The Transatlantic Data War

Europe Fights Back Against the NSA

Henry Farrell and Abraham Newman

Last October, the European Court of Justice struck down the Safe Harbor agreement, a 15-year-old transatlantic arrangement that permitted U.S. companies to transfer data, such as people's Google-search histories, outside the EU. In invalidating the agreement, the ECJ found that the blurry relationship between private-sector data collection and national security in the United States violates the privacy rights of EU citizens whose data travel overseas. The decision leaves U.S. technology companies with extensive international operations on shaky legal ground.

Although some informed American observers anticipated the decision, most were caught flat-footed; some seemed downright bewildered. Myron Brilliant, the executive vice president of the U.S. Chamber of Commerce, said, "It is particularly alarming that this long-standing agreement has been invalidated with no discussion of a transition period or guidance regarding how companies should comply with the law." Critics of the decision, including U.S. Commerce Secretary Penny Pritzker, argue that it will jeopardize the transatlantic digital economy, costing U.S. firms billions of dollars. Without a new agreement, there is a significant risk that personal data will have to be quarantined within Europe, creating what Eric Schmidt, the executive chair of Alphabet (previously Google), called "per-country Internets." If that occurred, he continued, it could risk destroying "one of the greatest achievements of humanity." Critics also charge that the EU is acting unilaterally

HENRY FARRELL is Associate Professor of Political Science and International Affairs at George Washington University's Elliott School of International Affairs. Follow him on Twitter @henryfarrell.

ABRAHAM NEWMAN is an Associate Professor in the Edmund A. Walsh School of Foreign Service and the Government Department at Georgetown University.

to protect its businesses against foreign competition, damaging the open, democratic nature of the Internet.

But the main reason that U.S. companies and officials are flustered is that they are used to being the ones who make the rules. Over the past 70 years, the United States has built a global system in which information, investment, and trade move quickly and easily across borders. That openness has created an interdependent world in which the national rules and preferences of one country can shape the rules and preferences of others. The outsized power of the U.S. economy usually gives that role to the United States.

In the aftermath of the 9/11 attacks, the United States began to exploit interdependence, deliberately using its economic power as an instrument of national security. Despite advocating the free flow of capital, it has systematically used sanctions to obligate foreign banks and financial actors to isolate businesses, people, and states from the global financial system. Despite publicly promoting an open and secure Internet, it has privately undermined the encryption of online communications and surreptitiously created vast international surveillance systems in cooperation with close allies, including the United Kingdom. In short, the United States has leveraged the world's reliance on its economy to influence and spy on foreigners.

This strategy is reaching its limits, and the Safe Harbor decision powerfully demonstrates that Washington needs to wake up to the strategy's costs. When the United States uses its global economic heft to bolster its national security, it rigs the game, making it nearly impossible for other states to push back and inspiring ill will abroad. It is difficult for EU countries to fight back directly, both because of the sheer might of the U.S. security apparatus and because EU member states free-ride on U.S. intelligence, military, and technological capabilities. Yet the EU may have found a way to force the United States to pay a price for its dominance. Although the ECJ has no jurisdiction over the U.S. National Security Agency (NSA), it does have jurisdiction over the European operations of American firms. Its ruling demonstrates that the more Washington tries to leverage the interdependence of the global system for its own security goals, the more other states and their courts will actively resist a U.S.-centered global economy.

WEAPONIZING INTERDEPENDENCE

One of the great luxuries of hegemony is the ability to take the world for granted. U.S.-led globalization has removed barriers to the free flow of money, goods, and information. Removing these barriers has come with political costs, but these have been borne primarily by other states, which have been obliged to adjust their domestic rules so that they may benefit from the open, integrated world economy.

A more integrated world economy benefits U.S. companies, allowing them to find new markets and build complex international supply chains that lower their costs. Businesses such as Facebook, Google, and Uber have exploited economic openness to replicate their business models throughout the advanced industrialized world, often deliberately challenging local and national rules in other countries. At the same time, the explosion of cross-border exchange has increased the importance of the U.S. dollar and the U.S. market as foreign firms seek access to American banks and consumers to raise money and sell goods.

In the past decade and a half, Washington has increasingly wielded this power as a weapon, shaping the decisions of foreign governments and firms that depend on access to the United States' currency, information sector, and markets. Rather than spread U.S. norms and preferences through indirect market mechanisms, the United States has directly harnessed the coercive might of its markets and information networks to achieve its own security and foreign policy goals—most notably combating transnational terrorism and confronting rogue states.

