
US Extraterritoriality: The Trump Card

EXPLAINER - DECEMBER 2024




Institut Montaigne is a leading independent think tank based in Paris. Our research and ideas aim to help governments, industry and societies to adapt to our complex world. Institut Montaigne's publications and events focus on major economic, societal, technological, environmental and geopolitical changes. We aim to serve the public interest through instructive analysis on French and European public policies and by providing an open and safe space for rigorous policy debates.

EXPLAINER - December 2024

US Extraterritoriality: The Trump Card



Institut Montaigne's Explainers are analytical short-reads, setting out key facts and figures to make sense of the world we live in and how it is evolving.



Explainer

To understand the world in which we operate

Issue Paper

To break down the key challenges facing societies

Policy Paper

To provide practical recommendations

Exclusive Insights

Unique data-driven analyses and practical scenario exercises

Report

Deep-dive analyses and long-term policy solutions

The new European Commission has made economic security a priority for its 2024-2029 agenda. It has promised to make the EU more competitive and protect its single market from distortion, technology theft and coercion. The EU has already adopted new instruments to reduce its supply chain vulnerabilities and is rethinking its industrial policy. However, its strategy has one key blind spot: the EU lacks a clear policy on extraterritoriality, not least on how to respond to coercive unilateral sanctions. This is shortsighted and could damage the EU's long-term economic and political interests.

US EXTRATERRITORIALITY: A FUTURE TRUMP CARD?

Extraterritoriality is a key tool to promote and defend US interests. Extraterritoriality – understood as the application of national laws abroad – is not a new phenomenon, but it is gaining traction. In a world characterized by strategic competition, mass subsidies, de-risking and weak multilateral organizations, countries are looking for new ways to safeguard their political and economic interests. Many are turning to law to achieve this. None more than the United States.

US extraterritoriality can target almost any individual, entity or company in the world. It can take many forms: primary sanctions to weaken hostile countries and criminal or terrorist organizations; secondary sanctions to target individuals, entities or companies whose activities threaten US national security interests; privacy, data-protection and intelligence-gathering laws; as well as regulations designed to limit market access and exports of sensitive dual-use technologies to hostile countries.

It is very difficult for European governments to ignore, let alone stop, US extraterritorial norms from applying. Companies that fail to

comply with US rules risk huge fines, handover of sensitive data, exclusion from the US market and its financial system and possibly prison time for their directors. The risk of exclusion is such a forceful deterrent that European companies prefer to comply with US rules, rather than abide by European measures designed to block their application.

There are good, bad and ugly uses of US extraterritoriality. The US has a very broad definition of national security, which it has used to justify its use of extraterritorial norms. Stated aims include: protecting the US' vital security interests when treaties and international organizations fail to; upholding and defending human rights, international law and global competition rules; preventing excessive risk-taking by companies; and curbing the threat posed by hostile countries, money-laundering networks and criminal organizations. In many cases, these goals align with European interests. However, the US has also been accused of using extraterritoriality as a way to secure market dominance and for industrial espionage and intellectual property theft.

Extraterritoriality has become a key tool to manage US-China systemic rivalry. Export controls are central to US strategy to hinder China's efforts to achieve greater technological self-reliance, particularly in sensitive and critical technologies. They target US firms exporting to China, but also European firms that are found to use software, components or processes from the United States. In response, China has also adopted its own set of export controls, which could soon apply to European companies doing business in, and with, China.

President-elect Trump has a love-hate relationship with extraterritoriality. During his first term, President Trump tightened export controls and expanded laws to punish those committing human rights abuses. At the same time, he rolled back banking regulations set up in the aftermath of the 2008 financial crisis. He has also criticized other extraterritorial measures, like the US' anti-corruption laws, arguing that they created unnecessary red tape and dissuaded foreign companies from working

with US firms. During the 2024 campaign, he warned that he would remove any sanctions that threatened the dollar's dominance in international financial transactions.

It is not clear whether a Trump 2 Administration would use extraterritoriality as a coercive tool – making it the perfect Trump card. President Trump is expected to be much tougher on export controls and have a tailored approach to sanctions. He has called “tariffs” “the most beautiful word in the dictionary”, and he is likely to rely more on tariffs than on other measures to attain US strategic goals. The real uncertainty is whether he would use extraterritoriality – or the threat of it – as a coercive tool to pressure the EU into reversing laws he does not like, such as the EU's General Data Protection Regulation (GDPR) or digital market rules, which affect the way US companies operate in Europe.

A MIXED BAG FOR EUROPE

US extraterritoriality has a mixed reputation in Europe. There are many reasons why US extraterritoriality is necessary. It has reduced global cases of corruption worldwide and has minimized risk-taking by banks since the 2008 financial crisis. It ensures that European companies do not support criminal activities and allows the US to sanction foreign governments accused of breaching international law (such as Russia and Syria).

US extraterritoriality becomes a problem when the interests of the US and EU do not align. For example, the US and the EU disagree on how to use European data stored on US servers. They sometimes apply different sanctions against third countries, in the case of Iran or Cuba for example. Since 2018, there has been a recorded €18.8 billion in direct losses for EU companies accused of non-compliance with US laws. Litigation processes have sometimes resulted in handover of commercial

data and industrial plans, as well as take-over of US-based activities by US competitors.

Navigating US laws is extremely complex. With many extraterritorial provisions in existence, a company's chances of breaking the law, even inadvertently, are high. To avoid penalties, European companies need to understand what their products are made of, where they are fabricated, and whom they are sold to and shared with. They also need to know how complying with US laws can conflict with EU and other third-country measures. European companies are increasingly caught in the crossfire of competing sanctions regimes.

The current Republican majority is good and bad news for European companies abiding by US laws. Both Republicans and Democrats embrace extraterritoriality – but disagree on the role that executive agencies should play. The recent Supreme Court's decision to overturn the 40-year-old Chevron precedent makes it clear that it is the courts, not executive agencies, that must clarify the application of US laws when Congress has failed to provide adequate guidance. This is good news for European companies looking to challenge the application and enforcement of US extraterritorial norms in court. However, it also creates greater regulatory uncertainty as action taken by executive agencies on tackling climate change or advancing clean technology, for example, could also be challenged in court.

The EU has been reluctant to challenge the US over its use of extraterritoriality. The current geopolitical context means that (most) member states have been reluctant to discuss extraterritoriality or take any measures that could be seen to weaken, or undermine, the transatlantic relationship – or give the US cause to rethink its security guarantees to Europe. It has also been reluctant to adopt a more offensive approach on extraterritoriality fearing that it would be accused of hypocrisy after years of castigating the US for its offensive uses.

The US prefers to bypass the European Union and discuss extraterritoriality with individual member states instead. This is especially the case for export controls of critical technologies to China. The US knows that it cannot prevent China from gaining technological supremacy alone and is putting pressure on the EU to follow its lead. Rather than deal with the EU, it has preferred to exert pressure directly on individual member states like it did when it got Japan and the Netherlands to agree to restrict exports of advanced chip-manufacturing equipment to China in January 2023. Yet, action taken by one member state can have consequences for the whole of the European Union. Since 2023, Beijing has been retaliating by limiting exports to the EU of gallium, germanium, graphite and several compounds used to make semiconductors.

TRUMP-PROOFING THE EU'S OFFER

The EU should engage in discussions with the Trump Administration on extraterritoriality, beginning with the US laws that President Trump himself has criticized. President Trump has been critical of several extraterritorial measures, such as the Foreign Corrupt Practices Act or the Foreign Intelligence Surveillance Act, both of which have historically posed challenges for the EU.

The EU needs to show why it is in the US's interest to coordinate sanctions. There are several reasons for this: first, to limit exports of strategic technologies to China; second, to slow down attempts to circumvent Western laws. Trade flows between Moscow, Beijing and Tehran have intensified in recent years, making it easier for their companies to ignore Western regulations. While financial transactions in dollars far outweigh those in other currencies, China has also been thinking of ways to internationalize the renminbi.

The EU should be clear-eyed about the possibility that dialogue may not yield results and be ready to make bargains. The Trump 2 Administration will be transactional. If the EU wants to lower the chances of coercive US laws, then it needs to be ready to offer something in return, for example more imports of gas and LNG. President Trump has said he wants to reduce the trade deficit the US has with the EU, making it a good starting point for bargaining.

The EU should develop an approach to extraterritoriality that is both defensive and offensive. Not all US extraterritorial norms are bad. But some do pose a challenge to the sovereignty of the EU and its member states. What's more, the EU's defensive measures, like the Blocking Statute, have been largely ineffective in shielding companies from US extraterritorial rules. The EU needs to shift its mindset on extraterritoriality and recognize, like it did in 2021, that it can be used as a coercive tool.

EU countries should let the European Commission take the lead in coordinating and devising an offensive strategy. It is not clear that the EU has the legal competence, or political support from member states, to develop a new strategy on extraterritoriality. It would make sense for the European Commission to take the lead, in close coordination with the Council of the EU. EU coordination is particularly important to thwart US attempts to divide member states and to prevent the fragmentation of the single market if individual member states adopt their own defensive measures. For that, the EU Commission will need to reassure EU governments and European companies that it can store, protect and keep any information confidential.

Executive Summary	5
--------------------------------	---

Introduction	14
---------------------------	----

1	The US Congress is mostly responsible for determining when extraterritoriality applies	18
----------	---	----

Box 1: The American obsession with the law and extraterritoriality	22
---	----

2	A closer look at US extraterritorial laws	23
----------	--	----

Table 1: Federal laws with extraterritorial reach	23
--	----

2.1. Sanctions to protect national security and counter terrorism	24
--	----

Box 2: Enforcing sanctions	28
---	----

2.2. Export controls	31
-----------------------------------	----

Box 3: Is ITAR undermining the transatlantic arms market?	32
--	----

Table 2: US export control regime	34
--	----

2.3. Corruption and anti-money laundering	37
--	----

Chart 1: European companies have received some of the heaviest fines for violating the US Foreign Corrupt Practices Act (FCPA)	39
---	----

2.4. Human rights abuses and consumer protection	41
---	----

2.5. Tax evasion 43

2.6. Data collection and intelligence gathering 44

Box 4: 80% of European data is stored on
 non-European servers 48

2.7. Enforcement: the discovery procedure 49

3

**Consequences of non-compliance:
penalties and threats of exclusion** 51

Box 5: Non-compliance risks
 for European companies 54

4

**The future of US extraterritoriality:
a Trump card?** 55

Acknowledgements 59

Georgina Wright

Georgina Wright is Senior Fellow and Deputy Director for International Studies at Institut Montaigne. She joined the Institute in January 2021 to expand the Europe program. She is also a Visiting Fellow at the German Marshall Fund of the United States.

Georgina has been analyzing the European Union and wider Europe for over a decade. Her current research focuses on the EU's economic security agenda, EU decision-making, foreign policy and France's influence inside the EU. She is a member of several expert committees for national governments and regularly advises the EU's institutions. She has represented Institut Montaigne in high-level conferences and has given evidence to parliaments across Europe and in the US.

Louise Chetcuti

Louise Chetcuti was Project Officer for US and Transatlantic Affairs and part of Institut Montaigne's Europe program from February 2023 to July 2024. She joined the Institute in 2022 as Editorial Content Officer. Prior to this, she completed an internship in the Political Section of the US Embassy in Paris and served as a Fulbright scholar to Colombia (2018-2019).

She holds a MA in International Development from Sciences Po Paris' School of International Affairs and a BA in Spanish and Global Studies from Saint Mary's College, Notre Dame, Indiana.

Most people have never heard of David Cohen. Yet, he was President Obama's closest adviser and has gone on to occupy some of the most important positions inside the US government. Dubbed the US Treasury Secretary's "*favorite combatant commander*"¹ and later Washington's "*sanctions guru*", he was tasked with a specific mission: to ensure the effective deployment of sanctions overseas to protect and defend American interests. His mission was successful and Cohen became the Oval Office's most frequent visitor.

Sanctions, export controls, laws with extraterritorial reach. Extraterritoriality – understood as a situation wherein a state or an international organization applies its legislative, executive or judicial power outside of its territory – has become an essential foreign policy tool. The first case of US extraterritoriality dates back to 1890 and today the US uses extraterritoriality more than any other country in the world. Obama, Trump and Biden have all made use of extraterritoriality – though the Trump 1 administration did limit the reach of financial laws and reduce the role of the central government in overseeing their enforcement.

Both political parties see extraterritoriality as a useful instrument of American economic statecraft.

Despite this, few people understand how US extraterritoriality works. **Most cases of extraterritoriality are good for the US but also for Europe.** In today's globalized world, business is rarely confined to one country: to ensure rules are respected, you need international treaties or effective laws that apply outside of national borders. For example, US extraterritorial measures have proven to be a formidable tool to fight organized crime and money-laundering, to enforce global competition rules and to punish those who breach international law and treaties.

