

"Digital Trade" and Reproductive Justice

Post-*Roe*, people who receive, provide, fund or otherwise assist with abortion services are increasingly vulnerable to prosecution and other forms of adversity. In this hostile climate, individuals are — by necessity — rightfully encouraged to take prudential measures to protect their privacy. At the same time, unequal access to technology and information, coupled with the unreasonableness of ensuring that one's self and those around them engage in a lifetime of perfect "spy craft" both pre- and post-abortion, point to the urgent need for municipalities, states and the federal government to adopt binding measures to better protect people's privacy for the long term. It is therefore crucial that the "digital trade" provisions in pending trade agreements that are designed to liberalize cross-border data flows and to harmonize regulations not be allowed to restrict governments' ability to enact policies designed to protect data privacy, including policies related to the collection, storage, transmission, trade and sale of individual's medical records, financial transactions, geolocation, search history, messaging and more.

In recent years, as the United States and the world have begun grappling with how to best regulate Big Tech in areas including consumer privacy, algorithm discrimination, gig economy worker protections, anti-trust and more, corporations have been quietly pushing for the adoption of "digital trade" rules in international agreements that lock in retrograde domestic digital governance policies and restrict new forms of regulation. Pending trade pacts that corporate lobby groups are pressing to include such deregulatory measures within include the Indo-Pacific Economic Framework (IPEF), the U.S.-EU Trade and Technology Council (TTC), the U.S.-Kenya Strategic Trade and Investment Partnership and the Americas Partnership for Economic Prosperity (APEP), among others.

So-called "digital trade" provisions undermine people's privacy and data security by prohibiting limits on data flows or rules on the location of computing facilities. Peoples' every move on the internet and via their cell phones are increasingly tracked, stored, bought and sold — as are interactions with the growing "internet of things" that many people may not even be aware are tracking them nor from which they have a feasible way to opt out. Trade pacts must not restrict governments from acting on the public's behalf in establishing rules regarding under what conditions individuals' personal data may be collected, where it can be processed or transmitted, and how or where it is stored.

Insofar as state governments and other bad actors turn to private corporations for aid in data tracking and analysis, surveillance tools like the ones increasingly used for predictive policing and sentencing, and other law enforcement functions designed to identify and prosecute individuals over abortion, pending trade rules that enable corporations to hide their source codes and algorithms as "trade secrets" are also very concerning. Trade deals must not be allowed to repurpose "trade secrets" rules or establish other "digital trade" rules that limit the ability of regulators, academics, civil society and the public to access and review the underlying technology and to shield corporations from liability for discriminatory conduct and civil rights violations.

Even before *Roe v. Wade*'s overturn, civil rights, consumer, labor and other civil society organizations were <u>warning about "digital trade" agreements</u>' likely adverse effects on data privacy and discrimination. The *Roe* decision further highlights the dangers of allowing international trade rules to restrict policymaking space when it comes to data privacy and algorithm transparency.

For more info, contact <u>info@tradejusticeedfund.org</u> or visit www.TradeJusticeEdFund.org