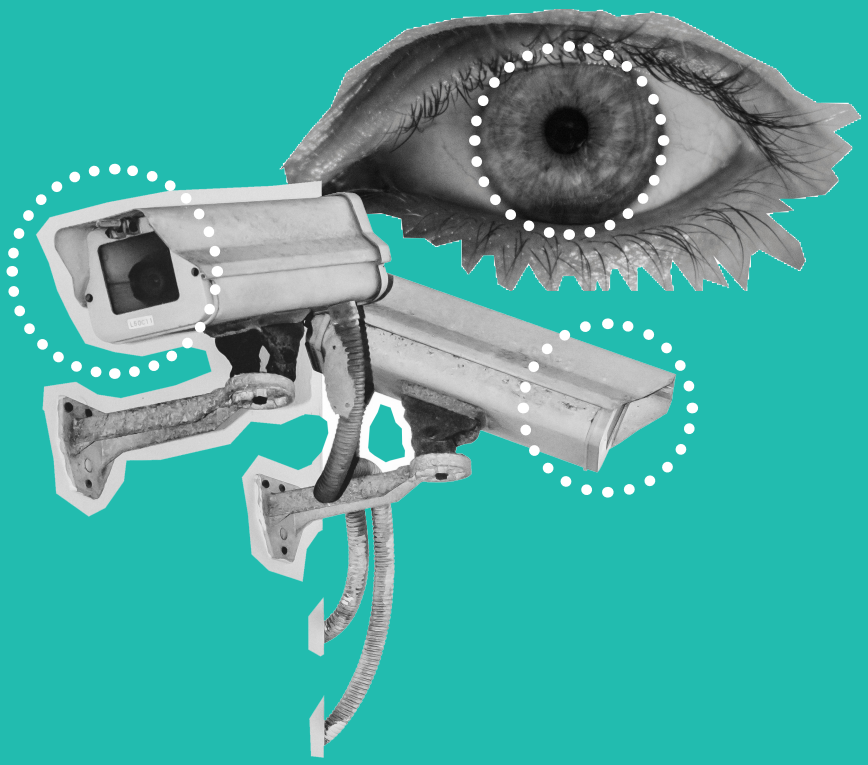
CROSS BORDER DATA FLOWS, PRIVACY, & GLOBAL INEQUALITY



Materials produced by Burcu Kilic and Renata Avila
for Public Citizen, under a

GOOD RESEARCH TAKES TIME AND EFFORT, PLEASE ATTRIBUTE ;)

FOR FURTHER INFORMATION, PLEASE CONTACT
bkilic@citizen.org **OR** renata@digitalcolonialism.org
OR VISIT https://www.citizen.org

PUBLICCITIZEN

OVERVIEW

The right to privacy is a fundamental right. However, this right is continually facing new threats in today's increasingly digitally connected age.

Until now, "Big Tech", the bloc of the dominate technology companies, has enjoyed a vastly unregulated global marketplace. However, a series of recent scandals involving the abuse of personal data have led to a backlash from the public and national regulators. Following the Facebook Cambridge Analytica scandal[1], the calls for regulation of online platforms are becoming louder, leading lawmakers, citizens, advocacy organizations, and governments to demand better privacy protections. Widespread awareness of Facebook's gross mishandling of their users' data provides us all with a better understanding of the stakes involved, as well as offering a prime opportunity to demand better protections and regulations to uphold the public interest and advocate for more of a balance between commercial and consumer rights.

WHOEVER CONTROLS THE DATA WILL CONTROL THE FUTURE

As more countries gain internet access and enter into digital marketplaces as users of online platforms and services, the flow of data is becoming more and more complex. Addressing questions around how private and public entities access and control data has become increasingly critical, especially as we consider issues related to privacy, human rights online, and global inequality.

DATA PROTECTION AND GLOBAL INEQUALITY

The goods and services that fuel our current and future digital economies run largely based on the enormous amount of data that users and consumers generate every day. Disparities in the flow of data between the developed and the developing world can have an enormous impact on local economies, as data, the new "oil" according to the Economist magazine[2], is extracted from the global south for economic gain in the global north. When big economies advocate for free, unconditional, unregulated and unrestricted flow of personal data, they are able to capitalize off of this valuable raw material without consideration to the benefits or rights of the consumers in the original jurisdiction. How, if algorithms are always trained and designed abroad, can small and medium sized economies grow their own competitive domestic markets, especially without the resources and scale of the larger companies? Some governments have suggested a nationalistic approach to force data localization. However, these policies would adversely affect citizens by driving up prices and potentially having serious repercussions for human rights.

The privacy and security gap exacerbates global inequalities and the vulnerability of much of the world's population. Due to new regulations, the data of European citizens is protected at a much higher standard than the rest of the world. American citizens also have additional safeguards for their personal information. Meanwhile, global platforms based in the U.S. push for uniform rules to regulate data extraction while at the same time advocating for weakening privacy rules outside the protected European Union. They argue that the free flow of data is a basic precondition for development everywhere. However, as this data mostly flows in one direction, this free flow inordinately benefits these big technology companies. At the same time, regulations in the developing world do not offer the same privacy protections as citizens of developed economies. Thus, the global balance tilts heavily against consumers form the global south.

---

[1] The scandal involved the harvesting of 50 million profiles from Facebook through data made available to third-party researchers by Facebook. For more details, see Carole Cadwalladr, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," The Guardian, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[2] The Economist: The world's most valuable resource is no longer oil, but data, May 6 th 2017, available at https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

IS NATIONALLY LOCALIZED DATA THE ANSWER?