Great powers have regularly used blockades, export restrictions, and sanctions to manipulate countries that depend on trade in physical goods. But the United States now has the power to manipulate financial and informational flows as well. Foreign financial institutions are crucially dependent on U.S.-dollar-based transactions, making them vulnerable to U.S. regulators, who can threaten them with dire consequences if they do not comply with U.S. rules. In an effort dubbed "Treasury's War" by one of its chief architects, Juan Zarate, who served during the George W. Bush administration as assistant secretary of the U.S. Treasury for terrorist financing and financial crimes, the United States has pressed foreign financial institutions into service as agents of Washington. Under Section 311 of the U.S.A. Patriot Act, the U.S. Treasury Department has the ability to classify a foreign financial

institution as a "primary money laundering concern." This classification can affect a bank's ability to operate in the United States and allows Washington to pressure other financial institutions affiliated with it that rely on U.S. markets.

Some of the United States' targets, among them Iran and North Korea, have few sympathizers. But the United States has also undercut its friends. In the service of counterterrorism, for example, it forced a Belgium-based financial-processing entity to provide it with a trove of information on worldwide electronic fund transfers, systematically breaking EU privacy law. It has also exploited global interdependence to push foreign governments to change their domestic rules and practices on issues seemingly unrelated to security, such as bank secrecy, foreign bribery, and money laundering. Swiss banks, which have long made it their business model to help the world's wealthy avoid paying taxes, now find themselves in the cross hairs of U.S. national security policy. As U.S. officials have woken up to the importance of the financial flows that fund terrorist networks, they have begun to target illicit banking practices.

THE END OF THE LINE

Too often, policymakers in Washington mistakenly assume that the narrow self-interests of the United States and its businesses should automatically go hand in hand with the global order they have helped create. When foreign regulators have sought to apply national rules to U.S. technology companies, the United States has accused them of having ulterior motives. U.S. President Barack Obama, for example, has interpreted foreign governments' efforts to protect their citizens' rights against U.S. companies as protectionism in disguise. Speaking in a February 2015 interview about European investigations into Facebook and Google, he said, "Our companies have created [the Internet], expanded it, perfected it in ways they [Europeans] can't compete [with]. And oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests."

Such claims are both wrong and politically unsustainable; soon enough, major states and jurisdictions will stop tolerating U.S. coercion. When the United States targets states or individuals that are perceived as breaking the rules, such as Iran or Russia, it can usually persuade enough other states to join in, giving its actions

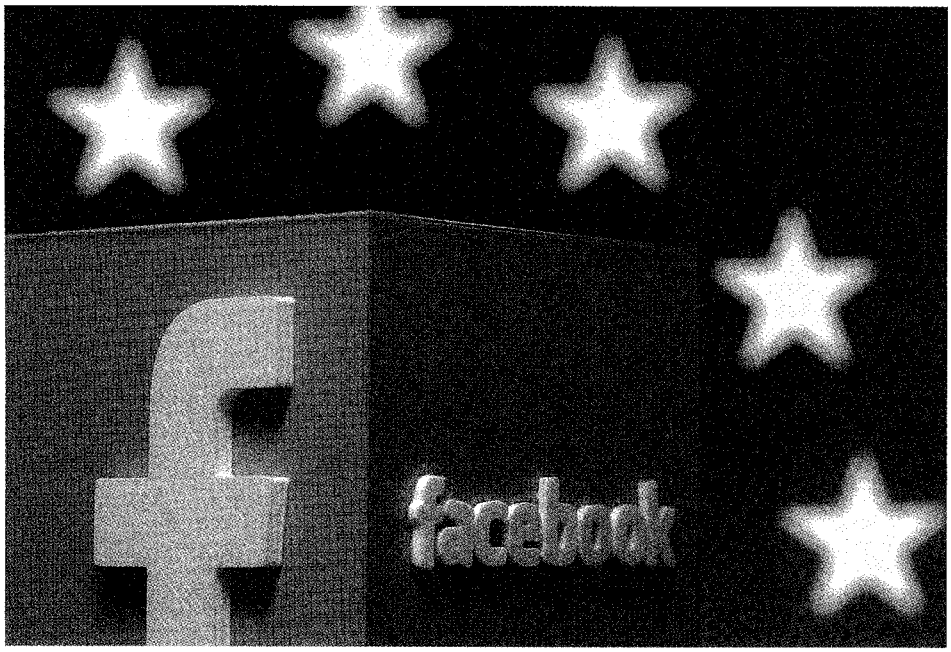
a veneer of legitimacy. But when the United States breaks the rules itself in ways that undermine the basic constitutional guidelines of other countries, it should expect a backlash. The more the United States seeks to exploit the system it has created, the more foreign states and businesses will challenge it.