¹ A. Lowrey, "Aiming Financial Weapons from Treasury War Room", *The New York Times*. (3 June 2014), para.3, <https://www.nytimes.com/2014/06/04/business/aiming-financial-weapons-from-war-room-at-treasury.html>, accessed 4 Jan. 2024.

US sanctions against Cuba, Iran, North Korea, ISIS, al Qaeda and Russia have helped to curb the threat these actors pose internationally. Global cases of corruption have dropped significantly since the US extended the international reach of its anti-corruption laws. Similarly, most banks are far more measured in their risk-taking since the US, the EU and others passed new regulations after the 2008 financial crash. US export controls have been used to prevent American but also European companies from exporting critical materials to countries the US has marked as hostile and posing a threat to its national security.

But US extraterritoriality can also be bad and frankly ugly for Europe – and even for some US firms. US extraterritorial measures have clearly hurt the EU's economy: €18.8 billion in direct losses for EU companies since 2018. In the last two decades alone, European companies have been among the main targets for US laws and pursuits by US federal agencies² – more so in fact than US firms. High-profile cases have involved BNP Paribas, HSBC, Commerzbank, Crédit Agricole and Alstom, to name a few. Not only have these companies faced fines worth tens of thousands of dollars, but some have even been forced to sell part of their US-based activities to US competitors. This has led some of the US' trading partners to accuse it of hidden motives: using extraterritorial measures as a way to secure US market dominance by reducing competition from abroad. Some have even gone as far as to suggest the US government was using extraterritorial measures for espionage and intellectual property theft.³

US firms have also complained about US extraterritoriality. Studies have shown that US extraterritorial norms can harm US competitiveness by dissuading foreign companies from collaborating with US counterparts. According to transatlantic tech trade associations, *“extraterritorial*

² M-H. Bérard et al., “American extraterritorial sanctions – did someone say european strategic autonomy?”, *Europe In The World*. (March 2021), https://institutdelors.eu/wp-content/uploads/dlm_uploads/2021/03/PB_210315_US-Sanctions_IJD-JDC-EJD_EN.pdf, accessed 4 Jan. 2023.

³ A. Laïdi, *Le Droit, nouvelle arme de guerre économique*. (Actes Sud, 2019), 1.

application of US export controls creates regulatory burdens on European stakeholders and discourages European entities from collaborating with US counterparts, creating incentives to avoid US technology or, in some cases, hire US persons.”⁴

But if the US can get away with it, it is because it is very difficult to ignore, let alone stop, US extraterritorial norms from applying.

Today, US laws can target almost any individual and company in the world – even when they have no direct links with the US. Companies that fail to comply with US rules risk huge fines, exclusion from the US market and its financial system, and possibly prison time for their directors. Although some executive bodies, including the EU, have adopted statutes to “block” US extraterritoriality, they have failed to deter companies from complying with US rules.

For all these reasons, US extraterritoriality has long had a mixed reputation. Many European firms and governments are also worried about how the US will use it in the future to contain China.

The Biden administration has significantly restricted exports of high-tech dual-use items to China and has added over 319 Chinese companies to the Department of Commerce’s Entity List, which subjects them to further restrictions and licensing requirements. Many of these export controls also apply to EU firms that export to China. There have also been cases of the US government putting pressure on individual EU governments to adopt similar export control restrictions.

Yet, as the war in Ukraine has illustrated, the West, and especially Europeans, need US extraterritoriality.

Clearly, no Western sanctions regime can work without American involvement and the US worked closely with its G7 partners to adopt a robust sanctions regime against Russia. **However, the war in Ukraine has also highlighted the limits of**

⁴ M. Eitel, “Export Controls – The Keys to Forging a Transatlantic Tech Shield”, CEPA. (20 July 2023), <https://cepa.org/comprehensive-reports/export-controls-the-keys-to-forging-a-transatlantic-tech-shield/>, accessed 10 Jan. 2024.

extraterritorial sanctions, including US ones. Moscow has been able to limit some of the impact of Western sanctions by finding ways to bypass them all together. It has strengthened its economic axis with Tehran and Beijing and invested in trade flows that are entirely separate from the US and European markets. Russian companies have preferred to use the renminbi instead of the dollar for international transactions. Similarly, they have found new markets to sell their goods and other markets from which to import Western goods, such as electric vehicles (EVs) and chips, that are included in the different sanctions packages. The only way to remedy this shortcoming is for the US and like-minded partners, including the EU, to work more closely on extraterritorial norms.

The EU needs a better strategy to counter the bad and ugly sides of third-country extraterritoriality, while also finding a way to work closely with its allies, including the US and other partners, on the good aspects of extraterritoriality. The US has at times shown flexibility and willingness to listen to its allies' concerns. But clearly, the EU will stand a better chance at getting the US to listen to it if it can show that it understands US extraterritorial norms and how they are deployed.

1 The US Congress is mostly responsible for determining when extraterritoriality applies

Lawyers have yet to agree on a definition of extraterritoriality. For the purpose of this paper, it is best understood as a situation in which a state (or international organization) applies its powers (legislative, executive or judicial) outside of its territory to sanction irregular and illegal behavior, to protect human rights and international principles, and/or to protect its political and economic interests.

The United States has a long history of adopting laws with extensive extraterritorial reach. This began with the Sherman Anti-Trust Act in 1890, which was designed to end anti-competitive behavior – including monopolies and cartels – in the US market. While the Sherman Anti-Trust Act was first limited to economic activity in the United States, US courts gradually began to expand its reach so that it applied to all economic activity deemed to have adverse effects on US commerce – that included US companies operating abroad but also foreign companies whose activity is deemed to pose a direct threat to the US market.⁵

Despite the US’ widespread use of extraterritoriality, US statutes and administrative laws rarely reference it explicitly. This is not entirely surprising. Extraterritoriality is tolerated under international law so there is no need for the US to acknowledge it directly. That said, the *Restatement of the Law, Fourth: Foreign Relations Law of the United States* authorizes the US government to “regulate extraterritorially”⁶ when

⁵ S. F. Kava, “The Extraterritorial Application of the Sherman Anti-Trust Act in the Age of Globalization”, *Journal of Business & Technology Law*, 15/1 (2019), <https://digitalcommons.law.umaryland.edu/jbtl/vol15/iss1/5>.

⁶ “A Primer on Extraterritoriality”, *Transnational Litigation Blog*. (22 March 2024), <https://tlblog.org/a-primer-on-extraterritoriality/>, accessed 20 March 2024.

there is a case of “genuine connection”⁷ between the US and the act it is legislating for or against. Many countries apply a similar logic to justify their use of extraterritoriality. **Unlike many of its allies, the US has a very broad interpretation of “genuine connection”, which explains why it is able to target almost any individual, company and property in the world.** In 1945, US jurisprudence broadened the definition of “nexus” to include any foreign activity that undermines US exports, even when it does not impact the US market directly (see *United States v. Alcoa*).⁸ This gave the US more leeway to interpret when extraterritorial application is lawful or not.

In line with the US Constitution, Congress is responsible for discerning a statute’s geographical scope and whether it applies abroad. This discernment relies on two presumptions:

- The “presumption against extraterritoriality”: US law applies domestically unless Congress has explicitly determined otherwise (though there are some exceptions, for example for export controls). Cases include 2010 *Morisson v. National Australia Bank*⁹ and 1991 *EEOC v. Arabian American Oil Co.*¹⁰

⁷ The 1927 Lotus principle makes clear countries can apply a law extraterritorially when there is a clear and identifiable nexus between the country legislating and the act it is legislating for or against. For more details, see L. Chetcuti, C. Vidotto Labastie and G. Wright, “Extraterritoriality: a Blind Spot in the EU’s Economic Security Strategy”, Institut Montaigne, (January 2024), <https://www.institutmontaigne.org/en/publications/extraterritoriality-blind-spot-eus-economic-security-strategy>, accessed 24 Sep. 2024.

⁸ This case related to antitrust regulations, which the United States had begun to apply more aggressively to anticompetitive conduct outside US borders.

⁹ The Supreme Court held that US law against securities fraud does not apply to investment deals that occur overseas, even if they have a domestic impact or effect.

¹⁰ The case was about workplace discrimination overseas and whether US laws against discrimination applied to Aramco (a Saudi energy corporation). The Supreme Court ruled in favor of Aramco stating that Title VII of the Civil Rights Act (which prohibits employment discrimination) did not apply extraterritorially to the company’s actions outside US borders.

- The “Charming Betsy” canon (dating back to the 19th century): when international obligations and domestic law conflict, courts should refer to Congress’ interpretation (this is known as the judicial deference doctrine).

Until recently, **the Supreme Court had ruled that courts could defer to government executive agencies’ interpretation of regulations and statutes**, in the event that Congress had not directly addressed the question at the center of a dispute (1984 *Chevron USA v. Natural Resources Defense Council* and 1997 *Auer v. Robbins*). This granted executive agencies limited but greater discretion in interpreting the scope of application of different laws adopted by Congress, and reduced the risk of protracted legal battles.

Republican administrations had repeatedly tried to limit the interpretative powers of executive agencies – preferring to rely on Congress’ interpretation instead. During the Obama administration, Congress tried, but failed, to push back against the Supreme Court *Chevron* principle. During the first Trump presidency, the House introduced the 2017 Regulatory Accountability Act to restrict government agencies’ power of interpretation. The Act has yet to pass through the Senate but stands a greater chance of passing now that the Republicans hold the Congress and Senate.

What’s more, the Supreme Court recently overturned the 40-year-old legal precedent called the *Chevron* principle in the *Loper Bright Enterprises v. Raimondo* case¹¹. From now on, courts are responsible for determining whether agencies have acted lawfully in implementing legislation. This is both good and bad news for European companies.

¹¹ The case was scheduled for argument before the Supreme Court of the United States during the court’s October 2023-2024 term. *Loper Bright Enterprises v. Raimondo*, No. 22–451 (U.S. June 28, 2024), [https://www.supremecourt.gov/opinions/23pdf/22-451_7m58.pdf], accessed 18 Nov. 2024.

On the one hand, it gives them a chance to challenge executive agencies' use of extraterritorial norms and enforcement directly in US courts. At the same time, it could create regulatory uncertainty as it makes it harder for executive agencies and departments to enforce any kind of ambitious legislation and regulation, including on climate and environmental issues for example. This, the Democrats argue, could undermine the day-to-day work of the US government.

Finally, the US government has also used the national security exception of Article XXI in GATT to justify the use of extraterritorial measures and trade defense measures.¹² There is a growing bipartisan view in the US that the WTO and international treaties are no longer fit-for-purpose to protect the US' vital interests in today's world. For example, the Trump 1 administration cited Article XXI to justify new tariffs on steel and aluminum imports from the EU in 2018.

¹² Section (b) of Article XXI in GATT states that the WTO agreements should not prevent any member from "taking any action which it considers necessary for the protection of its essential security interests". General Agreement on Tariffs and Trade (GATT 1947).

Box 1: The American obsession with the law and extraterritoriality

Unlike France, which has a civil law system, the US uses common law.¹³ In common law countries, case law – in the form of published judicial opinions – can shape US law.¹⁴ In civil law countries, codified statutes predominate. The US also has a very distinct understanding of the “rule of law”. As Danish scholar Helle Porsdam wrote, “Americans practically think and breathe in legal terms”¹⁵ and penalties can be a lot harsher.

According to US sanctions expert Sascha Lohmann¹⁶, three factors help explain the US’ prolific use of extraterritoriality:

- An ideological commitment that rights are inalienable and transcend national borders;
- A legal culture shaped by the experience of steady territorial expansion and domination;
- An independent judiciary that enjoys wide latitude to determine the geographical scope of statutory law and its implementation through administrative regulations.

¹³ Ireland, the UK, Cyprus and Malta (as it integrates parts of the UK Common Law) all use common law. “Legal experts say common law Ireland to be ‘isolated’ within EU after Brexit”, Irish Legal News. (11 Sep. 2013), para.1, <https://www.irishlegal.com/articles/legal-experts-say-common-law-ireland-to-be-isolated-within-eu-after-brexite>, accessed 4 Jan. 2024.

¹⁴ “The Common Law and Civil Law Traditions”, Berkeley Law. (2010), 1, <https://www.law.berkeley.edu/wp-content/uploads/2017/11/CommonLawCivilLawTraditions.pdf>, accessed 4 Jan. 2024.

¹⁵ “Rule of Law in American Life: A Long and Intentional Tradition”, American Bar Association. (22 Aug. 2019), para. 2, https://www.americanbar.org/groups/public_education/resources/rule-of-law/rule-of-law-in-american-life-a-long-and-intentional-tradition/, accessed 4 Jan. 2024.

¹⁶ S. Lohmann, “Extraterritorial U.S. Sanctions: Only Domestic Courts Could Effectively Curb the Enforcement of U.S. Law Abroad”, SWP (2019), 1, https://www.swp-berlin.org/publications/products/comments/2019C05_lom.pdf, accessed 4 Jan. 2023.

