Foreign Policy Through Code

Joel Todoroff

Between 2010 and 2012, the Arab Spring swept the Middle East and North Africa. People mobilized, often through cell phones and social media, to protest and demand government change.[1] Governments pushed back. Egypt, Libya, and Syria cut off internet access to their populations.[2] Tunisia wrote malware to steal social media passwords and delete Facebook accounts belonging to organizers and protestors.[3] Less than a decade later, mass protests broke out in Hong Kong, and again technology enabled mass mobilization. There, afraid of the Chinese government cutting off internet access or monitoring protests via the telecommunications network, protestors used Bluetooth to create local ad hoc networks to organize and pass information.[4] The fear was not unfounded: China censors internet traffic and uses technology as a tool of domestic repression.[5]

In February 2022, Russia invaded Ukraine. In the leadup to the attack, Microsoft quickly detected Russian malware designed to wipe Ukrainian government systems, notified the Ukrainian government, and released information to help identify and mitigate the malware.[6] It also took steps to limit Russian online propaganda.[7] At the same time, Google pushed updates to help refugees, provide civilians with air raid alerts, and disabled Google Maps features that Russia could have used to track Ukrainian forces.[8]

These examples illustrate that technology, often controlled by private companies, increasingly enables or constrains political activities. Protestors and activists use technology to organize; authoritarian regimes use it to censor, to identify dissidents, or even to track ethnic minorities.[9] But the behavior of both individuals and governments is shaped by the capabilities or constraints of technology itself. Government officials can easily censor a message transmitted between two parties if they can read it, but have a much harder time if the message is encrypted. If the technical functionality exists, people's phones can alert them of incoming missiles or air raids, otherwise a government will rely on sirens or other tools.

The Russian invasion stands out due to the open and concerted efforts companies made to support Ukraine. This response was both unique and admirable—but it was not, in general, a hard business decision. Russia was put under international sanctions, serious thinkers agreed that the invasion was unprovoked and unjustified, and many companies had limited business interests in Russia to begin with. There was little downside risk to siding with Ukraine. But it is not clear how industry would respond without this alignment of interests. What if a company did extensive business with the invading country? Or if the legitimacy of the invasion were in serious dispute?

What if there were a mechanism to link technological enabling or constraining functions to the pursuit of foreign policy or human rights, even without such a unique convergence of interests? Google, for example, could have phones delete location information associated with political protests, similar to a recent policy change regarding location data for individuals visiting reproductive care facilities.[10] Messaging applications could have built-in functionality to use Bluetooth or other protocols that can sidestep government monitoring capabilities or internet shutdowns. Operating systems or browsers could come with tools that ease secure and anonymous internet browsing that can avoid filtering and censorship.

Scholars have noted that the ability to act online is determined in part by code itself: an Apple user with a .me email address can send an email to a Gmail account, but they cannot send an iMessage to Google Chat or Whatsapp.

This is not because of a law, regulation, or sanction, but because the code behind email lets users from .me and .gmail communicate directly with one another, whereas the code behind iMessage does not—users must use another medium, such as SMS (text messages). But technical architecture—code—can and does change in ways that impact politics.

Other countries have recognized this. China's push for facial recognition systems designed to identify ethnic minorities comes to mind.[11] Similarly, Russia introduced draft legislation to ban protocols that hide the destination of internet traffic, something that could interfere with the System for Operative Investigative Activities (SORM), the censorship and surveillance system they compel telecom companies to install.[12]

Government activity in this space need not be limited to authoritarian regimes. Liberal democracies should develop formal mechanisms to play a role in these changes, engaging with private industry to further foreign policy aims, not through a traditional exercise of state power, but through the private sector creation or modification of technical architecture. Moreover, there should be mechanisms to incentivize—though not compel—this engagement. This could come in any number of forms, from indemnifying the company against potential market loss to providing access to capital at preferential rates.

The logic is simple: there is a limited universe of tools that liberal democracies can use to shape foreign domestic affairs. Existing tools include sanctions and providing, or withholding, foreign aid. But what preexisting tool of statecraft will limit the effectiveness of a foreign law enforcement officer to identify protestors? Or give an oppressed minority the ability to evade censors and tell the world about atrocities being committed against them? In at least some instances, changes in technology platforms will enable or constrain activity in foreign countries more directly than the alternatives, and without taking aggressive or escalatory steps. Moreover, depending on the platform or code in question, it may be possible to implement changes incredibly quickly. Of course, working with a private company to effectuate technical changes will not always be viable or desirable, but in some instances a formal mechanism to do so—and incentivize cooperation—could be uniquely valuable, both for its effects and for its speed.

The proposal undoubtedly comes with risks. If companies are seen as tools of Western foreign policy, they could be barred from doing business in both autocratic regimes and developing democracies that fear Western influence. In particularly volatile situations, companies, or their assets, may even be subject to more direct retaliation. For example, Russia declared that U.S. commercial satellites may be a legitimate target for military strikes given that they aid the Ukrainian war effort.[13] It is not implausible that, even outside of armed conflict, a company that changes its platform to interfere with a foreign government's activities will be subjected to cyberattacks or other direct retaliatory measures.

