Internet Freedom in Retreat

Internet Freedom in Retreat

The initial hopes associated with the spread of the Internet have gradually diminished. Both in democratic and in authoritarian systems, Internet freedom is contested. The need for reform creates possibilities for new actors to shape the future version of the Internet. A key challenge will be to prevent a splintered Internet.

By Julian Kamasa

The Internet architecture has undergone a wide range of changes since it was devised as a project idea at the European Centre for Nuclear Research (CERN) in Geneva in 1989. At that time, Tim Berners-Lee, a young British computer scientist, developed a concept that essentially founded the World Wide Web. The main emphasis was on the transfer of data enabled by universal standards of transmission. This idea was not driven by commercial interest, but rather a normative one – the creation of a widely available infrastructure for free exchange of information. Associated with this notion was the hope for a decentralization of information sovereignty from the state to users. A wide range of available information, so the aspiration went, would also lower the barriers to entry for lower classes and thereby reduce education inequalities.

Protesters wearing Guy Fawkes masks take part in a demonstration against ACTA (Anti-Counterfeiting Trade Agreement) in Vienna, February 25, 2012. *Lisi Niesner / Reuters*

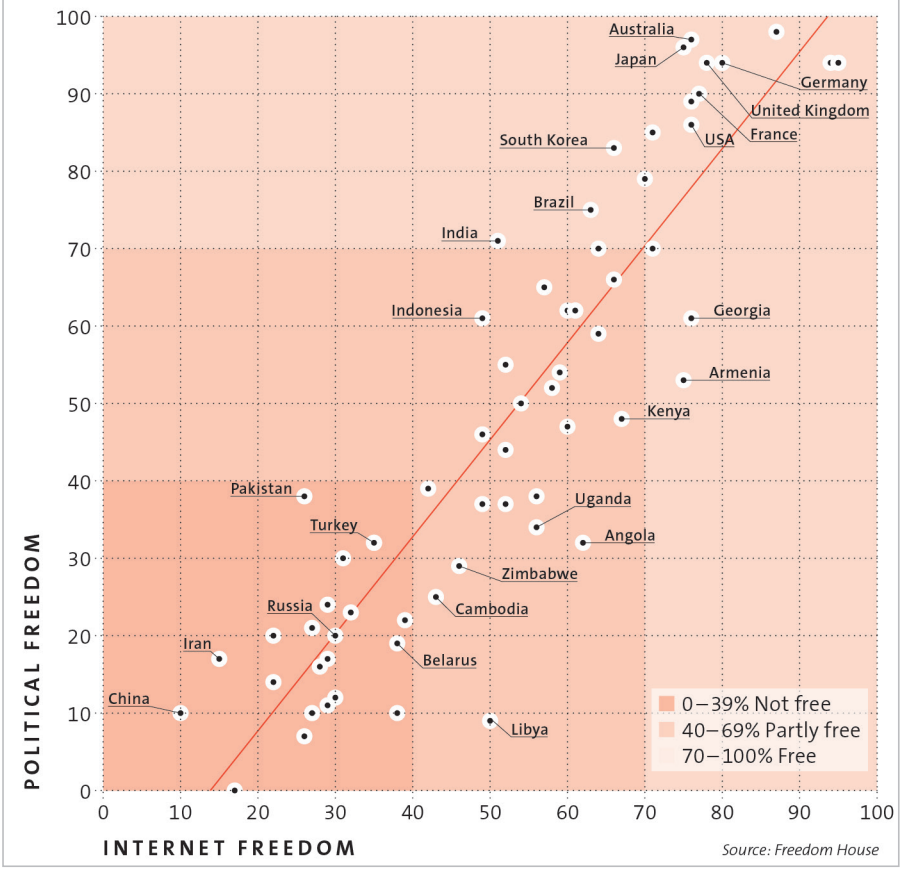
Linked to increased availability of information was also the hope of a democratization wave in non-democratic countries. Former US President George W. Bush said in 1999 "imagine how freedom would spread" with regards to the possibility of the Internet being widely used in China. While this did not transpire in China, elsewhere it certainly did. The rapid development of smartphones and social media platforms in the mid-2000s proved to be an effective tool for political mobilization during the Arab uprisings in North Africa in 2010/11, for example. Pro-democracy protesters in Hong Kong and Belarus are likewise using digital means for mobilization today.