2 A closer look at US extraterritorial laws

US extraterritorial norms are complex, have different goals and involve different federal agencies (see table 1 below).¹⁷

Table 1: Federal laws with extraterritorial reach

LAW	Atomic Energy Act (AEA), Arms Export Control Act (AECA) and Export Controls Reform Act (ECRA) (International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)) 1954, 1976 and 2018	Trading with the Enemy Act (TWEA) and International Emergency Economic Powers Act (IEEPA) 1917 and 1977	Foreign Corrupt Practices Act (FCPA) 1977	Iran Threat Reduction and Syria Human Rights Act (ITRSHRA) 2012	Clarifying Lawful Overseas Use of Data Act (CLOUD ACT) 2018
GOAL	Limit exports of “sensitive” items (civil & military).	Primary and secondary sanctions to protect US national security.	Anti-corruption laws.	Sanctions to counter the Iranian threat (nuclear, terrorism).	Protect data and fight terrorism, sexual exploitation of children and cybercrime.
PENALTIES FOR NON-COMPLIANCE	Loss of contracts, fines.	Fines, exclusion from US market, travel bans, frozen assets.	Fines, prison, exclusion from the US market and financial system.	Sanctions, exclusion from US market and financial system.	Fines.
HIDDEN/OR DISPUTED AIM	Maintain US market dominance.	Maintain US market dominance.	Weaken foreign competitors.	Expand US political dominance & ensure fair competition for US companies.	Data exploitation: espionage, intellectual property theft.

¹⁷ This paper includes a broad, but non exhaustive list of US laws with extraterritorial reach.

AGENCY IN CHARGE	State Department's Directorate of Defense Trade Controls (DDTC); Commerce Department's Bureau of Information and Security (BIS).	State Department, Justice Department, Treasury Department.	Justice Department, Securities and Exchange Commission (SEC).	Commerce Department, State Department, Treasury Department.	State Department, Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA).
COMPANY SUBJECTED TO PENALTY	Airbus	BNP Paribas, Commerzbank, Crédit Agricole	Alstom, ING Group	Tanker Pacific	Dassault Systèmes

2.1. SANCTIONS TO PROTECT NATIONAL SECURITY AND COUNTER TERRORISM

Sanctions¹⁸, whose primary concern is to ensure the national security of the United States have become an important tool for the US to exert pressure on hostile nations and to sanction persons and entities suspected of corruption. Examples of US federal statutes with extraterritorial provisions include:

- The **1917 Trading with the Enemy Act (TWEA)** and **1977 International Emergency Economic Powers Act¹⁹ (the IEEPA)**, arguably the most important statutory sources prescribing US sanctions in the realm of foreign and security policy. They give the US president power to end commercial or financial flows in times of war (thanks to the TWEA) and peace (thanks to IEEPA). The TWEA governs sanctions against Cuba, whereas US sanctions against other countries are generally derived from the IEEPA.²⁰

¹⁸ Many legal scholars dispute the use of the term 'sanctions' as these are often unilateral, and not based on a UNSC resolution. They prefer the use of the term unilateral sanctions.

¹⁹ "The International Emergency Economic Powers Act", *United States Code, Title 50, Chapter 35*, <https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter35&edition=prelim>, accessed 5 Jan. 2024.

²⁰ J. Buretta, M. Lew and M. Ardeljan, "US Sanctions", *The Guide to Sanctions. (Global Investigations Review: 2020)*, <https://globalinvestigationsreview.com/guide/the-guide-sanctions/first-edition/article/us-sanctions>, accessed 5 Jan. 2024.

- The **1996 Helms-Burton Act**²¹ (also known as the Cuban Liberty and Democratic Solidarity Act) and the **1996 Iran and Libya Sanctions Act** (ILSA, also called the D’Amato Act)²² are designed to prevent American and foreign companies from doing business with hostile nations (in this case with Cuba and with the petroleum sectors of Iran and Libya). ILSA was amended in 2012 and renamed the Iran Threat Reduction and Syria Human Rights Act (ITRSHRA).
- The **2017 Countering America’s Adversaries Through Sanctions Act** (CAATSA) governs sanctions against Russia, North Korea as well as additional sanctions on Iran (after the Trump 1 administration pulled the US out of the Joint Comprehensive Plan of Action – “JCPOA”). It also holds provisions to prevent foreign companies from making significant defense deals with these countries.²³

The US Department of Treasury’s Office of Foreign Assets Controls (OFAC) is responsible for enforcing these sanctions. At the time of writing, it is responsible for 38 sanctions programs and regularly updates lists of individuals and companies to which the sanctions apply.²⁴ Lists include **the list of Specially Designated Nationals (SDN List)**, the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List and the Non-SDN Palestinian Legislative Council List (among others).²⁵ Any individual or company on those lists will have their US assets blocked and “US Persons” (detailed below) are prohibited from doing business with them.²⁶

²¹ This statute is an update to the 1992 Cuban Democracy Act – also known as the Torricelli Act.

²² In 2006, ILSA was renamed to the Iran Sanctions Act (ISA). In 2012 ITRSHRA was passed, which amends portions of ISA.

²³ P. Jeydel et al., “A Detailed Look at the Countering America’s Adversaries Through Sanctions Act”, Steptoe. (Aug. 2017), <https://www.steptoe.com/en/news-publications/a-detailed-look-at-the-countering-america-s-adversaries-through-sanctions-act.html>, accessed 5 Jan. 2024.

²⁴ OFAC, “Sanctions Programs and Country Information”, US Department of Treasury, <https://ofac.treasury.gov/sanctions-programs-and-country-information>, accessed 5 Jan. 2024.

²⁵ “Sanctions Lists Search”, OFAC, <https://sanctionssearch.ofac.treas.gov/>, accessed 5 Jan. 2024.

There are two types of sanctions: primary and secondary. **Primary sanctions** tend to apply to “US Persons”, understood as:

- US nationals (regardless of where they live);
- Permanent residents and companies based in the US (along with any foreign branches or subsidiaries);
- Individuals or companies exporting US-origin goods (regardless of where they are based).²⁷

Primary sanctions can have broad application thanks to the “facilitation” rule, which prohibits a third-party from making a transaction that would be prohibited if conducted by a US person.²⁸ Paying in dollars, using the services of a US bank or US-based bank as well as stocking data on US servers all count as facilitation.²⁹ In 2014, US federal and state government agencies sanctioned French bank BNP Paribas for “conspiring to violate the IEEPA and the TWEA³⁰” by using the US financial system to process transactions on behalf of, among others, Iranian clients subject to US sanctions. The bank was fined \$8.9 billion. Similarly, in 2018, French bank Société Générale was fined \$1.3 billion for violating the IEEPA and TWEA.³¹

²⁶ OFAC, “Specially Designated Nationals and Blocked Persons List SDN”, US Department of Treasury. (28 Dec. 2023), <https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>, accessed 5 Jan. 2024.

²⁷ T. McKinnon, J. Terceño, K. Yamada, “Sanctions & Extraterritorial Effect”, Freshfields Bruckhaus Deringer. (10 Nov. 2022), United States Section, <https://riskandcompliance.freshfields.com/post/102i0ui/sanctions-extraterritorial-effect-why-multiple-restrictive-measures-may-apply>, accessed 24 Sep. 2024.

²⁸ “Overview of US sanctions laws and regulations”, Norton Rose Fulbright. (June 2019), (c) Direct and indirect liability and facilitation, <https://www.nortonrosefulbright.com/-/media/files/nrf/nr-fwib/knowledge-pdfs/overview-of-us-sanctions-laws-and-regulations-disclaimer.pdf?la=en-in&revision=>, accessed 5 Jan. 2024.

²⁹ D. Pilarski, “US Sanctions 101”, Watson Farley & Williams. (16 September 2020), US Person/Facilitation, <https://www.wfw.com/articles/us-sanctions-101/>, accessed 5 Jan. 2024.

³⁰ US Department of Justice Office of Public Affairs, BNP Paribas Agrees to Plead Guilty and to Pay \$8.9 billion [Press Release]. (30 June 2014), <https://www.justice.gov/opa/pr/bnp-paribas-agrees-plead-guilty-and-pay-89-billion-illegally-processing-financial>, accessed 5 Jan. 2024.

³¹ Board of Governors of the Federal Reserve, “Federal Reserve Board fines Société Générale S.A. \$81.3 million for firm’s unsafe and unsound practices primarily related to violations of U.S. sanctions against Cuba,” [Press Release] (18 Nov. 2018), <https://www.federalreserve.gov/newsevents/pressreleases/enforcement20181119a.htm>, accessed 25 March 2024.

Since the 1990s, the US has also been adopting secondary sanctions, which specifically target non-US persons if and when their activities are deemed to contravene US national security interests. The *Cuban Assets Control Regulations* (based on the TWEA) and the *Iran Transaction and Sanctions Regulations* apply to US but also non-US persons. A foreign company that invests in Iran's energy sector, for example, or decides to trade with companies blacklisted on SDNs, could easily be targeted by US secondary sanctions, even when it has no links to the US whatsoever. **While US law cannot prohibit a foreign company from doing business in a hostile nation, it can sanction the behavior when it can prove that the company's activities undermine US national security interests. Since the US adopts a broad definition of national security, these also include US economic interests.**³²

There are many examples of non-compliance. In 2015, the French bank *Crédit Agricole* agreed to pay \$787 million³³ for violating US sanctions against Iran, Sudan and other countries. *Crédit Agricole* admitted that it had permitted 11 Sudanese banks to keep accounts with *Crédit Agricole* – six of which were on the US' Specially Designated Nationals list (SDNs).³⁴ Germany's *Commerzbank* agreed to forfeit \$563 million and pay a \$79 million fine for sanction violations under the International Emergency Economic Powers Act (IEEPA) in 2015.³⁵ Dutch bank *ING* also settled \$619 million with the US Treasury Department's Office of Foreign Assets Control.³⁶

³² S. Lohmann, *Extraterritorial U.S. Sanctions*, 4.

³³ New York State Department of Financial Services, *NYDFS Announces Crédit Agricole To Pay \$787 million*, [Press Release]. (20 October 2015), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1510201, accessed 10 Jan. 2024.

³⁴ *Ibid.*

³⁵ US Department of Justice, *Commerzbank AG Admits to Sanctions and Bank Secrecy Violations* [Press Release]. (12 March 2015), <https://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million-and>, accessed 10 Jan. 2024.

³⁶ US Treasury Department, *Treasury Department Announces \$619 million Settlement with ING Bank* [Press release]. (12 June 2012), <https://home.treasury.gov/news/press-releases/tg1612>, accessed 10 Jan. 2024.

Box 2: Enforcing sanctions

There are several ways the US Department of Treasury's Office of Foreign Assets Controls (OFAC) can ensure sanctions are respected:

- 1. Fines:** Under the IEEPA, OFAC can impose fines on the basis of Economic Sanctions Enforcement Guidelines. These fines can go up to \$295,141 per violation – or twice the amount of the incriminated transaction. The process is not transparent, nor is it subject to judicial review under the 1946 Administrative Procedure Act.³⁷ These fines can apply to non-US persons.
- 2. Monitoring compliance:** asking companies and shareholders to hand over sensitive information. Non-compliance can result in exclusion from the US market and its financial system.
- 3. Refer violations to the Department of Justice for criminal proceedings:** convictions can result in further fines as well as prison time. Extradition treaties allow for non-US persons to be extradited and judged in the US.

The case of Iran is particularly interesting to understand how the US sees the role of sanctions in forcing foreign governments or entities to change behavior. In 2015, the Obama 2 administration signed the Joint Comprehensive Plan of Action (JCPOA) – a deal between Iran, the US, the EU, Russia and China to restrict Tehran's nuclear program and curb its nuclear ambitions. In return, signatories promised to ease sanctions on Iran. This was particularly beneficial to European companies that had invested in Iran in the past but had been forced to withdraw to avoid breaching US sanctions.

³⁷ *Ibid.*, 5.

The JCPOA has always been hugely divisive in the United States. When Donald Trump was elected in 2016, he delivered on his campaign pledge and pulled the US out of the agreement. The administration then reinstated sanctions that had been previously lifted to “*force the Iranian leadership into accepting demands to fundamentally change nuclear, but also regional and domestic policies.*”³⁸ The reinstatement of primary and secondary sanctions led many European, but also Asian companies, to completely withdraw from Iran – even though their own governments allowed trade and investment in Iran. More than 50 Iranian banks were cut out of the Belgium-based Society for Worldwide Interbank Financial Telecommunication (SWIFT) – the most widely used messaging system among international financial institutions – which made it almost impossible for Iran to trade internationally.³⁹ The sanctions even limited Iranians’ access to essential medicine.⁴⁰ Very quickly, Iran’s economic conditions worsened. The Biden administration has not brought the US back into the JCPOA.

