Education and Transparency should have Priority against Control and Expected Safety

This position statement from a person who has been witness of the emergence of the internet aims at establishing values for states' politics so that the internet remains a universal access to knowledge as it has emerged to be and does not come back to a nationalist and military oriented project.

The Internet has Evolved

Following the steps of a small technical experiment, fed by multiple communities boards, the internet has seen numerous technical evolutions, open standards establishment, and scale-up operations. It is now recognized as offering the major source of knowledge, of any kind and risks becoming the major source of false knowledge.

Open standards and the open-minded collaboration about them has been the guiding principle. Multiple attempts have been made, including the happy hippie perspective of using blank password, the competition-less supposed free-beer of online services, the apparent fully free discourse, or the open-ness to receive contact requests from anyone.

These have been, however, going to their limits: open systems such as the e-mail exchanges or social networks systems have been abused by armadas of spammers and phishing hackers. The electronic exchanges has offered unprecedented possibilities for citizens to exchange and organize: while masses of cute animals' photographs or short dances invade the networks, political debates can happen, but criminal organizations and degrading personal exchanges can happen too.

The big mash of the internet exchanges sounds to have degenerated in a dangerous jungle where you, your grand-mother or your grand-child, meet the next attacker or the next wrong idea after just a few clicks. This is not very different than a big city where one can meet anyone and start awkwards projects. But the distance enabled communication has made it much more intensive.

Tempting Protection Solutions

Because of these risks, we have seen multiple attempts of protection. I list some of these below and explain, then, why many are likely ineffective.

In many cases, when one recognizes a risk, one is tempted to introduce the expectation that it disappears by a state regulation or by a technical measure.

As the simplest example is the family of anti-virus softwares: They are generally well known to follow simple pattern matching rules and fail in the most refined attempts. While this family of software was prescribed and widespread, expectations of the population about it has drowned.

As the simplest and more dangerous type of measures is the regular mailing information in corporations to warn that some phishing mails is around in the recent days: Such mails often lead to lack of circumspection at other days and, thus, to effective phishing.

As a potential solution to the risk of encountering inappropriate content on the web, politics have been steadily enacting or proposing to:

- analyse content: requiring security instances to be able to watch any conversation.
 This brings the security instances in privileges which is known to have been successful in somes cases and abused in somes cases. It has lead multiple states to counter harshly state-critical voices. Large industries are being involved to contribute to this effort where one, falsely, expects automated content analysis based on AI to identify in an unbiassed fashion inappropriate content.
- prohibit content: requiring some websites to be inaccessible by a ban. In the EU, for example, rt.com has been banned (by simply removing the DNS entry); other countries such as China or Russia have been known to enforce this to a much larger extent. The result is that only state-agreeing voices are being heard and that a person wanting to evaluate how others transmit or perceive cannot do so: a state-lead filter bubble emerges.

Finally, another family of risks has been cared for since decades: the corporate risks. In order to protect corporations from being held liable, from suffering from this or that risk, the legal apparatus has been applied in the form of contracts. While laws and contracts are the basis of a modern society where democracy can evolve, their complexity has been known to be daunting. The worst risk compensation for corporate risks is expressed in the form of end-user-agreements: With the internet becoming the center of economy for everyone, almost all websites of the earth deliver a service following terms-of-services of their own. One could expect these to be simple but the will to protect against everything, the fact that anyone on earth can use the web, terms of services for the use of software organisations such as web-sites have grown in a gigantic fashion. This has lead to the routine "yes ok" to agree on some conditions that no-one reads. While this ok may be protecting the corporations, it puts the end-use at risk and it is precisely this risk which, to a barely perceivable degree, is used to finance "fee services" such as social networks: by including subtle allowances such as reselling the data in some form.

Sustainable Solutions as Value-Statements for States

These varying, and almost poetic, terms of use of most websites are in strong contrast to simple indications such as "this repository is under this well known license" (e.g. GitHub for software projects) or "you may share this OER under this methods" (the creative commons deed). The simple and understandable world depicted by these classifications allow developers or teachers to become active partipants with little fear for their actions.

The understandability is key to this process. In these two communities, the advantages of such participation has been understood as essential and very few makers contribute with non-mainstream conditions.

How can we transport this agency ability to the broader world of using the internet? Can the self-regulation appear with only a limited set of understandable regulations?

This can only work by both making understandable the legal possibilities and the possible actions of the people. In turn, this can only happen if the people develop their ability to understand.

A basic understanding to be able to become an active citizen of the web includes the functions of the web: how publications happen, how trust is established and challenged, how others can have different feelings in their participation, and how data can be transformed and put to value.

With such a background, which is not as big as that of a bachelor of computer science, citizens of any country are able to eliminate the vast majority of phishing, ridiculize the vast majority of spams, and take distance to any bothering statement. They can become critical actors if they are able to follow a sufficiently diverse information diet.

While it is desirable for any environment to become void of toxic content. The expectation to reach such a purity should never be satisfied: Any community manager, any country regulator, any school director needs to accept that the next day can see the expression of harmful content. As long as the critical abilities exist, the reflection on the harms and the recovery possibilities will exist.

I thus suggest that:

states, corporations and communities spend more efforts in developing the critical abilities of their members or users than in creating barriers to be applied by controlling forces, be them in the force of police teams, of AI powered data centers, of community managers.

For this to be enacted, states should spend more resources into raising the comptency of every citizen for the digital world than spending in surveillance infrastructure and teams or in prohibitions. This is largely not achieved.

Enforcement of the regulations should, moreover, stop thinking an "all or nothing" model, where disappearance is the only acceptable fate of an inappropriate statement. Bans done in the many countries are example such disappearances; take-downs at social network sites are the same. Instead, gradual warning models should be introduced which leave a possibility of action for and a way to reflect about this statement. Only by diminishing the bans to almost zero, is there a hope that citizens trust their legal frameworks: They can agree to what the laws/guards have flagged.

For this to be enacted by companies, the corpus of terms of services should be summarised using simple words and graphics. And these summarisations should become understandable by everyone because of their common practice. As an example that is very badly achieved thus far: Browsing history of most social networks is recorded and is sold to third-parties or used to provide advertisement. I would assume that the path to standardize the summarisations so that they will be understood will be long and will be in cooperation with educator teams. The budget of such an understandability entreprise should be raised at least to as much as the budget of a legal department. The goal should be a feeling of transparency for every user.

Paul Libbrecht is a developer, professor of computer science and data science, and researcher. The opinions expressed here are personal but have been repeatedly discussed with my surroundings.