Interdependence has already begun to work against the United States rather than for it. As U.S. businesses have entered international markets, they have become more vulnerable to other countries' rules and more anxious about U.S. policies and actions that irritate other governments. This is an especially big problem for technology companies, whose insatiable hunger for detailed personal information indirectly feeds the U.S. surveillance state. Since foreign countries cannot directly indict the NSA, they tend to turn to the targets whose behavior they can affect—U.S. businesses—to force the U.S. government to change its rules.

FOR EU EYES ONLY

Thanks to the revelations of the American privacy activist and former NSA contractor Edward Snowden, resentment toward the U.S. security state has grown into active opposition. Snowden's files showed that the United States, together with key allies, had systematically exploited technical vulnerabilities to spy on the world, gathering vast amounts of data on the personal communications of hundreds of millions of people and combing them for relevant security information. This meant that even as Washington had spent years advocating an open Internet and condemning digital surveillance by countries ranging from China to Russia, it had simultaneously been exploiting the open Internet on the sly. The United States had publicly proselytized for the free flow of information while secretly diverting these flows into NSA server farms. It had vigorously supported the global expansion of technology companies, championing the use of Twitter, for example, in pro-democratic movements such as those of the Arab Spring, while quietly requiring some of those firms to turn over troves of data and tapping into their servers overseas.

Of course, the United States is not alone in its cynicism. Some politicians who have publicly expressed fury at the Snowden revelations, including German Interior Minister Thomas de Maizière, have hypocritically tried to impose similar surveillance schemes on their countries' own civilians, and foreign intelligence agencies that depend



Unfriended: a 3-D-printed Facebook logo in Zenica, Bosnia and Herzegovina, May 2015

REUTERS / DADO RUVIC

on the CIA have minimized the scandal for fear of being cut off from U.S. intelligence-sharing programs. However, as U.S. actions have interfered with the basic rights of citizens abroad, they have drawn the ire of a different set of actors who are less easily cowed than politicians: judges, who often see their role as protecting fundamental constitutional protections rather than striking international compromises. The ECJ has already struck down a measure requiring European communications firms to keep customer data for up to two years, in part because it feared that this information might leave the EU. Now the court has gone one step further, challenging the basis of the transfer of personal information from the EU to the United States.

The Safe Harbor dispute stems from the fact that the EU and the United States have fundamentally different understandings of how privacy should work in the digital age. Beginning in the 1990s, European countries developed comprehensive rules governing the collection and processing of personal information, overseen by independent regulatory agencies called "data protection authorities." This approach to privacy was elevated to a fundamental constitutional right when the EU adopted its Charter of Fundamental Rights in 2009. The United States, in contrast, lacks a comprehensive approach to privacy, relying instead on an idiosyncratic patchwork of specific—and, in some cases, dated—rules governing sectors as diverse as health

care and video rentals. The problem for the United States is that European regulations have long prohibited the transfer of data to countries that the EU considers to have weak privacy protections, among them the United States.

Given the economic benefits of data exchange, the EU and the United States negotiated the Safe Harbor agreement in 2000 to work through these differences. As part of the arrangement, U.S. firms agreed to comply with a set of basic privacy principles overseen and enforced by the U.S. Federal Trade Commission. In the past 15 years, more than 4,000 U.S. firms have come to rely on Safe Harbor to facilitate transatlantic e-commerce and to transfer data across jurisdictions. The ECJ's ruling jeopardizes all of that.

In the wake of the Snowden revelations, privacy activists in Europe began exploring legal channels to curtail U.S. surveillance. In 2013, Max Schrems, an Austrian law student, brought a case in Ireland against the Safe Harbor agreement based on information revealed in the Snowden files. He argued that the NSA's spying showed that there was no effective data protection regime in the United States and that the Safe Harbor agreement could not protect European citizens from mass surveillance. Ireland's High Court appeared to agree, finding that "the Snowden revelations demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens. Their data protection rights have been seriously compromised by mass and largely unsupervised surveillance programmes." The ECJ, in its ruling, cited the Irish High Court's findings on the Snowden documents and directly tied the fate of the Safe Harbor program to the blurring of private-sector data collection and public surveillance in the United States, concluding that

By transforming technology companies into tools of national intelligence, Washington has damaged their reputations.

> national security, public interest, and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements. The United States safe harbour scheme thus enables

interference, by United States public authorities, with the fundamental rights of persons.