In many other cases, US sanctions have proven indispensable to protect the US and its allies. US sanctions have enabled US law enforcement agencies to reduce terrorist threats. In November 2023, Binance, one of the largest crypto exchange companies, was found guilty of money laundering and for violating the Bank Secrecy Act (BSA) and the International Emergency Economic Powers Act (IEEPA).⁴¹ In particular, judges found that Binance had failed to establish safety programs that

³⁸ *Ibid.*, 2.

³⁹ *It is set up under Belgian law. Iranian banks could no longer do business with G10 central banks including Banca d’Italia, Bank of Canada, Bank of England, Bank of Japan, Banque de France, De Nederlandsche Bank, Deutsche Bundesbank, European Central Bank, Sveriges Riksbank, Swiss National Bank, and the US Federal Reserve System.*

⁴⁰ T. Sepehri Far, “Maximum Pressure US Economic Sanctions Harm Iranians’ Right to Health”, Human Rights Watch. (October 2019), <https://www.hrw.org/report/2019/10/29/maximum-pressure/us-economic-sanctions-harm-iranians-right-health>, accessed 5 Jan. 2024.

⁴¹ US Department of Justice, Office of Public Affairs, *Binance and CEO Plead Guilty to Federal Charges in \$4B Resolution [Press Release]*. (21 Nov. 2023), <https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution>, accessed 5 Jan. 2024.

would prevent transactions with terrorist groups including Hamas and the Palestinian Islamic Jihad, but also Al Qaeda and the Islamic State of Iraq and Syria (ISIS).⁴² The company was fined \$4.3 billion.

The 2018 Nobel Peace laureate Nadia Murad is one of 400 Yazidi women suing Lafarge, a French cement company (now a subsidiary of the Swiss-based Holcim Group) for conspiring to provide construction materials to ISIS.⁴³ Lafarge's subsidiary located in Syria admitted to paying ISIS and the Nusra Front, another US-designated foreign terrorist organization, nearly \$6 million to cancel out any competition from other cement companies. Lafarge's subsidiary was also accused of selling cement to ISIS directly to construct underground tunnels wherein Yazidi and Western hostages were held and tortured.⁴⁴

These cases show that extraterritorial legislation is a powerful way to ensure that companies operating in high-risk environments, including war-torn countries, are not supporting criminal or terrorist activities. In many cases, US efforts to foster responsible corporate behavior and legal accountability have paid off.

⁴² B. Bushard, "Justice Department Cites Hamas' Use Of Binance In \$4.3 Billion Settlement", *Forbes*, (21 Nov. 2023), para. 4, <https://www.forbes.com/sites/brianbushard/2023/11/21/justice-department-cites-hamas-use-of-binance-in-43-billion-settlement/?sh=68f8d20030fd>, accessed 5 Jan. 2024.

⁴³ US Department of Justice, Office of Public Affairs, *Lafarge Pleads Guilty to Conspiring to Provide Material Support to Foreign Terrorist Organizations*, [Press Release]. (18 Oct. 2022), <https://www.justice.gov/opa/pr/lafarge-pleads-guilty-conspiring-provide-material-support-foreign-terrorist-organizations>, accessed 5 Jan. 2024.

⁴⁴ A. Clooney, L. Wolosky, "Opinion | Why We're Helping Yazidi Americans Get Justice", *The New York Times*, (17 Dec. 2023), para.6, <https://www.nytimes.com/2023/12/17/opinion/isis-yazidi-lawsuit.html>, accessed 5 Jan. 2024.

2.2. EXPORT CONTROLS

Export controls are also a form of extraterritoriality. The **1954 Atomic Energy Act (AEA)**, the **1976 Arms Export Control Act (AECA)** and the **2018 Export Controls Reform Act (ECRA)** provide the US president with the right to ban exports of US items, equipment and software that could undermine US national security interests. **The US export controls regulation landscape is very complex:** each regulation has its own list of controlled items that are subject to licensing authorizations.

The **AEA** gives the US president the authority to prohibit unlicensed exports of nuclear equipment and material. It is administered by the Department of Energy's Nuclear Regulatory Commission.

The **AECA** controls exports (and sometimes imports) of “sensitive military items” (i.e. military goods and related services that incorporate US technology or software). This statute is implemented by the International Traffic in Arms Regulations (ITAR) and is administered by several agencies, including **the US Department of State's Directorate of Defense Trade Controls (DDTC) and the US Department of Defense's Defense Security Cooperation Agency (DSCA)**. The US Munitions List (USML), which is part of ITAR, identifies which items are subject to export controls⁴⁵. The DDTC is responsible for granting licensing requirements (or exemptions) for exporting these items. Licensing requirements can sometimes cover reexports or transfers too. For example, reexports or transfers of ITAR items between NATO countries or between NATO and its allies (Australia, Israel, Japan, New Zealand and South Korea) do not require additional licensing authorizations from the DDTC.⁴⁶

⁴⁵ *The USML builds on the Missile Technology Control Regime (MTCR) Annex, a non-legally binding multilateral agreement involving 35 countries, that seeks to limit the proliferation of missile technology through a list of controlled items.*

⁴⁶ “Licenses for the Export and Temporary Import of Defense Articles”, Title 22, Chapter I, Part 123, Code of Federal Regulations, <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-123>, accessed 9 Jan. 2024.

Box 3 : Is ITAR undermining the transatlantic arms market?

ITAR has attracted widespread criticism from American and European companies alike. For them, the licensing process:

- **Poses supply risks:** ITAR licensing tends to be slow and unpredictable, resulting in delays to existing projects and creating reputational costs for businesses.
- **Is burdensome and costly:** for products using one or more US items (whether parts or software), a licensing agreement will be required for each part. This entails significant administrative and legal burdens, which are costly. It partly explains why some EU governments, including the EU Commission, have called on EU defense companies to limit the use of US technology and items to “reduce the burden and dependence on items subject to ITAR”⁴⁷ export controls.
- **Reduces the competitiveness of US firms:** due to the complexity of ITAR, some EU commercial space industries such as Alcatel, Morotta Surrey Satellite, and EADS (Astrium), have started to build products that are “ITAR-free”. Sales have since rocketed and US companies no longer dominate the global space market since the early 2000s. Some US firms have also begun to do the same: Boeing’s 787 commercial jet is largely ITAR-free, making it easier to export and reexport.

⁴⁷ *European Commission, Commission unveils significant actions to contribute to European Defence, boost innovation and address strategic dependencies [Press Release]. (15 Feb. 2022), https://ec.europa.eu/commission/presscorner/detail/en/IP_22_924, accessed 9 Jan. 2024.*

Several US administrations have tried to reform ITAR. With the Export Control Reform (ECR) Initiative, President Obama tried to reform overly-complex licensing processes that are a burden for companies and do not necessarily reduce risks to national security.⁴⁸ He failed to get congressional support. In May 2023, Republican members of Congress spearheaded a bill – TORPEDO Act – to ease ITAR export restrictions to the UK and Australia which, together with the US, are signatories to the AUKUS deal in September 2021. This bill has garnered bipartisan support and in September 2024, the Department of State amended ITAR to grant exemptions to its licensing requirements for companies based in the UK and Australia.⁴⁹

ECRA governs the export, reexport and in-country transfer of commercial, dual-use items and other military items of “lesser sensitivity”. These licensing agreements are much more detailed and complex than ITAR. ECRA is implemented by Export Administration Regulations (EAR), which are administered by **the US Department of Commerce’s Bureau of Industry and Security (BIS)**. Export licenses or exemptions are required for all items **listed on the EAR’s Commerce Control List (CCL)**.⁵⁰

⁴⁸ US Department of State, Bureau of Public Affairs, “The President’s Export Control Reform Initiative: Reinventing the System and Promoting National Security”, US State Department Archives. (10 May 2013), <https://2009-2017.state.gov/r/pa/pl/2013/209319.htm>, accessed 9 Jan. 2024.

⁴⁹ J. Risch, M. McCaul, “Congressional Republicans are seeking an arms export overhaul to cut red tape for the AUKUS agreement”, Politico Congress Minutes. (5 May 2023), <https://www.politico.com/minutes/congress/05-4-2023/aukus-legislation/>, accessed 9 Jan. 2024.

⁵⁰ J. Voetelink, “The Extraterritorial Reach of US Export Control Law. The Foreign Direct Product Rules”, *Journal of Strategic Trade Control*, 1/1, (2023), 5, <https://popups.uliege.be/2952-7597/index.php?id=57>.

Table 2: US export control regime

1976 Arms Export Control Act (AECA)
<p>Aim: Control exports (and sometimes imports) of “sensitive military items” (i.e. military goods and related services that incorporate US technology or software). This statute is implemented by the International Traffic in Arms Regulations (ITAR).</p>
<p>Enforcement agencies: Several agencies, including the US Department of State’s Directorate of Defense Trade Controls (DDTC) and the US Department of Defense’s Defense Security Cooperation Agency (DSCA).</p>
2018 Export Controls Reform Act (ECRA)
<p>Aim: Control the export, reexport and in-country transfer of commercial, dual-use items and other military items of “lesser sensitivity”. These licensing agreements are much more detailed and complex than those of ITAR. ECRA is implemented by Export Administration Regulations (EAR).</p>
<p>Enforcement agencies: The US Department of Commerce’s Bureau of Industry and Security (BIS).</p>

If the EAR is a sweeping assertion of extraterritorial power, it is because of the Foreign Direct Product Rule (FDPR). The FDPR stipulates that export controls are required:

- For products that are made with 10 to 25% (or more) of commercial or dual-use components that originate from the US⁵¹ – even when these items are made outside of the US.
- For items containing sensitive US technology or that use US manufacturing processes – even when these items are made outside of the US.
- For companies that are transporting these items.⁵²

Before 2013, there was just one FDPR. It applied to a small range of dual-use items and was limited to exports and reexports to specific countries that were considered hostile to the United States. Over the past decade, BIS has expanded the FDPR significantly thereby **allowing the United**

⁵¹ *Ibid.*, 8.

⁵² T. Johnson, D. Bade, *Export/Import Procedures and Documentation*. (New York: AMACOM, 2010), 187.

States to expand its jurisdiction over most ‘critical’ items that are manufactured using US software, equipment, or technology – even when these products are devoid of US components or manufactured abroad.⁵³ This is a significant headache for EU companies that specialize in the design, manufacturing, or transport of “critical” items as they are often required to comply with several export control regimes. In the case of non-compliance, they can be pursued by the US judiciary and government agencies.

During the Trump 1 administration, the US expanded EAR to restrict technology exports to China.⁵⁴ In 2019, the US Department of Commerce added Huawei and its 68 non-US affiliates (located in countries such as Belgium, Germany, Japan, the United Kingdom and Vietnam) to the Entity List.⁵⁵ Similarly, the Biden Administration amended EAR in October 2022 by adding semiconductor equipment, advanced chips and commodities containing chips to the Commerce Control List (CCL).⁵⁶ President-elect Trump has also promised to adopt more aggressive export control policies vis-à-vis China and harsher sanctions on companies that fail to respect them⁵⁷.

⁵³ S. Gearity, “Understanding the Foreign Direct Product Rule”, *Export Compliance Training Institute*. (20 Dec. 2022), <https://www.learnexportcompliance.com/understanding-the-foreign-direct-product-rule/>, accessed 9 Jan. 2024.

⁵⁴ T. Gehrke, J. Ringhof, “The Power of Control: How the EU can shape the new era of strategic export restrictions”, *ECFR*. (May 2023), <https://ecfr.eu/wp-content/uploads/2023/05/The-Power-of-Control-How-the-EU-can-shape-the-new-era-of-strategic-export-restrictions.pdf>, accessed 9 Jan. 2024.

⁵⁵ R. Burke et al., “US Designates Huawei to Entity List, Issues Temporary General License”, *White & Case LLP*. (23 May 2019), <https://www.whitecase.com/insight-alert/us-designates-huawei-entity-list-issues-temporary-general-license>, accessed 9 Jan. 2024.

⁵⁶ A. W. Palmer, “‘An Act of War’: Inside America’s Silicon Blockade Against China”, *New York Times*. (12 July 2023), <https://www.nytimes.com/2023/07/12/magazine/semiconductor-chips-us-china.html>, accessed 9 Jan. 2024.

⁵⁷ A. Slodkowski, J. Pomfret, and L. Chen, “Ready or not? How China scrambled to counter the second Trump shock”, *Reuters*, (November 2024), <https://www.reuters.com/world/ready-or-not-how-china-scrambled-counter-second-trump-shock-2024-11-08/>, accessed 18 Nov 2024.

