SOURCE CODE, CYBERSECURITY, AND TRADE

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

If you look around, everything is becoming internet-enabled — from our phones to our cars, from home appliances to hair dryers — and these devices are running software and hardware that is rarely audited. In the near future, attacks against software and hardware will become more common. As long as it is illegal to audit the software whose vulnerabilities precisely enable such attacks, the world cannot aim at a more secure and trusted technology ecosystem.

The opportunity is now to revisit global norms about source code disclosures, and demand that openness is required by law.

BACKGROUND

As more devices get connected to the internet, we increasingly rely on these devices to manage our daily tasks. With 8.4 billion connected devices in 2017 and more than 20 billion connected devices by 2020, they do everything from performing key roles in public health and transport facilities to overseeing the most intimate aspects of our lives.

But what if we cannot know what is happening inside those devices? What if, by law, we cannot have independent audits to make sure that the devices are doing what they are supposed to do, and nothing else? As was widely reported by the media, home devices have tracked all movements inside a household and have sent that data to their home servers at off-site data centers. And think of smart cars, for instance, which are becoming a Big Brother on wheels. They transmit tons of data to their manufacturers, including where the car goes and maybe eventually, recordings of conversations that take place inside the vehicle. Or, at a national and municipal level, entire governments will have to rely on the good faith of private providers to perform critical functions, at the cost of ignoring whether these services compromise the privacy and security of citizens. It is a matter of preserving and protecting key infrastructure. Citizens and institutions are already demanding that companies selling network-based services, products, and tools run software that is open and transparent so that anyone can audit it, improve it and increase its security.

SOURCE CODE

The term “source code” refers to a computer program in a human-readable format. Access to source code is important from the users and licensee’s perspective so that they can understand how a program works and adapt it to particular needs. The issue of source code access has lately become a contested topic in trade agreements. Since the Trans-Pacific Partnership negotiations, trade agreements have come to include provisions that restrict access to source code. The need for independent security audits becomes critical as everything around us becomes internet-enabled, and therefore vulnerable to malicious hacking. Restricting public access to source code therefore puts our privacy and security at risk.

PUBLICCITIZEN

WHO ARE INVOLVED?

Negotiating governments are the real actors in trade agreements. They are represented by ministries of trade and economy, which tend to represent a very specific set of multinational corporate interests — including Big Tech — in their countries. The negotiations are secret and take place behind closed doors. Public interest groups, the public, and the press are excluded from active discussions or information about draft texts.

WHY SHOULD I CARE?

Source code audits ensure that software has no vulnerabilities or functions that can be exploited for attacks. By restricting access to source code, our governments compromise cybersecurity and privacy. Key infrastructure is plagued with many failure points and security gaps, so the implications can be far-reaching. Regulators must be able to access source code to investigate or remedy anti-competitive, discriminatory, abusive or fraudulent behavior perpetrated by private actors.

FOR INTERNET ACTIVISTS, CONSUMERS AND WORKERS

Mandatory access to source code will not only make citizens more secure, it would also spur innovation as we would all benefit in gaining understanding on how our technologies are run and improve it to fit our needs. Software companies are traditionally uncomfortable about having outsiders look at their source code. But if the review is structured carefully, the value of increased public trust would vastly exceed the risk of disclosures.

Instead of restricting the access to code, we should demand that it is made available for viewing by everyone. This is especially important for source code of software that deals with children, health, safety and security issues, and key infrastructure. The global trade arena offers us an opportunity to reverse the trend and prevent future conflicts that threaten peace, security, competition, privacy, and freedom.

WHAT CAN I DO?

Demand that all trade agreements include provisions establishing access to source code as a default and that free software is rewarded as a tool to improve trade and foster innovation. With better audited code and more transparency, citizens would be more secure, and freedoms and rights of people would be effectively protected.

PUBLICCITIZEN