost or stolen. This is why most smartphones have installed by default tools which, in a few simple steps, encrypt the entire device, and it always is recommended to protect the privacy of data, accounts, contacts and user information.

Mobile Device Encryption: Example with Android

In geneal, as a good practice, you should not store unnecessary information in your devices, delete periodically. Even though you may be sure that everything you have is absolutely legal, remember that it is not you, but the power who decides what is legal and what isn't, and what today is legal might not be so tomorrow in case that the regime becomes authoritarian. Deleting and emptying the bin is not enough, you have to use specific tools that overwrite the data several times. More information and tools to do it here.

Note to the Spanish State: In the case that security forces confiscate someone's device because this person is under investigation , he or she has the right not to reveal encryption keys, PIN, unlock pattern, password or similar data, in accordance with the right not to testify against oneself (Criminal Procedure Law Art. 118 h & Art. 588 septies b 2; as explained in this document to the Secretariat of State of the European Union).

Hosting: privacy and security

The censorship of websites by authoritarian governments can happen at a deeper level when, instead of blocking access to the web through the network, the page is entirely closed down either by intervening in the servers or by seizing the domain. In this case, tools like Tor or a VPN will not help.

In order to foil such attempts (or create a *mirror* – copy of the same website – in a secure hosting if the web has already been censored), citizens living in authoritarian states should not choose a server within the territory of their country. It is

necessary to search and choose countries where the legal framework offers strong guarantees regarding freedom of expression and information about where to locate the *hosting*.

Neither should they register the domain of a website susceptible to be censored with *Top Level Domains* of their own country. It is easier for a government to intervene in its TLD than in others such as *.net*, *.eu* or *.is*. In Spain, we have recently experienced a preposterous example of this, unprecedented in the European Union, with the TLD *.cat*:

Finally, to protect your privacy and security (to avoid spam, spam, or other harassment), you should acquire your domain in registration services that offer strong legal security, eg Njalla.

Many domain registrars undertake not to publish the owner's data and to manage the requests they receive themselves, whether they are requests from buyers, individuals, or authorities and institutions. This type of service is known as private *whois*.

The importance of this requirement can be understood by entering, for example, https://whois.icann.org/ or https://www.nic.es/sgnd/dominio/publicInformacionDominios.action (for domains ending in .es) and looking for any web.

A file will appear in which all data will be output. If the person who owns the website has not used a provider which had undertaken to protect their privacy, his or her information will be published,and anyone from anywhere can see it:

REGISTRANT CONTACT (note that providing inaccurate or outdated information is punishable)

Name: …
Organisation: …
Street: …
City: …
State: …
Postal Code: …
Phone: …
Email: …

If the owner has taken the functional and customary measure that the requests are to be managed by the provider (has activated the private *whois* service), the data will be forwarded to the service provider. The provider will notify the owner if someone has searched or required it. It is important that the provider should assure you in the contract of the deadlines within which it provides you with the information. The more ethical providers which are respectful of the rights of their users usually offer deadlines between the requirement and the communication of your data to those who require it if you have not answered.

Not all domains agree because not all domains are managed in the same way. Generic domains, .com, .net, .biz, .org, etc… are managed by ICANN – the Internet Corporation for Assigned Names and Numbers, the leading Internet governance body, and this organization is the one which permits the use of domains that can have recourse to to Whois protection. The .es domains, on the other hand, are managed by Red.es and, these domains, do not allow hiding the data of the registry of users who want to acquire of a .es domain.

Messaging, VOIP, email and file sharing privately and securely

Massive surveillance of what we do and say on the Internet (and in all electronic communications) by governments has been clearly revealed thanks to Snowden's revelations. Below are some tips to help defend privacy against these practices using encryption tools.

Messaging

To protect the privacy of your communications always use messaging applications that have end-to-end encryption by default. We strongly recommend using Signal (Android | iPhone), an end-to-end encrypted messaging app whose use is easy and intuitive, and recommended by Snowden himself. Among other popular messaging applications, Whatsapp has also integrated end-to-end encryption in all communications by default (however, Facebook has already shared user data with WhatsApp and the social network, so Signal is still the best choice). Telegram, has encryption option but is not active by default.

