# *A Web in Respect of the Constitution is Possible*

**CARLO VON LYNX**
**{ secushare.org }**

**BERLIN**, 2014-10-29

**Introduction**

The Internet is broken, and it poses the greatest threats to our expectations of democracy since World War II. [1] Our constitutions expect our governments to secure our *Secrecy of Correspondence,* but the ease of use of mobile texting and electronic mail have in only two decades led the population of entire nations on the slippery slope of giving up such secrecy for mere convenience. In fact both texting and e-mail are now slowly giving way to web-based messaging systems such as Facebook, Twitter, Whatsapp or Snapchat.

As the authors of our constitutions did not foresee such developments, one could expect that they would have also considered the total knowledge of people's web surfing activities a threat to democracy. Whoever knows what a person will think and do before she even started clicking, can manipulate a whole population into thinking and doing differently. And in this day and age, it is all a question of automation. So whenever the instruments are suitable for delivering a precise heartbeat measurement of an entire nation's eligible voters, the actual intention of the Constitution has been infringed – and a lawyer would tell you that ultimately the *intention* is what counts, beyond the actual wording of your respective constitutions. It is severely overdue for Supreme Courts of the world to express themselves on these dramatic political shifts caused by technology.

While governments should focus on restoring the premises for a healthy democratic well-being, they have instead been lured by the illusion of *omniscience*

as a guarantor for security. Omniscience may enable one government to catch little fish as they plan committing little crimes, but it empowers big fish to take over a future government and dismantle democracy in the process.

Akin to Tor's hidden services [7], technologies such as Tribler [8], Edgenet [9], I2P [10], net2o [11], cjdns [12] and GNUnet [13], are indicating the way to a different architecture for a surveillance-resistant Internet as a realistic alternative to the currently established design, which can be barely improved, and never to a point to actually respect constitutional requirements. Together with Christian Grothoff and Bart Polot I have described in our position paper to the STRINT workshop [2] how such an architecture would look like, based on the paradigm shift of cryptographic routing. In this paper I will elaborate what this means for the Web and social interaction as it currently takes place on the Web. Governments of the world should focus on the research of these options.

## Server-centric Systems Violate the Constitution

The way the Web is architected, with most of the applicative intelligence residing on the server, indicating the browser what to do and how to interact with the user, has been a winning aspect for the Internet's general popularity – yet it has created enormous collecting points of data about humanity, and, faced with the impossibility to truly secure any server- or cloud-based infrastructure, [3] engineers like us have created the threat to democracy we face today.

This has been the easier and cheaper way to do things, but we must change our habits. We must introduce laws that require the entire industry to migrate to a safe architecture that shall respect civil rights and the ability of a population to develop an independent democratic will, such as this law proposal suggests: *“Obligatory anonymised and end-to-end encrypted communications in all telephony and computer appliances sold after 201x”* [4]

## My Device is My Home

Privacy means to allow no-one but the intended recipients to view shared information, be it wedding pictures, a silly comment about the weather or an insightful criticism of current political developments. In the Web of the future, this information shall only exist on the owner's own device as on the devices of the people she shared it with. It must not be accessible by any intermediate router or server. Even the fact that this interchange happened must not be measurable. Luckily, this can be achieved.

A “GNU Internet” infrastructure creates a scalable, obfuscated, secure link between just those devices. [2] From that point on web technologies can play their part as they already do according to the “app” paradigm: orchestrations of HTML, CSS and Javascript running locally on today's mobile devices.

## A Fully Distributed Social Network

Social interactions isn't the only thing that needs to be addressed, but it apparently is the number one issue of concern. With our *secushare.org* project we have been designing a fully distributed social network that employs the publish/subscribe paradigm with *multicast* distribution trees over the GNUnet platform to model all social networking interactions that users commonly expect from Facebook and similar technologies. [5] Instead of navigating to a web server, people have the entire social networking experience happening right there on their own device, even when they are out of range for Internet connectivity. This approach has been praised for holding the best potential of actually bringing privacy to social networking. [6]

## The Distributed Web

Most of the static web does not have to be served up

from a server, creating an artificial requirement of realtimeness, which is the root of most privacy problems (as Tor developers occasionally confirm). Accessing a website, the manual of a software for example, could instead by the subscription of a multicast (BitTorrent can be considered a variant of multicast, so this is already happening) which will bring a copy of that manual onto the devices of the interested readers, regardless of when, how much or how little they will actually spend time reading it. And most of all, the less the person is in a hurry to have it, the better the GNU Internet can hide her interest in that software and thus contribute to the defense of democracy. The incentives to actually reorganize the knowledge of humanity in a way that it will not undermine privacy and democracy might again need to be created by legislation as the market has no notion of such priorities. [14]

### Users Must Become Owners of Their Devices

This also introduces a requirement for future devices to actually be under control of their owners. No back doors in the software, hardware or microcode. A transparent Internet stack that can be reproduced from source, ensuring that apps can no longer infringe civil rights en passant as they upload the high score to the game server. This too can in fact be enforced by suitable laws as the above-mentioned proposal is in process of elaborating.

### Conclusions

It's late, but not too late to fix the Internet and its World Wide Web. The problem is bigger than most of the world's population realizes and the real solutions, not just the patchworks, are closer and more feasible than most experts expect. The biggest challenge seems to be to shift everybody's thinking and fight back on the helplessness that has kept politicians and population in a state of shock while there seems to be at least one good way to address this challenge.

**Acknowledgments**

The ongoing work in *secushare.org* and *youbroketheinternet.org* is being supported by NLnet and the Wau Holland Foundation respectively. If you like what we do, please contact us.

**References**

[1] J. Assange, J. Appelbaum, A. Müller-Maguhn, J. Zimmermann; 2012; "Cypherpunks: Freedom and the Future of the Internet"; https://en.wikipedia.org/wiki/Cypherpunks_(book)

[2] C. Grothoff, B. Polot, C. v. Loesch; 2014; "The Internet is Broken: Idealistic Ideas for Building a GNU Network"; submitted to "W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)"; https://gnunet.org/strint2014gnunet

[3] C. v. Loesch, G. X. Toth, M. Baumann; 2011; "Scalability & Paranoia in a Decentralized Social Network."; submitted to "Federated Social Web 2011"; http://secushare.org/2011-FSW-Scalability-Paranoia

[4] c. von lynX & contributors; ongoing since 2013; "Obligatory anonymised and end-to-end encrypted communications in all telephony and computer appliances sold after 201x."; Proposal for EU legislation; http://youbroketheinternet.org/legislation/ObCrypto-law-proposal.pdf

[5] G. X. Toth; "Design of a social messaging system using stateful multicast"; 2013; Master's, University of Amsterdam, Amsterdam; https://gnunet.org/design-social-messaging-system

[6] Alexander Altmann; "Vergleich und Bewertung Sozialer Netzwerke im Hinblick auf Architektur, Sicherheit, Datenschutz und Anbieterunabhängigkeit,"; Diplomarbeit Universität Potsdam; http://www.edition1.net/rs7/da/soziale_netze.pdf

[7] https://www.torproject.org/docs/hidden-services
[8] https://github.com/Tribler/tribler/wiki#grand-vision
[9] http://cultureandempire.com/html/edgenet.html
[10] https://geti2p.net
[11] http://net2o.de
[12] https://wiki.projectmeshnet.org/Cjdns
[13] https://gnunet.org

[14] Karl Polanyi; 1944; "The Great Transformation"