

USER-VERIFIABLE TELEMATICS

What is it?

A **research project** for the realization of software, hardware and processes that enable ordinary non-technical citizens to affordable access to any internet-based telematic communication with levels of privacy and security that are very very high and fully **user-verifiable**.

How?

It is based on state-of-the-art operating systems, internet communication software and encryption protocols, free/open source software licensing, and open expert review processes.

But the core innovation are processes and tools through which the user-verifiability of the integrity of a server room against tampering through legal or illegal access to the server room, is guaranteed in ways similar to the management of ballot boxes during good-old paper based elections, based on the constant presence of at least **5 individuals that are randomly-selected and/or with conflicting interests**.

If a court order is issued for the acquisition of certain logs or information on a user of the service, the authority would be given physical access to such specific piece of information, at the presence of 5 randomly selected users. This way it enables the efficient prosecution of investigations on suspected crimes by users of the system on the basis of evidence acquired externally.

True, there is a possibility that even the strongest and longest standing protocols may have been broken by some powerful third party through undisclosed computers and algorithms, but it is a "very" remote possibility for a host of reason. Therefore, once the technology is realized and properly tested by experts and crackers, we advise it's use for private social and political communication.

Thesis!

It is **not enough** for citizens to be told we have certain rights as users of a given telematic service, under a license (such as FLOSS), a state legislation (such as national and global privacy protection regulations) or a contract with the service provider (such as Terms of Use).

What is the use of privacy laws and rights if a single easy-to-deploy criminal activity can involve their continuous breach through the monitoring and analyzing of the telematic communications of millions, and the detection of such crime was very very difficult and unlikely (or pardoned by presidential decree)?

We believe that to be the case today.

We believe that such huge loss of privacy **is not an unavoidable price to pay for the comforts of information technology innovations**. It is based on the type of software running in current mainstream electronic communication devices and services.

And such software can be substituted, modified directly by users and providers, and indirectly by government through legislations.

Two solutions are therefore available:

1. Convince legislative body to enact far reaching rules, and detection and enforcement processes, that effectively enable all citizens to affordable access to most telematics devices and services with levels of security that are very very high and fully user-verifiable.
2. A group of citizens, organizations or even a municipality could develop and deploy “user-verifiable telematics” for its members.

Why?

In democratic political systems based on the secrecy of vote, substantial levels of privacy, integrity and authentication have been and are indispensable requirements to sustain the **internal communications of formal and informal democratic citizens’ organizations, as well as “social networks”**. A substantial level privacy and reliability of communications among 2 or more citizens has been and is indispensable to ensure the effectiveness of democratic process through the maintenance of a sufficiently free “market of ideas”.

Today, most human communications in the developed world today happen through 2-way telematic services involving software on both ends.

Current laws allow and encourage producers to market and distribute computers, electronic devices and telematic services that allow the potential illegal abuse of privacy of their users in a mass scale by several ICT companies, governmental agencies or other criminal groups, or just as well by sub-groups or individuals within such entities. But such risks have been around since the times of postage and telephone.

What has changed radically during the last few years is the **hugely decreased cost per person per minute of such communications privacy abuses**, together with the **greatly reduced ability of police and judiciary to ascertain such mass privacy legal breaches**.

For the first time in history, hugely lowered costs and risks make it economically feasible for a large number and type of entities to continuously monitor and analyze illegally millions of people, with extremely low risk of getting caught per each abuse.

On the contrary, since **very very secure operating systems and encrypted communication software and protocols are widely available through the world, criminal individuals and groups** (including entities illegally mass abusing citizens privacy!), can communicate via email and VoIP with a very very low possibility of even (legal) military or NSA agencies to decrypt or even detect such communications about

illegal activities.

We and a number of telematic security experts believe that software-based telematic solutions can be realized with limited resources that would allow non-technical ordinary citizens to cheaply have access to internet-based telematics communications with levels of privacy and security that are very very high and fully user-verifiable.