The Heritage Foundation

BACKGROUNDER

No. 3276 | JANUARY 9, 2018

The U.S. Must Draw a Line on the EU's Data-Protection Imperialism

Ted R. Bromund, PhD

Abstract

On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) will come into force. Described by the European Commission as a measure to strengthen individual rights in the digital age and facilitate business, the GDPR embodies and expands the EU's effort to apply its data-protection standards to governments and private enterprise inside and outside the EU. Together with an EU directive governing the processing of personal information by government authorities, the GDRP will mark the beginning of another phase in a long-running struggle between the U.S. and the EU over the handling of individual data by U.S. corporations and the U.S. government. The EU has persistently and hypocritically raised the bar in its demands on the U.S.—and only on the U.S. The EU sees no problem when European data is transferred to China or Russia. The U.S. has approached the EU as a friend, but it has been treated worse than China. It is therefore time for the U.S. to stop being played for a fool, to recognize the EU's hostility, and—before the GDRP takes effect—to take measures that will force the EU to recognize that the U.S. will not stand by as the EU exerts legal authority over U.S. firms.

On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) will come into force. Described by the European Commission as a measure that will strengthen individual rights in the digital age and facilitate business, the GDPR both embodies and expands the EU's effort to apply its data-protection standards to governments and private enterprise both inside and outside the EU.[1] Together with an EU directive governing the processing of personal information by government authorities, the

Key Points

- On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) will take effect. It continues the EU's effort to expand and apply its data-protection standards to governments and private enterprise both inside and outside the EU.
- The GDRP is the beginning of another phase in a long-running struggle between the U.S. and the EU over the handling of individual data by U.S. corporations and the U.S. government.
- The EU campaign has not been about data protection: It uses EU rule-making to discriminate against U.S. businesses and to increase the power of the EU.
- The EU raises the bar only on the U.S. It is time for the U.S. to stop placating the EU's ever-escalating demands, to withhold U.S. data from European authorities if the EU ends data transfers to the U.S. government or businesses, and to insist that EU law does not apply in the U.S.

This paper, in its entirety, can be found at **http://report.heritage.org/bg3276**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

GDRP will mark the beginning of another phase in a long-running struggle between the U.S. and the EU over the handling of individual data by U.S. corporations and the U.S. government.

This struggle has been marked by repeated U.S. efforts to satisfy EU demands, and by the EU's near-exclusive focus on the data-protection wrongs supposedly committed, or at risk of being committed, by the U.S. government and U.S. businesses. The EU has devoted far less attention to online businesses or governments in nations such as the People's Republic of China, and has even backed an Organization for Economic Co-operation and Development (OECD) initiative that would result in the routine and automatic sharing of bulk taxpayer information among governments worldwide. In short, the EU's campaign has not been about data protection: It has been a form of regulation protectionism that uses EU rule-making to discriminate against U.S. businesses and to increase the power of the European Union by appealing to the anti-Americanism of those who regard U.S. intelligence agencies, and the U.S.'s Section 702 authorities, as their enemy.[2]

The EU's campaign has sought to dampen regulatory competition, which helps governments and societies determine which forms of regulation more effectively promote consumer and citizen welfare. At its core, the EU campaign—of which Britain will, on current plans, continue to be part after Brexit—is the result of the fact that U.S. businesses have been more successful online than their European counterparts. It is time for the U.S. to end its quest to placate the EU's ever-escalating demands, to withhold U.S. data from European authorities if the EU ends data transfers to the U.S. government or businesses, and to stand firmly on the principle that EU law does not apply in the U.S., just as U.S. law does not apply in Europe. If it does not, the EU's offensive against the U.S. will continue, with resulting damage to U.S. firms, U.S. intelligence programs, and the broader competitiveness of the United States.

