Published on *The National Law Review* https://natlawreview.com

Russian War Affects Tech and IP

Article By:

Theodore F. Claypoole

Russia initiated a full-scale invasion of one of its sovereign neighbors and the Western world has responded with censure and fury. Our governments and financial institutions have cut off Russian access to money. Our tech companies, who have been vocally neutral in other conflicts, have sided with Ukraine against Russian. Putin noticed, and has struck back, leading to serious consequences for U.S. big tech, Western IP holders, and our treatment of cybersecurity at home.

Typical for a strangle-hold autocracy that maintains power through fear and intimidation, Russia works hard to control the narratives that its people can see. To that end, the Russian government blocked Instagram, after previously blocking Facebook. Meta's other large social media network, WhatsApp, may soon be blocked as well. Russia has successfully used social media to spread propaganda for years, but the Ukraine war has forced Big Tech to choose sides, with Russia punishing companies that that promote news items that the Kremlin wants suppressed. The Russian government knocked Twitter off the internet for millions of Russian citizens.

This battle has been coming since Russia's social media activity in the 2016 election. According to the Washington Post, "The incremental escalations over the past two weeks between Russia and the tech giants has forced the companies to rethink the ways they police speech online, rewriting their rules as they go in response to the fast-moving conflict. … In the wake of Russian interference in the 2016 election and a global pandemic, companies including Facebook, Twitter and YouTube have moved away from a historically hands-off approach to policing the content on their platforms, creating new rules to attempt to halt the spread of misinformation that they said could cause real-world harm. But the Ukrainian conflict has prompted a flurry of new rule-changing and policymaking as the companies have banned state media outlets and allowed some speech previously considered to be hateful."

Google's YouTube platform blocked all traffic from Russian state media, but Google earlier also removed an app to assist Russians in voting after Google's executives in Russia were threatened by Russian agents. Apple has accommodated the Russian government by configuring IPhones in Russia to promote Kremlin-backed social media platforms, and by refusing to activate Private Relay which could help Russians reach foreign new outlets. Russian law requires big tech companies to maintain executives in Russia, described by many as hostage law. The widening rift between the Kremlin and Big Tech may lead to many U.S. companies abandoning Russia completely.

Putin's move that may have the most significant long-term impact on U.S. business is lifting of patent

enforcement, effectively allowing Russian entities to steal patented Western technology without recourse. Ever the cynical self-serving actor on the world stage, Russia has never been a strong protector of business IP rights. For example, last year Russia was listed by the Office of the U.S. Trade Representative as one of the nine countries on a Priority Watch list for insufficient IP protection and enforcement, while Ukraine "continued to take positive steps . . . toward a transparent, fair, and predictable system for the collective management of copyright royalties." Copyrights are a primary protection for the software business.

Putin's decree drops legal protections for patent holders who are "registered in hostile countries." The decree could affect pharmaceutical companies holding patents on vaccines or other medicines, and may be used to reproduce inventions in the defense or technology industries. The more valuable a company's patents are in Russia, the more the company has to lose.

The next step along this road may be to drop protections for trademarks in Russia and allow local companies to effectively nationalize U.S. and European brands to serve the Russian people. The Washington Post reports, "The Kremlin has not issued any decree lifting protections on trademarks. But Russia's Ministry of Economic Development said last week that authorities are considering "removing restrictions on the use of intellectual property contained in certain goods whose supply to Russia is restricted," according to Russian state news outlet Tass, and that potential measures could affect inventions, computer programs and trademarks." This could allow Russian oligarchs to take over the local McDonald's franchises and simply open the restaurants under the company's trademarks with no payments to McDonald's and no risk of legal IP enforcement. It may also permit Russian companies to run bootleg copies of U.S. and European software and sell them in packaging and under names owned by the Western companies. We don't know how long these decrees will last – they may be the beginning of a new normal, where Russia simply flaunts international IP laws without recourse.

The Russian unprovoked attack on Ukraine and the Western opposition to it are creating indirect consequences for U.S. business technology. Given inflamed conflicts, Putin is likely to direct his electronic hacker army to target U.S. and European critical infrastructure and other important companies/institutions. We can probably thank this prospect for a federal data security reporting bill being fast-tracked by Congress, soon to be the first broad non-sector-specific federal incident reporting requirement enacted into law.

Last week both houses of Congress passed the Consolidated Appropriations Act, which should be executed by President Biden by the time this column is published. This huge government spending package not only funds the government for the next year, but it includes the Cyber Incident Reporting for Critical Infrastructure Act, mandating that certain companies across industries must report significant cyber incidents and ransomware attacks to the Cybersecurity and Infrastructure Security Agency (CISA) in the Homeland Security Department. We will not know which companies are affected by the new reporting requirements or what kind of cyber-attack will need to be reported for more than a year, when the CISA Director issues rules which include these definitions.

Financial institutions are subject to some cyber incident reporting requirements, but other critical businesses like energy, telecommunications and healthcare may not be required to report as long as personal data was not affected by the attack. CISA Director Jen Easterly issued a statement saying, "Put plainly, this legislation is a game-changer. Today marks a critical step forward in the collective cybersecurity of our nation," and that "CISA will use these reports from our private sector partners to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure. This information will fill critical information gaps and allow us to rapidly deploy

resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims.” Recent statements from the Biden Administration have encouraged companies to report cyberattacks, but this new legislation will create an environment of required reporting that could spread to other US industry.

Russia’s invasion of Ukraine has changed the world. Western technology and intellectual property will be affected in ways we never conceived, and will live with those changes indefinitely.

National Law Review, Volume XII, Number 74