The US has been putting pressure on its allies to better coordinate, and even align, export control legislation.⁵⁸ In January 2023, the United States, the Netherlands and Japan struck an agreement to further restrict exports of advanced chip-manufacturing equipment to China, such as lithography tools made by Dutch company ASML and Japan's Nikon and Tokyo Electron.⁵⁹ **US-China trade tensions flared up as a result.** In a bid to de-escalate tensions, the US and China set up in August 2023 new channels of communication for economic and commercial issues. These include a new bilateral forum to discuss export controls ("Export Control Enforcement Information Exchange") and the establishment of a new "Commercial Issues Working Group" to expand commercial opportunities.⁶⁰ Healthcare and clean technologies were identified as potential areas for cooperation, but it is unclear whether these have gleaned any significant results. Nor did it stop the Biden administration from passing new export controls in October 2023 on semiconductors, semiconductor manufacturing equipment and advanced computing equipment destined for China. As Noah Barkin noted, these measures have significant extraterritorial reach in that they introduced a zero-percent de minimis rule that allows Washington to assert jurisdiction over foreign-made lithography equipment, such as those produced by the Dutch firm ASML, even when it does not contain any US components.⁶¹ A Commerce Department communiqué added that these controls were aimed at restricting China's "ability to

⁵⁸ P. Haeck, "How the Dutch turned on Chinese tech", *Politico*. (9 March 2023), <https://www.politico.eu/article/chips-netherlands-mark-rutte-china/>, accessed 9 Jan. 2024.

⁵⁹ US Department of Commerce, Bureau of Industry and Security, "Federal Register: Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items", *Federal Register*. (18 Jan. 2023), <https://www.federalregister.gov/documents/2023/01/18/2023-00888/implementation-of-additional-export-controls-certain-advanced-computing-and-semiconductor>, accessed 9 Jan. 2024.

⁶⁰ US Department of Commerce, Readout of Secretary Raimondo's Meeting with Minister of Commerce of the People's Republic of China Wang Wentao [Press Release]. (28 Aug. 2023), <https://www.commerce.gov/news/press-releases/2023/08/readout-secretary-raimondos-meeting-minister-commerce-peoples-republic>, accessed 9 Jan. 2024.

⁶¹ N. Barkin, "Watching China in Europe", *GMFUS* (7 Nov. 2023), para. 12, <https://www.gmfus.org/news/watching-china-europe-november-2023>, accessed 9 Jan. 2024.

both purchase and manufacture certain high-end chips critical for military advantage [...] and close loopholes.”⁶²

2.3. CORRUPTION AND ANTI-MONEY LAUNDERING

The 1977 Foreign Corrupt Practices Act (FCPA), revised in 1998⁶³, **allows the Department of Justice to pursue entities suspected of corruption.** In particular, the Act prohibits individuals and companies from bribing foreign officials and requires them to maintain strict internal audits. Three categories of ‘people’ are concerned by the FCPA⁶⁴:

- “Issuers” – i.e. companies issuing securities on the US market and their directors, administrators, shareholders or any other person acting on their behalf;⁶⁵
- “Domestic concerns” – i.e. US citizens, residents and companies under US law (foreign companies and foreign nationals can be subject to the FCPA if they are seen to facilitate a breach of the FCPA);
- “Persons other than issuers or domestic concerns” – i.e. any natural or legal person, regardless of their nationality, using US interstate commerce or US postal services as a means to make a corrupt payment.

⁶² *US Department of Commerce, Bureau of Industry and Security, Commerce Strengthens Restrictions on Advanced Computing Semiconductors, Semiconductor Manufacturing Equipment, and Supercomputing Items to Countries of Concern [Press Release]. (17 Oct.2023), <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3355-2023-10-17-bis-press-release-acs-and-sme-rules-final-js/file>, accessed 9 Jan. 2024.*

⁶³ *It was revised after OECD nations signed and passed the Anti-Bribery Convention in 1997. The US began to apply the FCPA outside of its borders from 1998.*

⁶⁴ *L. Byrd et al., “Does the FCPA Apply to Foreign Companies?”, Oberheiden Security Litigation & Compliance, <https://federal-lawyer.com/securities-litigation/fcpa/apply-foreign-companies/>, accessed 9 Jan. 2024.*

⁶⁵ *S. Menegon, A. Murgier, W. Julie, “United States extraterritoriality: European Union sovereignty at stake. International Bar Association”, International Bar Association, US extraterritorial laws prohibiting corruption and money laundering, <https://www.ibanet.org/article/CF85E59E-6564-4AA3-9408-3F47C6449C9D>, accessed 9 Jan. 2024.*

The US Department of Justice’s Criminal Division, along with the Security and Exchange Commission’s (SEC) Enforcement Division, are responsible for pursuing and investigating violations of the FCPA.

Any company listed on the New York Stock Exchange (NYSE) is deemed to be within the FCPA’s reach. Evidence shows that US authorities have targeted both American and foreign businesses, but that the top fines have been paid by foreign firms. According to data from the Foreign Corrupt Practices Act Clearinghouse (FCPAC), out of the 10 companies hit hardest by FCPA sanctions since 1997, only one is American. The others were from Europe (5 companies), Latin America (3 companies) and Russia (1 company).⁶⁶ European businesses hit by FCPA sanctions include, among others Airbus, and its subsidiary in the Netherlands, Ericsson (Sweden), Siemens (Germany), Alstom (France) and Société Générale (France).⁶⁷ **The fact that foreign companies have paid more to the US Treasury, despite more US companies being sanctioned overall, has led many allies to question what other motives, beyond fighting corruption, were behind the Act** (see chart 1 p. 39 for more details). According to the FCPA Corporate Enforcement Policy Justice Manual, if a company voluntarily “*self-discloses, fully cooperates, and promptly remediates*”⁶⁸ before the start of criminal proceedings, the fine can be reduced by up to 50%. However, this often means handing over to US law enforcement authorities sensitive information about a company’s activities, account details and commercial flows.

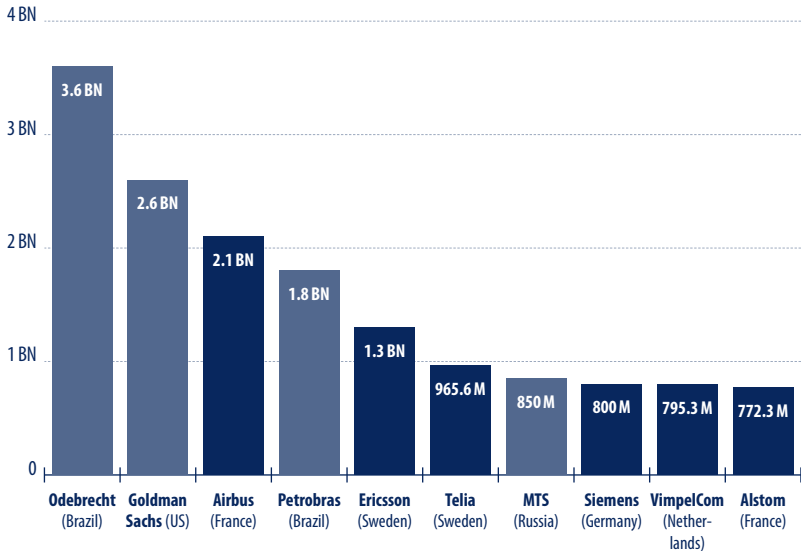
⁶⁶ Data retrieved from “Total and Average Sanctions Imposed on Entity Groups per Year”, Stanford Law School, <https://fcpa.stanford.edu/statistics-analytics.html?tab=2>, accessed 9 Jan. 2024.

⁶⁷ “How U.S. extraterritorial legal action affects European companies”, Brussels Report. (16 Dec. 2021), para. 25, <https://www.brusselsreport.eu/2021/12/16/how-u-s-extraterritorial-legal-action-affects-european-companies/>, accessed 9 Jan. 2024.

⁶⁸ “Foreign Corrupt Practices Act Of 1977 – Justice Manual”, US Department of Justice, 1. Credit for Voluntary Self-Disclosure, Full Cooperation, and Timely and Appropriate Remediation in FCPA Matters, <https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977>, accessed 9 Jan. 2024.

Chart 1: European companies have received some of the heaviest fines for violating the US Foreign Corrupt Practices Act (FCPA)

Amounts in billions of dollars



Source: Foreign Corrupt Practices Act Clearinghouse (FCPAC).

Until 2007, the annual penalties under the FCPA averaged under or around \$75 million. However, **fines increased significantly from 2008 onwards, reaching a record annual high of over \$6 billion in 2016. Since 2022, fines have been steadily decreasing (that year, they did not exceed \$1.5 billion).** In 2008, Siemens paid \$350 million to the SEC and \$450 million to the Department of Justice after it was found guilty of bribing foreign officials in Argentina, Bangladesh, China, Iraq, Mexico, Venezuela, and Vietnam.⁶⁹ Another high-profile example involved

French TotalEnergies which agreed to pay \$398 million in penalties in 2013 for illicit payments to an Iranian government official in return for access to oil and gas fields.⁷⁰ In 2020, Airbus – one of the world’s two largest manufacturers of commercial aircrafts – agreed to pay more than \$3.9 billion to authorities in the US, France and the United Kingdom on charges that it had violated the FCPA and the AECA, and its implementing regulation the ITAR (view section II). In 2018, the Trump 1 administration arrested Meng Wanzhou, CFO of Huawei Technologies on charges of fraud and conspiracy to commit fraud by selling US technology to Iran.⁷¹ Meng was arrested in Canada and extradited to the US.

President Trump has expressed his dislike for the FCPA, which he considers “horrible and unfair” for companies. In the Spring of 2017, he asked his then-Secretary of State Rex W. Tillerson to look into ways to scrap the FCPA without the need to involve Congress. He also tasked his advisor Stephen Miller to draft an executive order to repeal it. However, Tillerson, Miller and the then-Attorney General Jess Sessions pushed to maintain the anti-corruption legislation. While the number of investigations decreased, more companies were prosecuted under the Trump 1 administration, than they were under the Obama 2 administration.⁷²

⁶⁹ *Ibid.*

⁷⁰ R. Cassin, “Total SA pays \$398 million to settle U.S. bribe charges”, *The FCPA Blog*. (29 May 2013), <https://fcpablog.com/2013/05/29/total-sa-pays-398-million-to-settle-us-bribe-charges/>, accessed 9 Jan. 2024.

⁷¹ D. Wakabayashi, A. Rappeport, “Huawei C.F.O. Is Arrested in Canada for Extradition to the US”, *The New York Times*. (5 Dec. 2018), <https://www.nytimes.com/2018/12/05/business/huawei-cfo-arrest-canada-extradition.html>, accessed 9 Jan. 2024.

⁷² C. D. Leonnig and P. Rucker, *A Very Stable Genius: Donald J. Trump's Testing of America*, Penguin Press (2020).

2.4. HUMAN RIGHTS ABUSES AND CONSUMER PROTECTION

The 2016 Global Magnitsky Human Rights Accountability Act authorizes the US president to impose economic sanctions, revoke visas, freeze assets and deny entry into the United States to any foreign person suspected of committing human rights abuse or corruption. It builds on the 2012 Sergei Magnitsky Rule of Law Accountability Act, which banned access into the United States to all those involved in the death of Sergei Magnitsky, a Russian tax auditor who exposed cases of corruption in Russia.⁷³

On December 20, 2017, President Trump issued Executive Order (EO) 13818⁷⁴ to combat “*widespread human rights abuse and corruption*”⁷⁵. President Trump’s EO expanded the scope more to target all those responsible for, or complicit to, serious human rights abuses. The EO allows the Secretary of the Treasury, in close consultation with the Secretary of State and the Attorney General, to decide whether or not to impose sanctions. As is the case with sanctions regimes generally, **the Department of the Treasury’s Office of Foreign Assets Control (OFAC) administers the economic sanctions, while the State Department implements visa bans.**

⁷³ M. A. Weber, E. J. Collins-Chase, “The Global Magnitsky Human Rights Accountability Act”, Congressional Research Service. (28 Oct. 2020), <https://crsreports.congress.gov/product/pdf/IF/IF10576>, accessed 9 Jan. 2024.

⁷⁴ Administration of Donald J. Trump, “Executive Order 13818 – Blocking the Property of Persons Involved in Serious Human Rights Abuse or Corruption”, US Government Information. (20 Dec. 2017), <https://www.govinfo.gov/content/pkg/DCPD-201700923/pdf/DCPD-201700923.pdf>, accessed 9 Jan. 2024.