NO SILVER LINING

By transforming U.S. technology companies into tools of national intelligence, Washington has badly damaged their corporate reputations and exposed them to foreign sanctions. Their international profits—not to mention a substantial chunk of the U.S. economy—depend on the free flow of information across borders. Foreign officials, political activists, and judges who limit these flows to protect their citizens from U.S. surveillance strike at the heart of these companies' business models. The ECJ's Safe Harbor ruling has now forced Washington to decide whether it values its unrestricted ability to spy on Europeans more than an open Internet and the economic well-being of powerful U.S. businesses. The EU has, in effect, used the United States' own tactics against it.

Meanwhile, U.S. firms have few attractive long-term options if they want to transfer data across the Atlantic. In the short term, EU rules still allow businesses to use contracts, for example, to transfer personal data to the United States. But such transfers are no better protected against U.S. state surveillance than Safe Harbor transfers were. Hamburg's data commissioner has bluntly advised firms not to rely on these mechanisms and instead to simply keep their data on European servers.

European data protection authorities have given Washington a few months' reprieve to shape up but have threatened to take action if the United States has not reformed its privacy rules by the end of January 2016. They are demanding that the EU and the United States agree on a binding legal arrangement, such as a treaty, that guarantees European privacy rights by keeping data from U.S. intelligence agencies. If the United States does not amend its laws to protect Europeans, U.S. firms will likely need to Balkanize their data flows by quarantining European data in European data centers; otherwise, they will face sanctions from European data protection authorities. Microsoft's president, Brad Smith, warns that such fragmentation of the Internet risks a "digital dark ages" that could disrupt everything from credit-card payment systems to airline reservations, costing companies billions of dollars and threatening their global ambitions. U.S. efforts to exploit interdependence will

have led Europe to cut valuable personal data out of global networks and markets.

A NEW WORLD ORDER

By its very nature, interdependence can be a weakness as well as a weapon. As the Safe Harbor case illustrates, when the security preferences of the United States are at odds with the fundamental rights of citizens in other major jurisdictions, it is likely to face backlash. The United States needs global cooperation on a host of sensitive issues, ranging from money laundering and sanctions to the multilateral exchange of data. Yet it continues to insist on unilateralism, even when this damages the ability of U.S. firms to operate across jurisdictions.

In the context of a criminal investigation, for example, the United States is now demanding that Microsoft hand over personal data housed in its data center in Ireland. Rather than requesting the data through the ordinary processes of intergovernmental exchange, in which the U.S. government would make a request to law enforcement officials in Ireland, the United States is using the global reach of its legal system to demand the data even in the face of opposition from both the Irish government and Silicon Valley companies that fear this move will further blacken their corporate reputations. A group of powerful technology giants, including Apple and Cisco Systems, has filed a "friends of the court" brief in support of Microsoft and against the U.S. government's position. If this type of behavior on the part of the U.S. government continues, it will critically damage the aspirations of U.S. firms to build global cloud computing. Instead of a common cloud, firms will have to make use of segmented national data spaces hidden behind thickets of regulations and mutually incompatible cryptographic protection schemes. This will both threaten cloud providers' economies of scale and hurt U.S. providers that are seen, rightly or not, as more vulnerable to U.S. surveillance and the government's demands for information.

But such an outcome can still be avoided. The EU and the United States share broadly similar values and have figured out how to cooperate on the exchange of law enforcement data. They have reached the so-called Umbrella Agreement, under which the United States has committed to introducing laws that will give the citizens of EU states certain privacy rights in U.S. courts. The United States could likely resolve the Safe Harbor controversy by extending such protections to

cover surveillance and eliminating loopholes that allow both American and European intelligence agencies to exchange information without democratic oversight. Disputes such as the Microsoft case could be resolved through a more efficient system of multilateral exchange, with accompanying privacy protections. Many of the problems of interdependence could be solved by making civil rights interdependent as well, so that they are recognized and protected across multiple jurisdictions.

The United States faces a profound choice. It can continue to work in a world of blurred lines and unilateral demands, making no concessions on surveillance and denouncing privacy rights as protectionism in disguise. Yet if it does so, it is U.S. companies that will suffer.

Alternatively, it can recognize that globalization comes in different flavors and that Europeans have real and legitimate problems with ubiquitous U.S. surveillance and unilateralism. An ambitious strategy would seek to reform EU and U.S. privacy rules so as to put in place a comprehensive institutional infrastructure that could protect the privacy rights of European and U.S. citizens alike, creating rules and institutions to restrict general surveillance to uses that are genuinely in the security interests of all the countries.

More broadly, the United States needs to disentangle the power of a U.S.-led order from the temptations of manipulating that order to its national security advantage. If it wants globalization to continue working as it has in the past, the United States is going to have to stop thinking of flows of goods and information as weapons and start seeing them as public goods that need to be maintained and nurtured. Ultimately, it is U.S. firms and the American economy that stand to benefit most.