# The Case for Regulating Social Networks and the Internet

We don't need to miss out on the joys of technology in order to regain what liberty and democracy is supposed to mean, but the regulatory transformation we need to design and implement is of epic dimension.

Technology is not only a threat to our intimacy and liberty, it is making entire populations unable to vote according to their own interests. What do we need to do to fix this? Do we get to have all the apps on our smartphones that we love without trading in our civil rights and duties? Can we have the cake and eat it? At **#youbroketheinternet** we say, yes, indeed.

Why Do We Need a Next Generation Internet?

With the absence of alternatives in the public discourse, a fallacious idea of the inevitability of omniscient big data is being ingrained in the minds of leaders and policy-makers, similar to the folly that globalization is inevitable, when we could easily create transnational agreements on shipment taxation standards.

This is very dangerous as economists are looking at the current data monetization method as a rule of god, believing the fallacious comparison with oil: oil isn't sustainable, but at least it benefits just about everyone. Social big data instead puts a disproportionate amount of power into very few hands, enabling them to undermine the ability of the population to elect actual representatives or the ability of consumers to buy what they actually want, which supposedly is a precondition of a free market. Societally welcome uses of data such as the prediction of disease spread, the optimization of business processes and even law enforcement could as well be achieved without any such power concentration.

Democracy was not built for this abuse of technology, so we need to change it if we want to retain a somewhat free society. To some of you the word “democracy” itself has become tainted. Don't let the many regimes of the world that use that word lightheartedly distract you: The philosophical and legal achievement of Enlightenment, the creation of democratic constitutions, should not be underestimated just because nobody is obliged to use those words according to their actual meaning. They are still the only thing that hold free societies together.

Let's acknowledge democracy as the least worst form of governance we know and preserve it from an incumbent dark age of post-democratic technocracy. Let's systematically look at what we need technology to do to not be a threat to democracy. The number one problem is how citizens interact with each other over the internet, how they discuss anything from politics to private life in plain unencrypted visibility of the big data magnates.

The aggregation of such data enables us to not only predict the outcomes of elections, but to observe the performance of certain measures of manipulation, be it by electoral advertisements, search engine results or the opinions that appear in our social dashboards in real-time. You may trust the companies and the government not to manipulate this data, but a democracy must not operate on trust: democratic constitutions are meant to free you from having to trust anyone, because checks and balances should keep powers separate and under each other's control. We all know that doesn't always work out, but we would be living a much harsher life if it wasn't working most of the time.

The problem of someone having the power to see all our conversations can be solved with a simple legislational intervention. Let's stop looking at the state as something that keeps messing with our lives for a moment, and rather, imagine ourselves with the capacity to collectively decide how things should work and what kind of rules we need everyone to respect in order to all benefit, rather than letting a handful of lucky chaps run the show of our lives. You know that in the age of liquid democracy, we could actually implement a parliament of the people, combining the good sides of anarchism and democracy, but let that be a subject for another article.

Mandatory End-to-End Encryption

What about mandatory end-to-end encryption for all social interactions on the internet, not only between a few people as is customary today, but among entire social groups. Every time you post a comment about the weather to your social network, it should only be visible to the people you added to that network. By hiding your daily chit-chat you are protecting all the moments when you inadvertently expose those aspects of your personality which make you susceptible to certain demagogy. Your likes and status updates expose your mental vulnerabilities. Being able to predict which psychological biases you likely suffer from enables manipulators to confront you with appropriately tailored false information, just below your ability to question whether you are being presented propaganda. If a tiny company in Cambridge could do that, how many others can make you vote the opposite of what is in your own interest?

End-to-end encryption has gone mainstream with its adoption in Signal and Whatsapp. Unfortunately, since there is no way to tell whether the app on our phone is actually derived from any published source codes, we have no factual guarantees that our conversations are indeed private. In order to be able to trust our devices and apps not to steal our conversations, we need transparent and verifiable hardware, operating, and communication systems. Proprietary systems are an unacceptable threat to our liberties. We can, however, allow for proprietary apps to run in sandboxes as is already customary on smartphones, if we create a better permission system to define how apps may submit certain types of data to certain types of network entities  not giving them a blank cheque to access all of the internet.