⁷⁵ Donald Trump, “the prevalence and severity of human rights abuse and corruption [...] have reached such scope and gravity that they threaten the stability of international political and economic systems” and “constitute an unusual and extraordinary threat to national security.” in *Ibid.*

The 2010 Dodd-Frank Act⁷⁶ was adopted in the wake of the global financial crisis to protect consumers and taxpayers by improving the accountability and transparency of the global financial system and by limiting its risk-taking.⁷⁷ Section 619 of the Dodd-Frank Act, known as the “Volcker Rule”, prohibits “banking entities”⁷⁸ from engaging in “proprietary trading” and from acquiring or retaining an ownership interest in a hedge fund or a private equity fund (“Covered Funds”). **The Volcker Rule’s broad definition of the term “banking entity” is what justifies its huge extraterritorial reach:** it impacts US banks and US-based banks; insured depository institutions and US bank holding companies; and foreign banks with a US branch.⁷⁹ What’s more, if a foreign bank has a US subsidiary, the Volcker Rule applies to every one of its subsidiaries regardless of where they are located in the world. Finally, if a foreign bank holds at least 25% of share capital in a company that has links to the US, then the Rule applies to that company too.⁸⁰

This provision has been heavily criticized in Europe and Asia. Michel Barnier, France’s Prime Minister and former European Commissioner for Internal Market and Services from 2010 to 2014, argued that it was not “*acceptable that US rules have such a wide effect on other nations.*”⁸¹

⁷⁶ Also known as the Dodd-Frank Wall Street Reform and Consumer Protection Act.

⁷⁷ “Dodd-Frank Wall Street Reform and Consumer Protection Act”, Commodity Futures Trading Commission. (5 Jan. 2010), https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf, accessed 9 Jan. 2024.

⁷⁸ Defined as (i) any insured depository institution; (ii) any company that controls an insured depository institution; (iii) any [foreign banking organization]; and (iv) any affiliate of the foregoing.

⁷⁹ L.Bozhanova, “The Extraterritorial Effects of The Volcker Rule”, *Global Markets Law Journal*, Vol 4. (2016), 1., <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1017&context=global-markets>, accessed 9 Jan. 2024.

⁸⁰ V. Denoix de Saint Marc, “La Volcker Rule”, August Debouzy. (19 Dec. 2011), *L’application extra-territoriale de la Volcker Rule aux entités ayant un lien capitalistique avec une entité bancaire américaine*, <https://www.august-debouzy.com/fr/blog/738-la-volcker-rule>, accessed 9 Jan. 2024.

⁸¹ Commissioner Barnier proposal on Europe Economic Situation, originally published on the website of the European Commission in 2012. “Voorstellen eurocommissaris Barnier om economische situatie Europa aan te pakken”, *Parlement.com*. (23 Feb. 2012), https://www.parlement.com/id/vix8mpghdxzw/nieuws/voorstellen_eurocommissaris_barnier_om, accessed 11 Jan. 2024.

Erkki Liikanen, Chair of the European Union’s High-Level Expert Group on Banking Reform, criticized the Volcker Rule for being both too narrow – because it mainly targets proprietary trading – and too radical regarding proprietary trading.⁸² In a joint letter sent to US regulators on December 28, 2011, the Bank of Japan and Japan’s financial services regulator complained that restrictions on the trading of foreign sovereign bonds would “impose a significant burden and higher costs on foreign banks, including major Japanese firms.”⁸³

The Trump 1 administration proposed to roll back some of Dodd-Frank’s restrictions, notably its extraterritorial reach. In 2018, the Republican-held Congress passed the **Economic Growth, Regulatory Relief, and Consumer Protection Act** with some Democratic support. The reform retained the Dodd-Frank framework but limited its reach. In particular, the bill increased the threshold for stress tests from \$50 billion to \$250 billion, exempting many small and midsize banks from reporting requirement.⁸⁴

2.5. TAX EVASION

The US also enforces its tax laws abroad. The **2010 Foreign Account Tax Compliance Act (FATCA)** is a federal statute that applies to US Persons who hold assets in foreign accounts.⁸⁵ It applies to individuals as well as a broad scope of financial institutions (banks, investment funds, asset managers, life insurance companies) with links to the US. US taxpayers

⁸² E. Liikanen, “High-level Expert Group on reforming the structure of the EU banking sector Final Report”, European Commission. (2 Oct. 2012), https://finance.ec.europa.eu/publications/liikanen-report_en, accessed 9 Jan. 2024.

⁸³ F. Guerrero, T. Corrigan, S. Nixon, “EU Plans Complaint on ‘Volcker Rule’”, *The Wall Street Journal*. (27 Jan. 2012), para. 9, <https://www.wsj.com/articles/SB10001424052970204573704577185100193763384>, accessed 9 Jan. 2024.

⁸⁴ N. Berman, “What Is the Dodd-Frank Act?” Council on Foreign Relations. (May 2023), <https://www.cfr.org/background/what-dodd-frank-act>, accessed 22 March 2024.

⁸⁵ “What is FATCA?”, US Tax Financial Services, <https://www.ustaxfs.com/fatca/>, accessed 9 Jan. 2024.

must submit an annual tax declaration to the Internal Revenue Service (IRS), the US authority responsible for collecting federal taxes. The Federal Trade Commission (FTC) enforces FACTA and conducts audits of credit agencies and financial institutions.⁸⁶

The FATCA has garnered criticism as evidenced in a report commissioned by the EU Parliament's Policy Department for Citizens' Rights and Constitutional Affairs.⁸⁷ The 2018 report mentions negative effects on "Accidental Americans" (citizens and/or tax residents of EU countries who have US citizenship) including difficulties opening a bank account in an EU financial institution due to FATCA-related costs⁸⁸ and complex US compliance rules. In France, the Paris-based Association of Accidental Americans (AAA) filed a complaint against the US State Department.⁸⁹ Many Americans, especially those living abroad, have also pushed back against the FACTA.

2.6. DATA COLLECTION AND INTELLIGENCE GATHERING

US national security legislation also contains extraterritorial provisions to collect and process data stored in the US and, increasingly, overseas. Statutes include:

⁸⁶ *US Federal Trade Commission, FTC Issues Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity*, [Press Release], (29 Oct. 2004), <https://www.ftc.gov/news-events/news/press-releases/2004/10/ftc-issues-final-rules-facta-identity-theft-definitions-active-duty-alert-duration-appropriate-proof>, accessed 9 Jan. 2024.

⁸⁷ C. Garbarino, "FATCA Legislation and its Application at International and EU Level", *European Parliament Think Tank*. (14 May 2018), [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2018\)604967](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)604967), accessed 9 Jan. 2024.

⁸⁸ *Ibid.*, 6.

⁸⁹ "Association des Américains Accidentels", <https://www.americains-accidentels.fr/page/222256-qui-sommes-nous>, accessed 9 Jan. 2024.

⁹⁰ "FISA Section 702 Overview", *Director of National Intelligence, US Government*, <https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf>, accessed 9 Jan. 2024.

- **The 1978 Foreign Intelligence Surveillance Act (FISA)**, amended in 2008, which established the FISA Court to grant the US government the right to surveil “foreign targets” (terrorists or spies), in the US and abroad, who present a threat to the US national security. In 2008, Congress extended the extraterritorial provisions⁹⁰ thereby authorizing the US government to target almost any person abroad and to collect their emails and text messages without the need for an individualized court order (which was previously required).⁹¹ The FISA Court’s role is now limited to approving general procedures for surveillance, which are reviewed annually.⁹² FISA is enforced by several federal government agencies, including the FBI and the Justice Department’s National Security Agency.
- **The 2001 USA PATRIOT Act**, signed in the aftermath of 9/11 and amended in 2005, sets out national security surveillance and intelligence gathering provisions.⁹³ The 2005 amendment made it easier for the International Emergency Economic Powers Act (IEEPA) to block assets of individuals and entities suspected of terrorism. US courts can ask foreign companies to hand over data to US law enforcement agencies in the case of an ongoing investigation – especially if companies are based in countries that have a Mutual Legal Assistance Treaty (MLAT) with the US (which France does). The PATRIOT Act is not enforced by a specific agency, but instead gives broad authority to several agencies, from the Department of Defense to more local law enforcement authorities (police officers, FBI agents, federal prosecutors, and intelligence officials of the NSA and the CIA).

⁹¹ E. Goitein, “The Coming Fight Over American Surveillance”, *Foreign Affairs*. (6 June 2023), para. 16, <https://www.foreignaffairs.com/united-states/coming-fight-over-american-surveillance>, accessed 9 Jan. 2024.

⁹² *Ibid.*, para. 12.

⁹³ “Surveillance Under the USA/PATRIOT Act”, *The American Civil Liberties Union*. (23 Oct. 2001), <https://www.aclu.org/documents/surveillance-under-usapatriot-act>, accessed 9 Jan. 2024.

- **The 2018 Clarifying Lawful Overseas Use of Data Act (CLOUD Act)**, which replaced the 1986 Stored Communications Act (SCA), is a policy with extraterritorial reach designed to protect “national security, judiciary or fiscal interests.”⁹⁴ It contains two parts:
 - Part 1 clarifies cases where US law enforcement authorities can request data held by US providers abroad. This allows the US government to obtain electronic communications (emails, texts) as well as relevant metadata (timing of the message and contact details of the addressees).⁹⁵ Service providers must, in accordance with the Act, meet the US government’s demands and supply the necessary information.
 - Part 2 authorizes the US to enter into executive agreements with countries to expedite data-sharing. In practice, US law enforcement authorities have the right to demand data stored on servers in those countries (and, reciprocally, to share data stored on US servers). So far, the US has executive agreements with the United Kingdom and Australia – and is reportedly negotiating one with Canada, New Zealand and the EU.⁹⁶ According to the UK Home Office, part 2 can help speed up the Mutual Legal Assistance Treaty (MLAT) process and data-sharing across borders.⁹⁷

Although there are a number of safeguards in place to prevent abuse by law enforcement authorities,⁹⁸ many countries have voiced concerns over these data-sharing statutes – accusing the US of wider espionage (including industrial espionage to maintain an economic edge) and

⁹⁴ F. Godement, V. Zhu, “Cross-Border Data Flows: The Choices for Europe”, Institut Montaigne. (April 2023), 15, https://www.institutmontaigne.org/ressources/pdfs/publications/Institut%20Montaigne_actionnote_cross-border_data_flows_the_choices_for_europe_0.pdf, accessed 9 Jan. 2024.

⁹⁵ E. Lostrì, “The CLOUD Act”, CSIS. (2 Oct. 2020), <https://www.csis.org/blogs/strategic-technologies-blog/cloud-act>, accessed 9 Jan. 2024.

⁹⁶ F. Godement, V. Zhu, *Cross-Border Data Flows*, 35.

⁹⁷ “Policy factsheet on the UK-US Data Access Agreement”, UK Home Office. (21 July 2022), <https://www.gov.uk/government/publications/uk-us-data-access-agreement-factsheet/policy-factsheet-on-the-uk-us-data-access-agreement>, accessed 9 Jan. 2024.

undermining privacy. As Institut Montaigne experts François Godement and Viviana Zhu⁹⁹ demonstrate, Section 702 of FISA and the 1981 Executive Order 12333, together with the CLOUD Act, facilitate the NSA's broad collection and use of intelligence from foreign networks. On 12 April 2024, the House of Representatives reauthorized Section 702 of FISA for only two years (instead of five) marking a major defeat for privacy advocates and some Republicans, including President Trump, who were calling on the introduction of additional warrants to avoid abuses and "backdoor searches", which he falsely believed the Biden administration was using to investigate him.¹⁰⁰

EU countries have been especially critical. Ever since the 2013 Snowden NSA revelations, Europeans have been largely distrustful of the US' handling of EU data¹⁰¹ and believe the US' approach contravenes EU privacy and data protection laws. European countries, but also other countries like China, have begun to ask companies to store their citizens' data on national servers. In 2021, the French Government pushed for the creation of a *Cloud de Confiance*,¹⁰² a French cloud to store sensitive data. The Gaia-X initiative, which emanated from a Franco-German proposal in 2019, was set up to create a common European data and cloud infrastructure. However, **migrating the data away from US servers to European servers has proven difficult.**

⁹⁸ For example, a Stored Communications Act (SCA) order will only be granted if US law enforcement authorities can demonstrate that a particular criminal offense has likely been committed and that the information sought after is relevant to the ongoing criminal investigation. Service providers also have the right to challenge these SCA orders where they conflict with domestic law (H.R.4943 – CLOUD Act – 115th Congress (2017-2018)).

⁹⁹ F. Godement, V. Zhu, *Cross-Border Data Flows*, 15.

¹⁰⁰ "CDT Issue Brief: Debunking Myths & Fixing FISA §702 Backdoor Search Loophole", Center for Democracy & Technology. (10 January 2024), <https://cdt.org/insights/cdt-issue-brief-debunking-myths-fixing-fisa-s702-backdoor-search-loophole/>, accessed 22 March 2024.

¹⁰¹ Edward Snowden, a former NSA employee, revealed that the NSA was tapping Americans' phones and collecting their data in bulk – effectively spying – even where there was no identified security risk. He also claimed that the NSA had targeted EU governments and companies with its spying activities. E.Snowden, *Permanent Record* (Mc Millan, 2019).

