AUGUST 15, 2018 eff.org

Google Needs To Come Clean About Its Chinese Plans

Eight years after Google initially took a stand against Internet censorship by exiting the Chinese search market, we are disappointed to learn the company has been secretly re-considering an extended collaboration with the massive censorship and surveillance-wielding state. According to an Intercept report released at the beginning of the month, Google is working on a censored version of its search service for release in China.

In 2010, EFF and many other organizations praised Google for refusing to sacrifice the company's values for access to the Chinese market. At the time, this move followed public backlash and several attacks on Google's infrastructure that targeted the personal data of several prominent Chinese human rights activists. Google's departure from China showed that strong core values in fundamental human rights could beat out short-term economic gain in the calculus of an Internet company.

But now it seems the company has reversed course.

This news comes amid other reports of American tech giants compromising values to enter or remain within China: Facebook has piloted a censored version of its own platform, and Apple recently faced criticism for moving its customers' data into China-hosted servers, and adding code to filter the Taiwanese flag emoji in Chinese locales.

Within China, Google's direct competitor, Baidu, has been facing a significant amount of social, regulatory, and economic backlash over recent advertising malpractice, such as monetizing questionable medical advertisements, heavily deprioritizing non-Baidu services, and allegedly promoting phishing sites. There may well be a growing demand for competition within the Chinese

search engine market.

In even considering these changes, Google needs to tread carefully. In the wake of the last wave of engagement with the Chinese market, and to prevent Internet companies being complicit with human rights' violations, the company joined with Microsoft and Yahoo! to create a set of standards for working in countries with poor human rights records: the Global Network Initiative's Implementation Guidelines. EFF was a founding member of the GNI, but subsequently left the coalition in 2013 due to concerns that the companies were unable to be forthcoming about their involvement in state surveillance, even within a confidential environment.

From the outside, it's unclear to us whether this project has yet to be considered in the light of that agreement. GNI's Executive Director has told reporters, in part, that "All member companies are expected to implement the GNI Principles wherever they operate, and are subject to independent assessment, which is overseen by our multi-stakeholder Board of Directors." It might reassure Google's own staff and external critics to be told that process was being followed, and if both the GNI and Google were more public about the results of that procedure.

But for now, it seems the company has opted to prepare new Chinese plans outside the view of the public, and even behind the backs of many of their own employees.

From 2006 to 2018: Both Google and China are more powerful than ever

Our original concerns from 2006 still stand today, but in 2018, the potential for damage when large tech companies co-operate with repressive states has grown.

Since 2006, Google's capabilities have expanded massively. We live in an era in which Google-owned tracking scripts are present on an incredible 75% of the top million websites. Google's personalized profiles of its users across several online services help it provide "relevant" search results and advertisements.

Simultaneously, in order to sustain their position on strong censorship, the Chinese government has had to implement broad and pervasive surveillance laws and technology. In particular, the explosive dominance of centralized applications like Weibo and WeChat, whose communications and transactions are regularly surveilled and censored, has ultimately transformed the digital landscape in China.

2017 in particular saw a new wave of regulatory crackdowns aimed towards strengthening digital surveillance practices across the Chinese Internet. In particular, the government began restricting tools used for anonymity and privacy by arresting local VPN providers, banning end-to-end chat

applications like WhatsApp, and mandating Internet platforms to require offline identity verification. In certain regions of China, citizens merely attempting to use foreign or encrypted applications like WhatsApp or Telegram can have their service cut off and are asked to report to the police.

It's not clear how or whether Google's planned offerings will comply with these new national regulations, or whether exemptions would be worked out for the tech giant.

At this early stage, it's this lack of transparency that concerns us most.

What happened to transparency within Google?

Google once prided itself in its internal organizational transparency, especially when compared to giants like Apple, famous for their secrets veiled in black cloth. However, as we saw with Project Maven, Google's controversial AI contract with the Department of Defense, executives within the organization are willing to keep projects quiet in the face of potential backlash. The initiative was not publicized, and came to light only when employees noticed and brought it to the forefront of internal discussion forums.

Unlike in 2006, when Google was open (and even apologetic) about the quality and nature of its service in China, this new iteration was developed with little external or internal visibility. A source at The Intercept reports that knowledge about Google's China project was "restricted to just a few hundred members of the Internet giant's 88,000-strong workforce." Though Project Maven was not publicized, this information was at least available to employees. This time, the vast majority of employees discovered the existence of the China project only after these emails were leaked to the public media.

That means certain questions remain unanswered, not just publicly, but even among Google's own staff. What sacrifices will Google make to its own operating practices in order to enter the Chinese market? Will it have to comply with China's internal strict regulations, and how will these compromises affect its offerings outside of China?

The public, Google's users, and Google's employees have been kept increasingly in the dark about compromises on the company's own values that could massively affect the lives of not only citizens within China or the U.S., but also Internet users around the world. Google has already committed to processes that consider human rights when entering new markets in the Global Network Initiative. Is it following them?

Google is an effective gatekeeper of the Internet for a large majority of the world. It's the portal

through which many access the Internet, and through which Google itself continues to collect troves of information about these users across a variety of platforms. With that kind of responsibility, everyone — inside and outside Google — needs to stay vigilant and continue to hold the giant accountable. Avoiding internal oversight and criticism will not evade the backlash that will come from launching a complicit service, or the damaging consequences to Chinese users when Google's compromises are used against them. It is better to have this debate now, in public, than to pick up the pieces when the damage has been done.