It is still considered a complicated challenge to enable end-to-end encryption in social groups and chatrooms, but that is actually correlated to the way our current internet requires privacy to be bolted on top rather than planned for by design, and to the way commercial entities have no interest in providing any such encryption if it instantly makes them less competitive on the data market. Only when this business model becomes illegal for all business equally, will it make sense for them to oblige to the new rules.

With such legislation in place we can imagine that social networks could continue to be run in cloud computing systems by commercial entities. The law would mandate that decryption happens in a safe way on the devices of the citizen, allowing commerce to only place generic advertisement, not targeting the citizen based on the content of their communications. The efficiently scalable mechanisms of cloud computing would persist and the elimination of targeted advertising would be equal for all advertisers; thus, there would be no economic disadvantage.

However, some companies may need to explicitly charge for their services if non-targeted advertising isn't sufficient to pay the bills. With the abolition of surveillance capitalism the day must come for micropayment systems. Back in the 90's there was an attempt to deploy DigiCash into the web. Its advantages were compelling: it offered micropayment that allowed consumers to remain anonymous while the merchant's earnings were transparent, thus guaranteeing that appropriate taxation would take place. It was also a million times more energy efficient than Bitcoin. Unfortunately DigiCash Inc. did not release public source codes and tried to monetize on the implementation itself, which boosted the popularity of web advertising.

Twenty years later competent cryptographers have published a free software implementation of DigiCash called GNU Taler. But even now it isn't in a good position to replace the surveillance economy which is, if you put the ethical externalities aside, more efficient. Citizens may at first dislike paying for services, but that would simply replace the price they have been paying in civil liberties up to that point.

In an unregulated market, ethical priorities can't win. There is no way that democracy can be protected by the citizen's free and spontaneous will to care about it. Democracy defends itself by constitutional law, which needs to be updated to the technological reality of today. Mandatory encryption could be step one.

Deny Collection of Tracking Data

We should consider it implicit in step one, that citizens can only interact with companies over end-to-end encrypted channels. But even the data that companies collect and share among each other easily grows to the point of making political views of citizens (and other ethically questionable data like medical conditions) transparent to the advertising big data giants.

So, in order to protect democracy, we must also forbid any kind of tracking and collection of the "surfing" activity of citizen. There may be several ways to address this technically, but they all may leave some loopholes. A rather complete approach could be to disallow any website from including content from any third party website.

The entire surveillance economy is built on third-party inclusions, from the way advertising space is delegated to the advertising networks directly in your browser and auctioned off to an advertiser that interacts directly with you  on the basis of your existing customer profile which is itself generated from more subtle mechanisms such as the presence of Like buttons or inclusion of Google fonts, analytics or Javascript frameworks. It is utter folly that many open source web applications come shipped with hooks for Google to monetize on in the default HTML templates.

Disabling third party inclusions is a simple requirement to implement in web browsers. Some browser extensions allow you to try that out. You will see how most of the existing web stops working or at least doesn't look as intended. Again, if it is a legal requirement, then the web must adapt to function without third parties, which is in fact easy to implement in most cases. Just give everyone a deadline by which time all the web sites should better make sure they have no such dependencies and host all files themselves.

Must All Metadata Be Protected?

Metadata is the information on who is interacting with whom, how frequently, at which times and places. It's data which is generally visible to internet and social media service providers, even if all content was encrypted.

It is known that mere metadata is sufficient to produce impressive knowledge about each individual. Research has shown that the sexual orientation of citizens can be determined by the friends they have,([1](#fn1)) and that the shape of each person's social graph is so unique that it can be recognized across different social networking platforms,  even if all the participants were using pseudonymous account names.([2](#fn2))

It is elementary, Watson, that metadata can also give all the necessary information to predict citizen's political positioning and expose them to undemocratic manipulation. So the third requirement we would have to make for a "constitutional" next generation internet is to protect the metadata of the large majority of citizens.

This is easy to ask for, but technically complicated to implement. Since there is no commercial gain in this ability, even popular distributed technologies such as blockchains are not providing any metadata protection. It would take a redesign of cloud computing to integrate with distributed anonymity systems. Research in this area has been going on for several years, although there is no product ready to be deployed.([3](#fn3))

A policy for mandatory metadata protection with a reasonable deadline for implementation would ensure that the entire computing industry focus on adopting and perfecting solutions to this problem. If such a policy were in place, many existing internet protocols can no longer be considered fit for purpose. Luckily, suitable technologies to replace them are being or have been developed. Examples are GNUnet to replace TLS, CADET instead of BGP, GNS instead of DNS and X.509, pubsub multicasts instead of the static web, distributed search instead of Google and secushare as a replacement to Facebook.