At the same time, widespread revelations of mass surveillance and increasing security concerns have driven some countries to enact laws demanding that require data to be stored locally. There is evidence that these policies have resulted in increased costs for companies and as a consequence, higher prices for consumers, but there is little to no data on the economic benefits of local storage/computing facilities in the middle and long term. For example, there is not much information available on how data localization could contribute to domestic industrial development in machine learning or even AI.

Before any decision is made on international binding standards for the flow of data, besides consideration of the issues of privacy and security, there must be serious investigation of the effect of transnational data flows on developing economies. Many claims are made regarding the societal and economic benefits of the free flow of data. As of the time this document was published however, there are little to no rigorous studies investigating the economic and social impact of the free - deregulated - flow of data.

It is vital that there are no attempts to rush regulatory decisions that will have far reaching consequences for the future global economy and relationships of power between states.

Any such action must be approached cautiously and made only on the basis of thorough and in-deoth research exploring the many social, econòmic, and political repercussions of these policies. An adverse decision could lead to a dysfunctional arrangement which could further consolidate the monopoly of Big Tech, exacerbate global inequality, and erode the privacy rights of citizens around the world.

WHO ARE THE PLAYERS INVOLVED?

The future of data in the global trade arena involves three general groupings of countries.

1. The first group advocates for the free flow of data and privacy safeguards based on individual jurisdictions, and encompasses countries which host the leading companies and the Big Tech lobby. For these countries, the idea of subjecting digital privacy and data flow issues to the rules of global trade is convenient. Since these countries tend to dominate trade negotiations, it offers their tech industries a convenient platform to establish predictable rules to protect the status quo and their considerable market share.

2. The second group of countries advocates for local storage of data and stricter domestic privacy controls. While some of these countries may adopt these policies out of a desire for greater governmental control over citizens, these policies are also frequently adopted due to privacy or security concerns, or as a protective measure to allow domestic industries to grow. This group of countries has been severely criticised by the first group, which has accused them of attempting to "balkanise the Internet."

3. The third group of countries has very little say in these policy debates, as their local industries and markets are so small, and the installed technical capacity is so low that imposing restrictions on data flows would mean companies leaving them with no alternative. Many of the countries in this third group share a similar profile: they have among the lowest privacy standards and consumer protections in the world, and a significant portion of their populations are still disconnected from the internet.

Europe occupies a position between the first and second groups, advocating for the free flow of data from the developing world, while establishing regulations to protect its own citizens. Many have called for the GDPR (General Data Protection Regulation) to extend beyond European borders to become the global standard. However, it is unclear at this point if these actors will remain committed to advocating for this standard outside of European jurisdictions.

WHY SHOULD I CARE?

Data and its role in society – from allegedly disrupting referenda and elections to worsening discrimination — is under more scrutiny than ever. The repercussions of inadequate and unenforceable privacy protections against certain forms of data profiling are now beginning to be seen in countries around the world. At the same time, data, which was not a commodity ten years ago, is driving the most advanced industries in the world, while the economic benefits of this data remain out of reach for the vast majority of countries.

As Professor Steven Weber indicates "the more data you have, the better the data products you can develop; and the better the data products you develop and sell, the more data you receive as those products get used more frequently and by larger populations." Quasi monopolistic companies in Europe and America are rushing to connect the next billion people to the internet. But if all the world's data flows in one direction, without restrictions or taxes, this will further reinforce their monopolies over the world's data, widening the privacy gap, and leaving developing countries as consumers or data points, rather than participants in the digital economy.

FOR INTERNET ACTIVISTS, CONSUMERS AND WORKERS

So far, the only leverage many countries have is that their populations – the global poor – continue to lack access to data services, and remain disconnected from the digital economy. From the perspective of Big Tech, these are untapped markets, and these countries may be forced to liberalise data flows in order to attract companies. More often than not, those countries with the lowest Internet penetration also lack two key public interest components: 1) privacy and data protection regulations and 2) consumer protection laws. Liberalising data flows in these countries could have adverse effects. Before worldwide data liberalisation becomes a reality, certain necessary steps must be taken. What we need is a global standard of privacy and data protection norms and for governments to align themselves to demand these protections.

PUBLICCITIZEN

THE BIGGER PICTURE

Companies and governments are rushing to connect the next billion people to the internet. There is no shortage of proposals for how Big Tech can improve the lives of the poor across the Global South. From deploying biometric readers that determine the age of refugees, to using electronic cards to track and improve the habits of those receiving conditional cash transfers, there is a tendency to experiment with new technologies on marginalized or vulnerable communities. What is lacking is the political commitment to treat all netizens equally, affording everyone the same level of trust, privacy and security, regardless of nationality or economic circumstance.

At the same time, advocates for data liberalization are arguing that privacy is something relative, connected to cultural norms and practices, and that therefore citizens in different jurisdictions should be protected differently. There is a general refusal among data liberalization advocates to adopt the highest privacy and data protection available: the European standard, enshrined in the GDPR. Meanwhile, the Supreme Court of Justice in India has boldly opposed this consensus, issuing a robust judgment in favor of privacy rights for its citizens.

The web has made our world increasingly borderless, and digital privacy should be a privilege enjoyed by all jurisdictions. Strong, global, and uniform privacy and personal data protection, together with efficient and effective enforcement mechanisms, is the sine qua non requirement for a digital society promoting equality and development.

WHAT CAN I DO?

- Encourage your government to better understand what data means domestically and to invest in innovative ways to develop local data capacities.
- Demand that the platforms you use respect your privacy and that you are given the higher standard of privacy granted to users in Europe and North America.
- Campaign to reverse the trend of privatization of data infrastructure, making sure your government and domestic industries are not left behind in the digital revolution.
- Stay vigilant on all the bilateral and multilateral agreements your country signs, which might undermine your privacy and data rights.

PUBLICCITIZEN