RELATED UPDATES

PRESS RELEASE | AUGUST 6, 2019

EFF Delegation Returns from Ecuador, says Ola Bini's Case is Political, Not Criminal

San Francisco – A team from the Electronic Frontier Foundation (EFF) has returned from a fact-finding mission in Quito for the case of Ola Bini—a globally renowned Swedish programmer who is facing tenuous computer-crime charges in Ecuador. Bini was detained in April, as he left his home in Quito to...

DEEPLINKS BLOG BY BEN BALLARD, VERIDIANA ALIMONTI | JULY 23, 2019

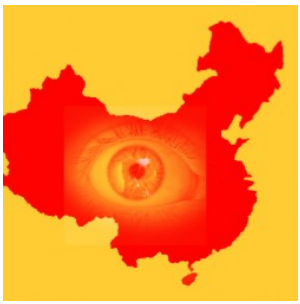
New Chilean ¿Quién Defiende Tus Datos? Report Shows Greater ISPs Commitment to User Privacy

Derechos Digitales, the leading digital rights organization in Chile, published its third annual **Who Defends Your Data** report today, in collaboration with EFF. The report assesses whether the country's top ISPs enforce privacy policies and practices that put their users first. Kurt Opsahl, EFF's Deputy Executive Director and General...

DEEPLINKS BLOG BY DANNY O'BRIEN, JASON KELLEY | JUNE 11, 2019

EFF to U.N.: Ola Bini's Case Highlights The Dangers of Vague Cybercrime Law

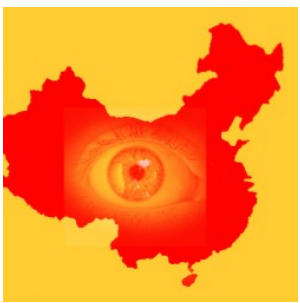
For decades, journalists, activists and lawyers who work on human rights issues around the world have been harassed, and even detained, by repressive and authoritarian regimes seeking to halt any assistance they provide to human rights defenders. Digital communication technology and privacy-protective tools like end-to-end encryption have made this work...



DEEPLINKS BLOG BY THREAT LAB | JUNE 4, 2019

30 Years Since Tiananmen Square: The State of Chinese Censorship and Digital Surveillance

Thirty years ago today, the Chinese Communist Party used military force to suppress a peaceful pro-democracy demonstration by thousands of university students. Hundreds (some estimates go as high as thousands) of innocent protesters were killed. Every year, people around the world come together to mourn and...



DEEPLINKS BLOG BY GENNIE GEBHART | MAY 7, 2019

Human Rights Watch Reverse-Engineers Mass Surveillance App Used by Police in Xinjiang

For years, Xinjiang has been a testbed for the Chinese government's novel digital and physical surveillance tactics, as well as human rights abuses. But there is still a lot that the international human rights community doesn't know, especially when it comes to post-2016 Xinjiang. Last Wednesday, Human Rights Watch...

DEEPLINKS BLOG BY DANNY O'BRIEN | APRIL 16, 2019

The Ecuadorean Authorities Have No Reason to Detain Free Software Developer Ola Bini

Hours after the ejection of Julian Assange from the London Ecuadorean embassy last week, police officers in Ecuador detained the Swedish citizen and open source developer Ola Bini. They seized him as he prepared to travel from his home in Quito to Japan, claiming that he was attempting...

DEEPLINKS BLOG BY DANNY O'BRIEN | MARCH 26, 2019

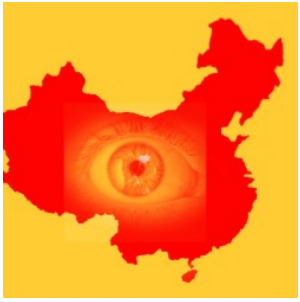
EU's Parliament Signs Off on Disastrous Internet Law: What Happens Next?

In a stunning rejection of the will of five million online petitioners, and over 100,000 protestors this weekend, the European Parliament has abandoned common-sense and the advice of academics, technologists, and UN human rights experts, and approved the Copyright in the Digital Single Market Directive in its entirety...

DEEPLINKS BLOG BY VERIDIANA ALIMONTI | MARCH 21, 2019

Who Defends Your Data? Report Reveals Peruvian ISPs Progress on User Privacy, Still Room for Improvement

Hiperderecho, the leading digital rights organization in Peru, in collaboration with the Electronic Frontier Foundation, today launched its second ¿Quien Defiende Tus Datos? (*Who Defends Your Data*?), an evaluation of the privacy practices of the Internet Service Providers (ISPs) that millions of Peruvians use every day. This year's...

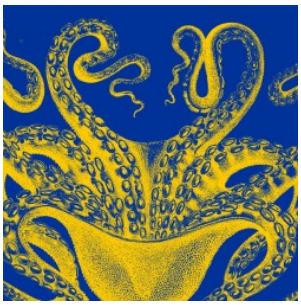


DEEPLINKS BLOG BY DANNY O'BRIEN | MARCH 1, 2019

Massive Database Leak Gives Us a Window into China's Digital Surveillance State

Earlier this month, security researcher Victor Gevers found and disclosed an exposed database live-tracking the locations of about 2.6 million residents of Xinjiang, China, offering a window into what a digital

surveillance state looks like in the 21st century. Xinjiang is China's largest province, and home to China's Uighurs...



DEEPLINKS BLOG BY KATITZA RODRIGUEZ | FEBRUARY 21, 2019

What's the Emergency? Keeping International Requests for Law Enforcement Access Secure and Safe for Internet Users

Law enforcement access to data is in the middle of a profound shake-up across the globe. States are pushing to get quicker, deeper, and more invasive access to personal data stored on the global Internet, and are looking to water down the international safeguards around privacy and due...