These are real, and compelling, concerns. Decisions by the government to work with the private sector in this way should not be taken lightly, and there should be a process to ensure not only the legitimacy of the aims, but also to assess the potential blowback on private industry. But it would be a mistake not to take account of the role and power of private industry in affecting foreign policy. And fears of a backlash are likely overstated—authoritarian regimes already believe Western businesses are suspect. In fact, a clear articulation of the mechanisms by which governments will work with, and incentivize, private industry may help show a delineation between industry and government. As Western businesses engage abroad, such a partnership could be directly contrasted with practice and legal regimes in places like Russia and China where it is clear that the government exploits industry to further authoritarian aims.[14]

Moreover, it would be a mistake to assume companies will not unilaterally engage in behaviors impacting foreign affairs—private industry choices have broad ramifications. The private sector response to the Russian invasion of Ukraine is one example of this. Another is the messaging application Signal's introduction of code that claims to hinder the operation of an investigative tool (Cellebrite) used by law enforcement entities around the world.[15] So too are Apple's and Tesla's decisions to open data centers in China.[16] Realistically, companies have no choice but to take actions that enable or constrain government activities—the private sector is at the center of everything from the movement of data across the internet[17] to critical infrastructure.[18] It is hard to imagine private industry decisions in such spaces *not* having an impact on governments.

These are not all exact analogies: some are policies, not examples of code enabling or constraining. But they speak to the larger point that private companies can directly influence what was once understood as a domain owned by

nation-states: foreign policy and foreign affairs. Their policy and code can enable or constrain foreign governments. Their platforms can facilitate democratic values or, in some cases, enable repression. And companies already realize this. They are making decisions that intersect with government policy interests. But we lack established mechanisms to guide and incentivize these behaviors.

In the late 1990s, Lawrence Lessig explained that, on the internet, technical architecture is law. Today, it is clear that it is much more: it is also foreign policy. And we're late to the game. Authoritarian regimes are already working to make technology platforms further their policy aims. Businesses have recognized their role. But the West has yet to articulate a framework for using private sector platforms as a mechanism to further liberal democratic values. It can, and should, do so.

Disclaimer: This article was written in the author's personal capacity. Opinions expressed in the article are the author's own and do not necessarily represent the views of the United States government.

Joel Todoroff is Special Counsel at the Office of the National Cyber Director.

[1] "Arab Spring anniversary: When Egypt Cut the Internet," Al Jazeera, January 25, 2016, https://www.aljazeera.com/features/2016/1/25/arab-spring-anniversary-when-egypt-cut-the-internet; Deji Olukotun and Peter Micek, "Five Years Later: The Internet Shutdown That Rocked Egypt," Access Now, January 21, 2016, https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/.

[2] "Internet Censorship in the Arab Spring," Wikipedia, https://en.wikipedia.org/wiki/Internet_censorship_in_the_Arab_Spring.

[3] Peter Beaumont, "The Truth About Twitter, Facebook and the Uprisings in the Arab World," The Guardian, February 25, 2011, https://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings-arab-libya.

[4] Jane Wakefield, "Hong Kong Protesters Using Bluetooth Bridgefy App," BBC, September 3, 2019, https://www.bbc.com/news/technology-49565587.

[5] "Freedom on the Net 2021: China," Freedom House, 2021, https://freedomhouse.org/country/china/freedom-net/2021.

[6] Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

[7] Brad Smith, "Digital Technology and the War in Ukraine," Microsoft, February 28, 2022, https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/.

[8] Kent Walker, "Helping Ukraine," Google, March 4, 2022, https://blog.google/inside-google/company-announcements/helping-ukraine/; Gavin Butler, "Google Turns Off Maps Features in Ukraine That Inadvertently Showed Russia's Invasion," Vice News, February 27, 2022, https://www.vice.com/en/article/5dgjka/google-maps-ukraine-live-traffic-russia-invasion.

[9] Drew Harwell and Eva Dou, "Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says," *The Washington Post,* December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/.

[10] Nico Grant, "Google Says It Will Delete Location Data When Users Visit Abortion Clinics," *The New York Times,* July 1, 2022, https://www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html

[11] Drew Harwell and Eva Dou, "Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says," *The Washington Post,* December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/.

[12] Adam Satariano, Paul Mozur, and Aaron Krolik, "When Nokia Pulled Out of Russia, a Vast Surveillance System Remained," *The New York Times,* March 28, 2022, https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html; Catalin Cimpanu, "Russia Wants to Ban the Use of Secure Protocols Such as TLS 1.3, DoH, DoT, ESNI," ZDNET, September 22, 2020, https://www.zdnet.com/article/russia-wants-to-ban-the-use-of-secure-protocols-such-as-tls-1-3-doh-dot-esni/.

[13] "Russia Warns West: We Can Target Your Commercial Satellites," Reuters, October 27, 2022, https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27/.

[14] E.g. Christopher Bing, "U.S. Warned Firms About Russia's Kaspersky Software Day After Invasion -Sources," Reuters, March 31, 2022, https://www.reuters.com/technology/exclusive-us-warned-firms-about-russias-kaspersky-software-day-after-invasion-2022-03-31/.

[15] "Exploiting Vulnerabilities in Cellebrite UFED and Physical Analyzer from an App's Perspective," Signal, April 21, 2021, https://signal.org/blog/cellebrite-vulnerabilities/; Dan Goodin, "In Epic Hack, Signal Developer Turns the Tables on Forensics Firm Cellebrite," Arstechnica, April 21, 2021, https://arstechnica.com/information-technology/2021/04/in-epic-hack-signal-developer-turns-the-tables-on-forensics-firm-cellebrite/.

[16] Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China," *The New York Times,* May 17, 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html; "Tesla Opens New China Research, Data Centers; Will Store Data Locally," Reuters, October 25, 2021, https://www.reuters.com/business/autos-transportation/tesla-opens-new-china-research-data-centers-will-store-data-locally-2021-10-25/.

[17] Tim Greene, "What Is the Internet Backbone and How It Works," Network World, March 12, 2020, https://www.networkworld.com/article/3532318/what-is-the-internet-backbone-and-how-it-works.html.

[18] "Critical Infrastructure," Federal Emergency Management Agency, June 2011 https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.