The so-called Arab Spring was a wake-up call for many authoritarian regimes in that regard. Comprehensive digital surveillance and censorship is increasing in many authoritarian systems. In democratic states, however, the extension of digital surveillance tools, aimed at combatting terrorism for example, is often part of a wider sociopolitical debate related to the crucial question of whether the Internet can grant both national security and Internet freedom or whether there might be an inherent trade-off situation. Internet freedom can be de-

fined by three criteria: access, content, and user rights. Ideally, the first is not constrained by infrastructural, economic, or politically motivated barriers such as shutting down the whole Internet or certain social media platforms. Content should not be limited by filtering, manipulating, censoring, or blocking procedures essentially constraining media diversity. User rights are given, when surveillance is proportionate and users do not experience severe consequences such as imprisonment or physical attacks for online activities.

It is worth noting that the ambitious visions of 1989 concerning the role of the Internet have not fully materialized even in democracies, let alone in authoritarian states. In democratic systems, the Internet can be seen as a double-edged sword. On the one hand, new elements of democratic practices, such as grassroots movements or citizen labs and assemblies, are well-organized thanks to the Internet and its effective use in spreading pro-democratic messages. At the same time, radically anti-democratic, highly simplified, and heavily misleading messages may also be amplified by the use of digital means, thereby seriously undermining the role of media as the fourth estate of democracy. Not only democratic systems are challenged, but, according to reports by Freedom House, digital freedoms on the whole are in steady decline, while state-controlled Internet is on the rise. Diverging versions of the Internet could become problematic for standardization processes of the global Internet architecture. Many actors with different visions are currently trying to shape this process, which has become increasingly political. This development raises the question of whether the final outcome will be more control for users, states, or big-tech, and whether the Internet will be able to increase both security and freedom.

Internet and Political Freedom in 2020



Digital freedoms on the whole are in steady decline, while state-controlled Internet is on the rise.

Internet Freedom in Democracies

A free, open, and rule-based Internet as an additional channel of free speech has become an important component of democratic systems, since it enables freedom of expression for people whose voices may be unheard when using non-digital means of expression. Since 2014, Freedom House has issued a yearly report on Internet freedom measuring obstacles to access, limits on content, and violation of user rights in 65 countries, which account for 87 percent of the global Internet user population. Similarly, it analyzes political freedom in 195 countries, taking into account political rights and civil liberties. Countries are classified into three categories: free, partly free, and not free. A comparison of the two reports suggests that there is a link between political freedom, on the one hand, and Internet freedom, on the other (see graph). Indeed, 80 percent of the 15 countries with a free digital sphere are also politically free. It would, however, be misguided to assume that political freedom serves as a precondition for Internet freedom and *vice versa*.

Citizens in Armenia and Georgia are, for instance, granted similar levels of digital freedom as in the US, Japan, and the UK. Yet, basic political rights in both countries are constrained by their respective governments. Conversely, in Brazil, India, and South Korea there are strong violations of user rights, which, in India, are combined with striking obstacles to Internet access. In South Korea, despite high digital literacy and excellent network coverage, pro-government commentators attempted to manipulate discussions online and prosecutions related to the spread of pro-North Korean content took place. Furthermore, the Infectious Disease Control and Prevention Act aimed at containing the coronavirus has increased digital surveillance, substantially resulting in state access to credit card records and security cameras as well as phone location tracking (see CSS Analysis 264).

The state of the Internet is far from perfect in democracies. Sharing personal data for more personalized content serves as a necessary precondition for basic online activities. This user-tailoring may be beneficial for politically harmless activities such as video streaming, holiday planning, or online shopping. However, when citizens receive politically relevant information, it is ever more crucial that news is not misleading and well-balanced. Yet, filter bubbles limit the possibility of having one's view

challenged by contradictory opinions. Instead, such bubbles confirm pre-existing beliefs of target audiences and, in addition, have the potential to amplify strong anti-democratic views, misleading information, and conspiracy theories. This has become a considerable challenge for democracies not only during the still ongoing pandemic, but also before important elections. Many governments increasingly have to balance supporting well-informed citizens and the need to regulate, or even censor, some messages without compromising democratic norms and values.