¹⁰² P. Roche-Bruyn, "Entre mesures extraterritoriales et lois de blocages, quel ordre économique mondial ?", IRIS. (March 2023), https://www.iris-france.org/wp-content/uploads/2023/03/Prog-GeopoEntre_Extraterritorialite_Mars-2023.pdf, accessed Nov. 2023.

Box 4: 80% of European data is stored on non-European servers

Today, more than 80% of European data is hosted by non-European Cloud Service Operators (CSOs) – most of which are American. Amazon Web Services (AWS), Microsoft Azure and Google Cloud alone account for more than two-thirds of the European market,¹⁰³ making it easier for the US, through the CLOUD Act, to obtain the data.

As demonstrated in a paper for Institut Montaigne,¹⁰⁴ governments do not access, store, share and use data the same way. In 2019, the US Department of Justice published a White Paper highlighting the advantages of the CLOUD Act for foreign governments.¹⁰⁵ For example, a data-sharing agreement with the US can generate faster and greater access to foreign data stored in the US for criminal investigations.

At the same time, several countries are trying to strike privacy agreements with the US to manage cross-border data flows. After years of talks, the EU Commission adopted in July 2023 an adequacy decision confirming that the US provides the same level of protection of EU data that the EU does.¹⁰⁶ This is part of the EU-US Data Privacy Framework

¹⁰³ F. Verzelen, “La présidence française de l’Union européenne, une opportunité unique pour l’Europe du digital”, *L’Usine nouvelle*. (16 Jan. 2022), para. 4, <https://www.usinenouvelle.com/article/avis-d-expert-la-presidence-francaise-de-l-union-europeenne-une-opportunit-e-unique-pour-l-europe-du-digital.N1175557>, accessed 9 Jan. 2024.

¹⁰⁴ F. Godement, V. Zhu, *Cross-Border Data Flows*.

¹⁰⁵ “The Purpose and Impact of the CLOUD Act”, US Department of Justice. (Ap. 2019), https://www.justice.gov/d9/pages/attachments/2019/04/10/doj_cloud_act_white_paper_2019_04_10.pdf, accessed 9 Jan. 2024.

¹⁰⁶ “Questions & Answers: EU-US Data Privacy Framework”, European Commission. (10 July 2023), 1. What is an adequacy decision?, https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752, accessed 9 Jan. 2024.

concluded in March 2022 and provides a legal basis for transfers of personal data from EU countries to the US.¹⁰⁷ The deal gives Europeans the ability to object when they believe their personal information has been collected improperly by US intelligence agencies.¹⁰⁸ In September 2023, France was the first country to challenge the deal before the European Court of Justice. In his statement, French MEP Philippe Latombe argued that the deal “*violates the Union’s Charter of Fundamental Rights, due to insufficient guarantees of respect for private and family life with regard to bulk collection of personal data and GDPR rules*.”¹⁰⁹ The US-EU adequacy agreement is likely to be supplemented by bilateral agreements between the US and individual member states.

2.7. ENFORCEMENT: THE DISCOVERY PROCEDURE

The discovery procedure refers to the pre-trial phase in a US lawsuit during which parties obtain and exchange evidence.¹¹⁰ It is extremely invasive: for most of the laws listed in this paper, US courts can ask non-US parties – including individuals, companies and sometimes

¹⁰⁷ US Department of Justice, Office of Public Affairs, *Justice Department Statement on the European Union’s Adoption of Trans-Atlantic Data Privacy Framework* [Press Release]. (10 July 2023), <https://www.justice.gov/opa/pr/justice-department-statement-european-unions-adoption-trans-atlantic-data-privacy-framework>, accessed 9 Jan. 2024.

¹⁰⁸ Any complaint laid before a national authority within the European Economic Area (EEA) is transmitted to the US Civil Liberty Protection Officer whose role is to ensure compliance by US agencies with fundamental rights. If the individual does not agree with the decision reached, he or she can appeal to an independent review body – the Data Protection Review Court (DPRC) – composed of non-US-government officials, selected based on particular qualifications and that will hear European appeals. EU Commission, *Questions & Answers: EU-US Data Privacy Framework*.

¹⁰⁹ L. Kayali, “French lawmaker challenges transatlantic data deal before EU court”, *Politico*. (7 Sep. 2023), para. 4, <https://www.politico.eu/article/french-lawmaker-challenges-transatlantic-data-deal-before-eu-court/>, accessed 9 Jan. 2024.

¹¹⁰ “How Courts Work: Discovery”, *American Bar Association*. (28 Nov. 2021), https://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/discovery/, accessed 9 Jan. 2024.

governments – to submit information and documents.¹¹¹ **In many cases, judges’ requests are sent directly to companies, often bypassing diplomatic channels.** For example, the 1996 Helms-Burton Act made it easier for US courts to start legal proceedings against foreign persons or companies, including European ones, deemed to be ‘trafficking’ in property expropriated by Cuba from US nationals. **Some foreign governments are worried that this procedure poses a serious risk for their companies, especially if the judge or the disputing party exploits the litigation process to access confidential information about the other company’s activities.**¹¹²

In March 2023, the United Nations High Commissioner for Human Rights (OHCHR) questioned the compatibility of US extraterritorial jurisdiction with international human rights standards, including freedom of movement and the right to due legal process. **France has been one of the most vocal critics of US data-gathering laws** with former French Prime Minister Édouard Philippe commissioning a parliamentary report – the Gauvain Report¹¹³ – to look into how US extraterritorial norms and jurisdiction were impacting French companies.

In recent years, foreign litigants have started to rely on foreign data protection laws to resist the discovery procedure – EU companies have

¹¹¹ L. Cohen-Tanugi, “The Extraterritorial Application Of American Law: Myths And Realities”. (February 2015), <http://dx.doi.org/10.2139/ssrn.2576678>, accessed 9 Jan. 2024.

¹¹² A. Giuliani, “Beyond European extraterritoriality, for legal intelligence and compliance in the service of sovereignty”, Fondation Robert Schuman. (30 Jan. 2023), 2/5, <https://www.robert-schuman.eu/en/european-issues/0654-beyond-european-extraterritoriality-for-legal-intelligence-and-compliance-in-the-service-of>, accessed 9 Jan. 2024.

¹¹³ R. Gauvain et al., « Rétablir la souveraineté de la France et de l’Europe et protéger nos entreprises des lois à portée extraterritoriale », Vie Publique. (26 June 2019), 11., https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/194000532.pdf, accessed 11 Dec. 2023.

¹¹⁴ I. (Wuerth) Brunk, “Foreign Data Protection Laws: Greater Impact on U.S. Discovery than Foreign Blocking Statutes”, Transnational Litigation Blog. (25 Oct. 2022), Foreign Data Protection Laws, <https://tlblog.org/foreign-data-protection-laws-greater-impact-on-u-s-discovery-than-foreign-blocking-statutes/>, accessed 9 Jan. 2024.

turned to the EU's General Data Protection Regulation (GDPR), for example.¹¹⁴ GDPR has also been used to fine US companies when they are found to contravene EU privacy rules. In May 2023 Meta (an American multinational tech giant) was fined a record €1.2 billion euros for transferring data from Facebook users in Europe to US authorities.¹¹⁵ The extraterritorial reach of GDPR has been criticized by both China and the US on the grounds that it is overly restrictive and limits the power of their tech giants.

3 Consequences of non-compliance: penalties and threats of exclusion

With many extraterritorial laws in existence, a company's chances of breaking the law, even inadvertently, are high. Over the last years, the US has imposed billions of dollars' worth of fines on foreign firms, including European ones, for failing to comply with its sanctions regime. **The legal uncertainty for companies is considerable:** firms need to understand what their products are made of, where they are fabricated, and whom they are sold to and shared with.

As seen in section I (p. 19), the reason why the US is able to target so many foreign companies – even those with no business activity in the US – is because its jurisprudence has a very broad definition of “nexus”, which justifies when extraterritorial application is lawful or not. The following examples have been used to justify US extraterritoriality:

- **Trading in dollars/using the services of US or US-based banks:** any entity or person processing transactions in dollars can be targeted by US extraterritorial norms.

¹¹⁵ A. Satariano, “Meta Fined \$1.3 Billion for Violating E.U. Data Privacy Rules”, *The New York Times*. (22 May 2023), <https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>, accessed 9 Jan. 2024.

- **Being listed on the New York Stock Exchange (NYSE):** any company listed on the NYSE can be targeted, including subsidiaries based elsewhere in the world.
- **Stocking or sharing data through US-based servers:** storing data on US servers can count as a US nexus. As does the transit of data through US platforms (i.e. banking system, the stock exchange, servers).
- **Exporting US technology:** the US subjects certain foreign-made items that are produced with US technology, software, or equipment to the jurisdiction of the Export Administration Regulations (EAR) – even if they contain no US-origin content and are traded between parties outside the US. Exemptions are listed on the EAR's Commerce Control List (CCL).

Export controls are primarily used by the US as tools to protect its national security. Given its large market and the global role of the US dollar, US sanctions and export controls provide the United States with tremendous leverage. For many companies, access to US banking and dollar clearing systems is so crucial that they often agree to plead guilty to violations – even when they do not think they are at fault. In some cases, US authorities do not even need to start legal proceedings as the simple prospect of being excluded from the US market is enough to get companies to end their activities. It also acts as a deterrent: **the threat of losing access to the US financial market outweighs the benefits of trading with states the US considers hostile (like Iran), leading to a high compliance rate – even over compliance by foreign companies.**

Consequences for non-compliance can be significant:

- **Civil and criminal penalties:** sanctions and export controls violations may result in fines of up to \$1 million per violation, costly legal proceedings and even prison sentences of up to 20 years.¹¹⁶

¹¹⁶ “What are Primary & Secondary Sanctions?”, *Comply Advantage, Who Must Comply with Primary Sanctions?* <https://complyadvantage.com/insights/primary-secondary-sanctions/>, accessed 9 Jan. 2024.

- **Exclusion from the US market:** no imports or exports to the US; loss of US presence or contracting opportunities (which can affect a company's shareholder value); travel bans and being added to the SDN list.
- **Exclusion of the US financial system:** Closing down the access to payments in dollars is, in the words of sanctions expert Sascha Lohmann, "*the Wall Street equivalent of the death penalty*".¹¹⁷
- **Reputational damage:** export control violations and sanctions breaches are widely publicized as national security risks, and may cause damage to brand and personal reputations.
- **Company restructuring or downsizing:** to comply with US regulatory demands¹¹⁸ and monitoring obligations, companies may have no other choice but to restructure their operations to adhere to regulations (see Box 5, p. 54 for more details).
- **Espionage:** when a company is accused of breaching US law, US authorities can ask it to hand over sensitive information about its operations, such as industrial designs and contracts, as part of the investigation. Although there are a number of safeguards to prevent abuse by law enforcement authorities, some countries have accused the US of espionage as a way to maintain an economic edge and market hegemony over foreign competitors (see Box 5 for more details).

¹¹⁷ S. Lohman, *Extraterritorial U.S. Sanctions*, 4.

¹¹⁸ *The contractualization of ethical and compliance obligations can now be imposed by the customers or partners of any business. These present further legal risks and breaches can result in the termination of a contract.*

Box 5: Non-compliance risks for European companies

Company restructuring – the case of Alstom

In 2014, Alstom (a French power and transport group) reached a deal with the US Department of Justice to pay up to \$772 million for foreign bribery charges – one of the largest fines in a foreign corruption case ever recorded – after the US authorities suspected Alstom of paying a total of at least \$75 million in bribes in Egypt, Saudi Arabia, the Bahamas, Taiwan and Indonesia.¹¹⁹ Alstom pleaded guilty in 2014 and agreed to sell 70% of its power and grid businesses to General Electric (GE) for \$13.6 billion. This case raised uncomfortable questions about US motives and techniques, with some arguing that US authorities had facilitated the buyout to advance the commercial interests of an American company (GE). The buyout also put a stop to any potential merger between Alstom and Shanghai Electric Company, which had been under discussion at the time.¹²⁰

Hand over of sensitive documents – the case of Airbus

When the European aerospace company Airbus was found guilty of violating different US anti-bribery and export controls laws in 2020, the US Department of Justice and the US Department of State asked it to turn over millions of internal business documents as part of the investigation.¹²¹

¹¹⁹ US Department of Justice, *Alstom Pleads Guilty and Agrees to Pay \$772 million [Press Release]*, (22 Dec. 2014), <https://www.justice.gov/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery>, accessed 9 Jan. 2024.

¹²⁰ “Former exec of French firm Alstom: Yesterday Alstom, today Huawei, and tomorrow?”, *The Straits Times*, (29 May 2019), para. 7, <https://www.straitstimes.com/asia/east-asia/former-exec-of-french-firm-alstom-yesterday-alstom-today-huawei-and-tomorrow>, accessed 9 Jan. 2024.