Is Anonymity a Threat to Society?

Communications can be anonymous in the sense that third parties are not entitled to recognize who is talking to whom, yet they should be authenticated to all of the participants of any conversation, thus cutting out some so-called "cybercrime" such as spam mail, which possibly contains malware or viruses.

This kind of "anonymity" is mostly useful to people that already know each other. It wouldn't foster the creation of dark markets where people with illegal interests find each other.

What Does It Mean to Have a Secure Internet?

Since we, as a society, never experienced such a thing, let's consider the many effects this would bring.

A strategic advantage for any nation that introduces this before others: Others can no longer spy on such nation while that nation can still see everything others are sending over good ole TCP/IP.

A huge leap in the security of information technology in general, if we introduce that no computer can talk to any other computer without knowing the recipient's encryption key (which in next generation internet stacks usually is also the routing address). No more scanning of networks on the hunt for vulnerable Windows systems, no SQL injections found in traffic lights or wind energy turbines, no easy ways into hospital facilities. The list could go on to fill the entire XRDS magazine.

Out of the requirement of providing all the functionality people expect from tools such as Facebook and Whatsapp, but in a way that is conformant to democratic principles, a distributed social network operating from within our computers and smartphones would, as a side effect, enable us to leverage the collective intelligence of our social neighborhood. For example, we could have search engines that leverage what our friends know without intervention by any company. They can provide us with a consensus on where to buy cat food, offer couch-sharing, run a digital neighborhood flea market or taxi services among people with friends in common. Who needs middle men for that?

Isn't this simply the kind of internet we always expected the internet to become? An internet that would treat censorship as damage and automatically route around it? Well, that popular myth could now become reality, if we want it enough.

Telephony Without Location Tracking

The problem of metadata is also raised by our current mobile telephony system which generates big data on who is meeting whom in which parts of town. This information alone can be, when aggregated and analyzed using artificial intelligence, enough to give one party an advantage in an election campaign over another. Therefore we should have telephones that allow payment for services through anonymous micropayment.

If you're familiar with Tor, these telephones could check into a backbone that operates similarly to Tor, but at microsecond speeds, so that there is no easy way to keep track of them each time they switch from one network access point to another. With all telephones operating like this, an outside observer would only see a lot of people moving around the streets, but easily lose track of who is who. Unless, of course, that special law enforcement protocol has been activated.

A Proposal

Since Snowden's revelations we have been working on a proposal to legislate exactly these things. You can find it on our homepage.([4](#fn4)) It doesn't say how such a Next Generation Internet would work. It only makes the list of requirements, allowing the market to come up with solutions.

Author Bio

After having developed the PSYC chat system in the late 90's, carlo von lynX realized the server-based federation model was not going to satisfy neither the privacy nor the scalability requirements of humanity, so he initiated the secushare.org project which set out to implement an ideal distributed social network, capable of scaling with the size of participation right out of the devices the people are using, while providing maximum privacy and defense against manipulation. What sounded like a funny side project from a bunch of paranoids, turned out to be barely paranoid enough: the only reasonable alternative to rid ourselves of the Facebook problem. youbroketheinternet.org is a think tank of people working on an alternative internet stack to replace the current internet.

Footnotes

|  |  |
| --- | --- |
| [[1](#bn1)] | Jernigan, C., and Mistree, B. F. - [Gaydar: Facebook friendships expose sexual orientation](https://journals.uic.edu/ojs/index.php/fm/article/view/2611/2302). First Monday, 14(10)(2009) |
| [[2](#bn2)] | Narayanan, A., and Shmatikov, V. - [De-anonymizing Social Networks](https://www.cs.utexas.edu/~shmat/shmat_oak09.pdf). Security and Privacy, 2009 30th IEEE Symposium on (2009), 173-187. |
| [[3](#bn3)] | <https://secushare.org/literature> |
| [[4](#bn4)] | [https://youbroketheinternet.org/#legislation](https://youbroketheinternet.org/" \l "legislation) |