Contract for the Web

Sir Tim Berners-Lee, inventor of the World Wide Web, issued a contract in cooperation with over 80 organizations. After a public consultation process including inputs from more than 600 people, the contract was drafted and published in July 2019. It contains specific principles for governments, companies, and citizens with the aim of improving the state of the Internet. Governments should guarantee **connectivity** to the Internet for everyone, ensure that **availability** is given at all times as well as protecting fundamental **privacy and data rights** of citizens online. Companies, on the other hand, are supposed to enable both an affordable and available Internet for everyone, build more trust online by protecting personal data, and create human-oriented technologies. Finally, citizens are urged to act as online creators and collaborators, to exchange with one another in a respectful and dignified manner, encouraging strong "community building", and, lastly, to defend the Internet. Supporters of this contract include not only big companies such as Google, Facebook, Microsoft, Twitter, and Amazon, but also non-governmental organizations, including Reporters Without Borders, or non-profit organizations, such as the Open Data Institute.

Digitalized State Control

In authoritarian systems, the role of the Internet is very distinct from the one in democracies. Since governments are well-aware of its potential to educate users, censorship tools are in place in numerous countries. This creates narrower filter bubbles, which allow governments to be in control of the narrative. The most extreme restrictions are in China and Iran, but the overall trend is toward a more controlled Internet, even in countries with past ambitions of EU accession. In Turkey, for example, a new law forces social media platforms to be compliant with its censorship and surveillance policies, which effectively constrains an important channel of free speech. Digital surveillance is far more sophisticated and aimed at increasing domestic security and political stability. Attempts to express critical political opinions online by journalists, activists, or bloggers may result in them being arrested, physically harmed, or even killed.

Since 2017, the Internet went down in 18 other African countries for political and not technical reasons.

On a more fundamental level, it is not uncommon to shut down access to social media or the Internet as a whole. This happened in Zimbabwe after anti-government protests in 2019, leaving citizens cut off from the Internet and social media. Since 2017, the Internet went down in 18 other African countries for political and not technical reasons. In Russia, the so called "Sovereign Internet" law could further reinforce an already ongoing trend, which is reflected in the large-scale blocking of foreign websites. This legislation could potentially decouple Russian citizens from the global Internet.

The number of countries with the most severe Internet restrictions has increased from 15 states in 2014 to 22 countries in 2020, while the number of countries with a free Internet is steadily decreasing. Out of the countries with no free Internet for its citizens, Pakistan is the only one with significantly less restrictions in the non-digital sphere, especially as far as civil liberties are concerned. The opposite case is, however, more clearly pronounced in countries such as Angola, Belarus, Cambodia, Libya, or Uganda. This is particularly observable in Libya, where political rights and civil liberties are practically non-existent, whereas digital freedom is comparable with the one in India and, to some extent, Singapore.

From Internet to Intranet

The prime example of digital control is in China, which has effectively resulted in a nationalization of the Internet. Its Great Firewall is a digitalized national border which enables the blocking, filtering, and censoring of information entering and leaving the country. Services provided by tech companies from the US such as Twitter, Facebook, or Google have been unavailable to users in China for almost a decade. In 2009, Twitter was blocked before the 20th anniversary of the Tiananmen Square protests. Facebook and YouTube experienced the same after both were used during the July 2009 Ürümqi riots in Xinjiang. Google then was banned in 2010. Attempts to return to China with a compliant and thus censored search engine, called Project Dragonfly, were met with strong opposition by Google employees and had to be cancelled. All banned US services have domestic equivalents, some of which are globally successful. Sina Weibo has more users than its rival Twitter and Tiktok could surpass its competitor Instagram.

In Iran, access to the Internet is likewise heavily restricted. A nationwide shutdown of the whole internet for one week as a response to mass protests in late 2019 is one of many examples of governmental measures to restrict citizens' digital liberties. Attempts to publish political messages online can also result in years of imprisonment. A draft partnership agreement with China foresees, among other things, Chinese assistance to Iranian authorities in extending control of the Internet as well as providing essential solutions by Chinese tech companies such as the *Beidou* satellite navigation system or 5G telecommunications networks. Even if this proves a success for China, it would be ill-advised to assume that Beijing has an explicit plan in exporting its version of the Internet on a large scale. Instead, it represents an attractive alternative model which, to some extent, many like-minded states are willing to follow.