¹²¹ This case started in 2016 after Airbus reported irregularities in payments made to third-party consultants. This violated both the US Foreign Corrupt Practices Act (FCPA), the Arms Export Control Act (AECA) and its implementing regulation the International Traffic in Arms Regulations (ITAR).

4 The future of US extraterritoriality: a Trump card?

In the last few years, the US has moved toward a more expansive definition of national security with, at its core, the need to protect its economic and geo-economic interests. **Washington sees extraterritorial norms as an effective tool to safeguard these interests and to prevent any developments abroad – whether military, technological or civil – that could undermine its national security.** Obama, Trump and Biden have all made use of extraterritoriality – though the Trump 1 administration did limit the reach of some laws and reduce the role of the central government in overseeing their enforcement.

The use of US extraterritoriality is only likely to grow over time and could become a more prominent tool in containing China’s rise. This would have implications for US firms that export to China, but also European ones. **The US sees China’s inroads in emerging technologies as posing a national security risk** and has redefined its national security to adapt to this new geopolitical reality¹²². Export controls have become a key foreign policy tool – with both the Trump I and Biden administrations adding many more Chinese entities to export restrictions lists. As seen in section II, the US and China agreed in August 2023 to hold regular conversations on official channels about commercial issues and tech restrictions, in an attempt to de-escalate tensions.¹²³ But this has not stopped the US from adopting stringent export controls to reduce China’s ability to further develop its Military-Civil Fusion strategy.

¹²² “Remarks by National Security Advisor Jake Sullivan at the SCSP Global Emerging Technologies Summit”, *The White House*. (16 Sept. 2022), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/>, accessed 10 Jan. 2024.

¹²³ A. Swanson, K. Bradsher, “U.S. and China Agree to Broaden Talks in Bid to Ease Tensions”, *The New York Times*. (28 Aug. 2023), <https://www.nytimes.com/2023/08/28/business/economy/united-states-china-trade-talks-raimondo.html>, accessed 10 Jan. 2024.

What does this mean for Europe?

In many cases, US extraterritoriality has been vital – both as a way to safeguard the US’ interests and those of its allies. But its excessive use has also been a point of contention in the transatlantic relationship.¹²⁴ In August 2023, the French National Assembly's Foreign Affairs Committee called on the French Parliament and the Treasury to better monitor the impact of international sanctions on French companies.¹²⁵

Cooperating on the “good”, while stopping the “bad” uses of US extraterritoriality will continue to be a concern for EU governments. As we highlight in our paper *Extraterritoriality: a Blind Spot in the EU's Economic Security Strategy*,¹²⁶ the EU itself is gradually adopting defensive measures, such as the Blocking Statute, to respond to third countries’ extraterritorial measures. It has also adopted laws with extraterritorial reach such as the General Data Protection Regulation (GDPR), Digital Markets Act (DMA), Digital Service Act (DSA) and Artificial Intelligence Act (AI Act) – laws which the US has itself been very critical of. However, **the EU needs a new strategy to work with the US where their extraterritorial laws align and push back against it when they do not.** Coordination on sanctions, like those imposed on Russia after its invasion of Ukraine, is positive. But the EU must also have clear arguments to level against the US when it uses extraterritoriality excessively.

¹²⁴ S. Erlanger, “Europe Struggles to Defend Itself Against a Weaponized Dollar”, *The New York Times*. (12 March 2021), <https://www.nytimes.com/2021/03/12/world/europe/europe-us-sanctions.html>, accessed 10 Jan. 2024.

¹²⁵ *French Bulletin Quotidien*, 30 August Edition, 2023, “12-13.”

¹²⁶ L. Chetcuti, C. Vidotto Labastie and G. Wright, “Extraterritoriality: a Blind Spot in the EU's Economic Security Strategy”, Institut Montaigne. (January 2024). <https://www.institutmontaigne.org/en/publications/extraterritoriality-blind-spot-eus-economic-security-strategy>, accessed 20 March 2024.

The US also has an incentive to talk to the EU about extraterritoriality. As we have seen, the war in Ukraine has exposed the limit of extraterritorial sanctions, even US ones. The US worked closely with its G7 partners to adopt a robust sanctions regime against Russia. Despite this, Moscow has been able to limit some of the impact by further developing a separate economic axis with Tehran and Beijing. Russian companies have been using the renminbi instead of the dollar for international transactions. Similarly, they have found new markets to sell their goods to – and other markets from which to import Western goods, such as EVs and chips, that are included in the different sanctions packages. The only way to remedy this is for the US and like-minded partners, including the EU, to work more closely on extraterritorial norms. Washington also knows that it will only be able to prevent China from gaining technological supremacy if allies adopt similar measures.

The EU may find a sympathetic ear in some parts of the US. Not everyone in the States looks favorably on US extraterritoriality. Sanctions and trade embargoes have compelled US companies to leave markets – and their departure is quickly filled by foreign companies. When the US imposed stringent sanctions on Cuba in the late 1990s and early 2000s, Russian and Chinese companies were all too happy to take their place.¹²⁷ Meanwhile, US extraterritorial norms can also dissuade foreign companies from collaborating with US firms. President Trump has also been critical of some US sanctions, such as the FCPA. For him, these sanctions pose two major risks to the US economy:

- First, they could weaken the dollar's dominant position in foreign transactions. Trading in dollars is often a sufficient reason for US sanctions to apply to a foreign company – which is why some have been tempted to trade in other currencies.

¹²⁷ S. Blockmans, "Extraterritorial sanctions on trade and investments and European responses", Policy Department for External Relations, European Parliament. (Nov. 2020), [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653618/EXPO_STU\(2020\)653618_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653618/EXPO_STU(2020)653618_EN.pdf), accessed 11 Jan. 2024.

- Second, they risk making US firms – and trading with the US – less attractive. Complying with US laws is costly and complex. This can put US firms at a commercial disadvantage compared to their international competitors and dissuade foreign companies from doing business in the US.

The Trump 2 administration will continue to use extraterritoriality – though whether it embraces the full spectrum of US extraterritorial norms is unclear. It is best seen as a (foreign policy) Trump card, which, depending on the use, will have good and bad implications for Europe. The Trump 2 approach to extraterritoriality is likely to be a fine balancing act between the need to advance and defend US interests vs. the need to avoid regulations that stifle US exports and weaken the dollar's dominant position in international transactions. The one notable exception are export controls. The next Administration is likely to tighten export rules, while exerting pressure on European countries to align. It is likely to use every available leverage to force EU countries into agreement, including threatening to scale back the US military presence in Europe or by imposing new tariffs on European exports to the US.

Discussing extraterritoriality is vital and should form part and parcel of any transatlantic discussion on economic security. The EU position will only be heard if it can prove that it has understood US extraterritoriality and that it has a credible strategy in place to respond to it – a strategy that aligns with the US where necessary and pushes back where US extraterritoriality undermines its core interests.

Acknowledgements

This paper, like our first paper on extraterritoriality published in January 2024,¹²⁸ is the result of in-depth research and many conversations, including:

- Over 60 primary and secondary sources analyzed;
- Over 15 interviews with senior officials from EU institutions, member-state governments and third countries, including the US;
- Over 20 interviews with senior representatives from the private sector, public sector (including national parliaments) and academia;
- 3 workshops with leading experts and companies dealing with the repercussions of extraterritorial measures.

The authors extend their gratitude to the senior officials, business representatives, experts and external reviewers they spoke to, all of whom substantially improved this paper. They are particularly grateful to their colleagues **Dr. Marie-Pierre de Bailliencourt**, **Dr. Mathieu Duchâtel**, **Cécilia Vidotto Labastie**, **Énora Morin**, **Lola Carbonnel**, **Mélissa Westphal** and **Vera Edwall** for their helpful comments and suggestions.

¹²⁸ L. Chetcuti, C. Vidotto Labastie and G. Wright, “Extraterritoriality: a Blind Spot in the EU’s Economic Security Strategy”, Institut Montaigne. (January 2024). <https://www.institutmontaigne.org/en/publications/extraterritoriality-blind-spot-eus-economic-security-strategy>, accessed 24 Sep. 2024.

*Institut Montaigne welcomes thoughts and ideas
on how to address these issues collectively
and put forward recommendations which serve
the public interest.*



Institut Montaigne
59 rue La Boétie, 75008 Paris
Tél. +33 (0)1 53 89 05 60
institutmontaigne.org/en

Printed in France
Legal filing: December 2024
ISSN: 1771-6756

ABB France	Dassault Systèmes	Kea	RATP
AbbVie	Delair	Kearney	Renault
Accenture	Deloitte	KPMG S.A.	Ricol Lasteyrie
Accor	De Pardieu Brocas	Kyndryl	Rivolier
Accuracy	Maffei	La Banque Postale	Roche
Actual Group	Domia Group	La Compagnie	Roche Diagnostics
Adeo	Edenred	Fruitière	Rokos Capital
ADIT	EDF	LCH SA	Management
Air Liquide	EDHEC Business	Lenovo ISG	Rothschild & Co
Airbus	School	Linedata Services	RTE
Allianz	Ekimetrics France	Lloyds Europe	Safran
Amazon	Engie	London Stock	Sanofi
Amber Capital	EQT	Exchange	SAP France
Amundi	ESL & Network	L'Oréal	Schneider Electric
Antidox	Eurogroup	LVMH - Moët-	ServiceNow
Antin Infrastructure	Consulting	Hennessy - Louis	Servier
Partners	FGS Global	Vuitton	SGS
ArchiMed	Forvis Mazars	M.Charraire	SIER Constructeur
Ardian	Getlink	MACSF	SNCF
Arqus	Gide Loyrette Nouel	Média-Participations	SNCF Réseau
Arthur D. Little	Google	Mediobanca	Sodexo
AstraZeneca	Groupama	Mercer	SPVIE
August Debouzy	Groupe Bel	Meridiam	SUEZ
AXA	Groupe M6	Microsoft France	Synergie
A&O Shearman	Groupe Orange	Mitsubishi France	Teneo
Bain & Company	Hameur et Cie	S.A.S	The Boston
France	Henner	Moelis & Company	Consulting Group
Baker & McKenzie	Hitachi Energy	Moody's France	Tilder
BearingPoint	France	Morgan Stanley	Tofane
Bessé	Howden	Natixis	TotalÉnergies
BNP Paribas	HSBC Continental	Natural Grass	TP ICAP
Bolloré	Europe	Naval Group	Transformation
Bouygues	IBM France	Nestlé	Factory
Bristol Myers Squibb	IFPASS	OCIRP	Unicancer
Brousse Vergez	Incyte Biosciences	ODDO BHF	Veolia
Brunswick	France	Oliver Wyman	Verian
Capgemini	Inkarn	Ondra Partners	Verlingue
Capital Group	Institut Mérieux	OPmobility	VINCI
CAREIT	International SOS	Optigestion	Vivendi
Carrefour	Interparfums	Orano	Wakam
Chubb	Intuitive Surgical	PAI Partners	Wavestone
CIS	Ionis Education	Pelham Media	Wendel
Clariane	Group	Pergamon	White & Case
Clifford Chance	iQo	Polytane	Willis Towers Watson
CNP Assurances	ISRP	Publicis	France
Cohen Amir-Aslani	Jeantet Associés	PwC France &	Zurich
Conseil supérieur du notariat	Johnson & Johnson	Maghreb	
D'Angelin & Co.Ltd	Jolt Capital	Qualisocial	
	Katalyse	Raise	

Extraterritoriality – the application of national laws abroad – has grown exponentially over the last two decades. In a world characterized by strategic competition and weak international organizations, many countries are turning to law to secure their interests. None more than the United States.

There are good and bad uses of US extraterritoriality. It has become a key tool to uphold international law and to safeguard the US' interests. It has helped to sanction hostile states and combat corruption, money laundering, organized crime and terrorism. It has helped to reduce excessive risk-taking by companies and has been used to manage US-China systemic rivalry. However, the US has also been accused of using it as a way to assert market dominance.

Could extraterritoriality be the next Trump Card the United States plays? During his first term, President Trump tightened export controls and expanded US laws to combat human rights abuses. At the same time, he rolled back banking regulations and asked his team to review US laws that created unnecessary red tape. Recently, he warned that he would remove any sanctions that weakened the dollar's dominant position. The extent to which extraterritoriality is used to exert political pressure on EU countries is unclear.

The EU must be better prepared. Companies that fail to comply with US rules risk huge fines, handover of sensitive data and exclusion from the US market. European companies often prefer to comply with US rules, rather than abide by European measures designed to block their application. This poses a direct challenge to the sovereignty of the EU and its member states.

Institut MONTAIGNE's latest issue paper provides a framework for understanding all dimensions of US extraterritoriality and offers decision-makers and businesses a roadmap for an informed response. **Understanding the implications of US extraterritoriality is crucial for governments and businesses, and should be integral to the EU's approach to economic security.**

10 €

ISSN: 1771-6756

NCL2412-01