It is important to note that, even though they are encrypted end-to-end, the above applications are associated with the user's mobile number. Hence, even if the communication is encrypted (a third person cannot see the content) it is not

anonymous and the identity of the sender and receiver, as well as connection and geolocation times are known.

Video calls – VOIP

You can make encrypted calls and video calls over the Internet with Signal (and Whatsapp) to a contact. MeetJitsi allows you to make group video calls. Calls and video calls through Skype, Hangouts or others do not sufficiently protect the privacy of your communications.

Encrypted email

In the case of e-mail, it is important to know that all e-mail sent and received can be read (and is actually processed) by the mail service providers. Some of them, when required by the authorities, show little concern about the privacy and legal security of their customers/users. We do not recommend the use of services like gmail, yahoo, hotmail, etc. In any case, it should be known that sending any email without encryption is almost the same as sending a letter in an open envelope. In order to protect the right to confidentiality of communication, it is possible to use encryption with **PGP**. This allows you to ensure the privacy of communications and files sent via email. This guide from Security in a Box explains how to use email with PGP with Linux I MacOS I Windows.

Again in this case, the communication is encrypted in terms of content, but not anonymous.
What does this mean? It means that, even if we do not indicate our name, or we use an email account in which our identity does not appear, or a throw-away one, all electronic communication leaves a trail , the so-called IP address, which

is a unique address assigned to each device on the network and indicating the point from which a communication has been made. In addition, the sender, recipient, and subject of the message as well as other “metadata” of the mail are not encrypted and indicate who receives it, when, and other data. Therefore, the only real anonymity possible for transferring files and information can be achieved through the Tor network, because this communication is not made from point A to point B but the connection passes through several intermediate nodes within the Tor network, none of which knows the origin and destination at the same time. Obviously, accessing our regular account of gmail or any social network through the Tor network will reveal the identity even if the IP address is hidden.

One example of how to deliver information privately and securely is the XnetLeaks mailbox for reporting corruption, based on Globaleaks and accessible through Tor.

Blocking of messaging applications

Alternatives to private and public communication in case Signal or Whatsapp messaging applications and social networks are blocked.

FireChat: for Android and iPhone

FireChat is a messaging application that allows communication between devices and publishing in public forums between nearby devices through *mesh-networks*.

- Public rooms: like *#PublicRoom1*, are open chats in which all messages reach all participants in the chat. **All messages**

are public and not encrypted. The creators of FireChat recommend that people should not use personal data and that they should be careful with personal information that is shared in the public chats.

- Private Messages: Private messages are encrypted and can only be viewed by the sender and the recipients, which can be one or several.

  This is the application used by demonstrators in the yellow umbrella revolution in Hong Kong when their communications were blocked. Julian Assange recommends it (along with Briar) for this type of situations.

  Download FireChat for Android or iPhone: https://www.opengarden.com/firechat.html

  How to use FireChat: https://www.opengarden.com/how-to.html

Internet shutdown

In the extreme case of a shutdown in which the Internet connection is completely cut off, as happens in situations of great repression, there are applications that allow communication between mobile devices, even without

connection.

Briar: for Android and iPhone

Briar is an open source messaging application designed for activists, journalists and anyone else who needs a secure, easy and robust way to communicate. Unlike traditional messaging tools such as email, Twitter or Telegram, Briar is not based on a central server: messages are synchronized directly via p2p between users' devices.

If the Internet is down, Briar can synchronize messages via Bluetooth or Wi-Fi, and thus maintain the flow of information in case of crisis. The devices must be able to connect between them so the maximum distance in the case of Bluetooth is 70 meters approx. or a little more in the case of Wi-Fi depending on its scope. In the case of groups or forums, the larger the group the greater the reach of p2p synchronization.

With Internet connection, Briar is synchronized through the Tor network, protecting users from surveillance.

Download Briar: https://briarproject.org/download.html

Howt to use Briar: https://briarproject.org/manual/

More

This guide contains a series of basic guidelines for preserving your rights on the Internet. For greater security and privacy on the Internet, visit Security in a Box.

Finally in terms of basic logistics, it is recommended that you should always leave home with your devices charged and, if possible, with external batteries for greater autonomy.

Front page from Accessnow's campaign KeepItOn.