European Initiatives

In an environment marked by a decline in digital liberties and competition for technological supremacy between Washington and Beijing, Europe could find a niche in order to provide an alternative Internet model to the ones put forward by the US and China. The latter model is clearly at odds with norms and values, such as freedom of expression, which European democracies stand for. However, there are ongoing differences with US tech companies too. A record high antitrust fine of 2.4 billion EUR in a landmark case of the EU Commission against Google has caused strong anti-EU reactions in the White House. The recent annulment of the US data-sharing agreement by the European

Court of Justice is another instance of diverging views on market competition and user rights. The regulatory approach of the EU has been relatively successful in the case of the General Data Protection Regulation (GDPR). But, even though the GDPR was able to indirectly shape certain standards outside of the EU, for example in California, it still has limited regional scope. Most importantly, the GDPR will not have a direct effect on the entire Internet architecture.

The US achieved technological dominance but it did not do so through regulation. Therefore, the question is whether the EU will be willing to go beyond its regulatory approach and shape the Internet through innovation too. The biggest leverage in setting standards offline is the EU's highly competitive Single Market. Hence, the creation of a Digital Single Market may provide a way forward toward a globally competitive and innovative ecosystem of regional and global tech companies that shape standards through patent applications. Becoming a world-leading block of technological innovation would result in the EU being truly recognized on the world stage, which can be a decisive factor as far as standardization processes of the overall Internet architecture are concerned.

On a less political level, the inventor of the Internet, now Sir Tim Berners-Lee, has chosen to initiate a Contract for the Web in a multi-stakeholder approach with companies, non-governmental organizations, and policy experts (see box). The aim is to improve the current state of the Internet in order to make the Web what Berners-Lee initially hoped it would be: a mechanism for granting everyone the possibility of using the Internet to learn, exchange ideas, collaborate, and create a space without restrictions on freedom, abuse, disinformation, or violations of privacy. A team of researchers at the Swiss Federal Institute of Technology in Zurich (ETH Zürich) has developed project SCION, which seeks to decentralize data flows and reduce complex Internet protocols (IP) based on US-standardization from the 1990s. This technical reform of the Internet architecture aims to increase trust through significantly enhanced IT security and is already being used by the central bank of Switzerland for communication purposes with its branch in Singapore.

The question is whether the EU will be willing to go beyond its regulatory approach and shape the Internet through innovation.

Outlook

The emergence of new technologies has great potential to considerably transform today's over 30-year-old Internet architecture. Since growth in users is limited, the main expansion is expected in devices that will result in increased connectivity between users and devices, on the one hand, and among devices, on the other. This is more commonly known as the Internet of Things (IoT). The disruptive potential of the IoT, in combination with significant progress made in the field of Artificial Intelligence, has important geopolitical implications.

Technological leadership is part of increased competition among great powers. To what extent this may influence processes of standardization, as well as global Internet governance, is unclear for the moment. However, the structural inability of the World Trade Organization to act shows what kind of negative ramifications an erosion of multilateralism can have for global trade. Increasing protectionism is, essentially, a zero-sum-game, in which powerful states will have the means for unilateral action, at the expense of smaller states. The already splintered Internet runs the risk of going in a similar direction. In contrast to trade, which does not directly affect industries oriented on domestic markets, digital protectionism would hit every user of the Internet hard.

It is, therefore, necessary for actors with the ability to set standards to opt for lowest common denominators and provide constructive criticism in order to prevent the erosion of multilateralism in cyberspace. The presentation of a new IP by the Chinese company Huawei has met rather fundamental opposition. While critics may reject the idea of a new Chinese IP, the old US-based IP is still in need of reform. This has likewise been recognized by the Swiss scientists designing SCION. For actors with the capacity to shape the Internet architecture, the very idea of a Chinese Internet should be a wake-up call and an invitation to answer Chinese ambitions not primarily with criticism, but with competitive ideas.

For more on perspectives on Socio-technical resilience, see CSS core theme page.

Julian Kamasa is a Researcher in the Swiss and Euro-Atlantic Security Team at the Center for Security Studies (CSS) at ETH Zürich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zurich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Névine Schepers
Language editing: Lisa Watanabe
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000447265