The Cambridge Security Initiative

'APPLE LAW' BANS WON'T HELP RUSSIAN CONSUMERS, BUSINESSES

DECEMBER 2019

Dr. Victor Madeira

Vladimir Putin has signed a bill banning the sale of electronic devices unless they have pre-installed (so far unspecified) Russian software. Expected to become law on 01 July 2020, this would benefit consumers and help local companies compete with foreign ones, say officials. But Apple—which does not pre-install third-party software—has joined Russian voices in criticising the step. It is the latest toward a Kremlin aim of 'sovereign internet', increasingly free of western technology, allowing for greater domestic surveillance, censorship, and repression.

The so-called 'Apple law' covers 'smart' televisions, phones, computers, and tablets. Publicly at least, politicians seem confident that Apple will not follow through on hints that it may leave Russia if the bill becomes law. This confidence may simply be political 'spin', deflecting attention from accelerating state efforts to take away control of the information and communications technology (ICT) sector from western market leaders. If not, then such politicians underestimate the collective impact of recent Russian government actions.

For example, in 2018, *Rospatent*—officially the intellectual property regulator—rejected an Apple trade mark application for a product name including the term 'AR' (for augmented reality) despite it being common in ICT circles. Yet even government websites describe *Rospatent*'s main role as "providing legal protection for state interests" on "military, special and dual-purpose research and development and technological work". Apple lost its appeal hearing in June 2019.

Shortly after, the Federal Anti-monopoly Service launched an anti-trust investigation, following a Kaspersky Lab complaint about Apple's AppStore access policies that Apple called unfounded. Western intelligence increasingly suspects Kaspersky of links, willing or not, to Russian intelligence. This year, Apple and other foreign businesses have also had to locate data servers in Russia, potentially giving state security unchecked access to user data. And Apple too has been forced to show Crimea as part of Russia on online maps accessed from inside that country.

OUTLOOK

All this has potential implications for anyone either operating, or with a client base, in Russia. State demands for pre-installed Russian software raise serious security, privacy, and compliance risks. Some consumer electronics manufacturers may leave the relatively small local market, giving consumers less choice, decreasing 'e-ecosystem' diversity, creating more vulnerabilities, for example to malware. The risks above will only increase as Russia builds 5G networks with

Chinese technology—much of it poorly designed and insecure, and subject to western sanctions/bans.

The greatest risk remains regulatory uncertainty because Kremlin goals affect how the state applies laws. It is unclear how the new bill would benefit the consumer. Assuming their products would work across different platforms, near-term sales and revenue for local software and related firms could rise as the state drives out western competition. But their ability to meet demand and geopolitical tensions are key variables. Russian companies may well end up in a 'Huawei scenario': shut out of key contracts/markets even if more successful than expected.