The European Union's GDPR

The EU's incoming data-protection regime consists of Regulation (2016/679) on the protection of personal data, and the movement of such data, and the accompanying Directive (2016/680) on the protection of personal data, and the movement of such data, when used by competent government authorities, to prevent, detect, or prosecute criminal activities. The regulation enters into force on May 25, 2018; the directive enters into force on May 5, 2018, and must be enacted into law by the member states of the EU by May 6, 2018. In spite of Brexit, the British government has introduced a Data Protection Bill that will incorporate the GDPR into U.K. law, a step that will make it more difficult for the U.K. to negotiate modern and beneficial trade agreements after it exits the EU.[3]

The GDPR imposes direct statutory obligations on data processors. Among other changes, it enhances the purported "right to be forgotten" and strictly regulates the automatic processing of data. It allows the EU to impose fines up to 4 percent of the total worldwide financial turnover in the preceding year in case of a breach, a sum that could amount to hundreds of millions, or even billions, of dollars.[4] The GDPR applies to all personal data that originates in the EU, regardless of the location of the data processor. The directive allows EU governments to transfer person-

1. For the EU's overview, see European Commission, "Justice: Protection of Personal Data," http://ec.europa.eu/justice/data-protection/ (accessed December 14, 2017).
2. Though European campaigners sometimes stretch this point by treating even their own governments as the enemy. See "German Court Rules Against Foreign Intelligence Mass Communications Surveillance," Reuters, December 14, 2017, https://www.reuters.com/article/us-germany-surveillance/german-court-rules-against-foreign-intelligence-mass-communication-surveillance-idUSKBN1E82RS (accessed December 14, 2017), which reports on a German court decision that the German foreign intelligence agency is not allowed even to store phone numbers of international calls.
3. U.K. Department for Digital, Culture, Media and Sport, "Data Protection Bill: Factsheet–Overview," September 14, 2017, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644634/2017-09-13_Factsheet01_Bill_overview.pdf (accessed December 14, 2017). For an overview of the issues raised for the private sector in the context of Brexit, see Lori Baker, "The Impact of the General Data Protection Regulation on the Banking Sector: Data Subjects' Rights, Conflicts of Laws and Brexit," *Journal of Data Protection and Privacy*, Vol. 1. No. 2 (2017), pp. 137–145, https://www.henrystewartpublications.com/sites/default/files/JDPP%201.2%20-%20Lori%20Baker.pdf (accessed December 14, 2017).
4. See Regulation (EU) 2016/679 of the European Parliament and of the Council, April 27, 2016, Article 83, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (accessed December 14, 2017).

al data for law enforcement purposes, but only if the receiving jurisdiction has "adequate" protections.[5] While the directive sets out factors that the commission must consider in assessing adequacy, it does not provide a definition of this concept. The European Court of Justice (ECJ) has previously ruled that only laws equivalent to the EU's are adequate.[6]

U.S. Efforts to Placate the EU's Data-Protection Demands

The past 20 years have seen two extended transatlantic crises on the subject of data protection, and many minor ones. In 2000, the U.S. and the EU negotiated the Safe Harbor agreement, thereby concluding the first crisis; when the ECJ ruled that this agreement was inadequate, the U.S. returned to the table and in 2016 negotiated the Privacy Shield agreement, ending the second crisis. In the midst of these negotiations, the U.S. made a further effort to satisfy the EU with the Judicial Redress Act of 2015, which allows citizens of designated nations to file a civil action against U.S. government agencies that intentionally or willfully violate conditions for disclosing records, or refuse an individual's request to review or amend his or her records. Prominent U.S. attorney and former Assistant Secretary for Policy at the U.S. Department of Homeland Security Stewart Baker described this law as Congress's decision to go from "inactive to supine" in the face of the EU's demands.[7]

The U.S.'s efforts to arrive at a deal that satisfies both sides have not placated the EU. According to the ECJ, the cause of these crises are the U.S.'s 702 authorities, which allow the U.S. government, governed by targeting procedures approved by the U.S. Foreign Intelligence Surveillance Court, to serve orders on data processors that store foreign customers' data in the U.S.[8] Because U.S. firms dominate the online world—at least in the West—the U.S. can access more data than its allies. U.S. court orders are used to detect, prevent, and prosecute criminal and terrorist offenses, and the data obtained through U.S. court orders are relied on by U.S. allies around the world, not least by European nations. Yet in spite of the fact that the U.S. intelligence community is subject to far more publicity, and legal oversight, than its European counterparts, the ECJ and the European Parliament have persistently regarded it—and the U.S. legal system as a whole—as a rogue requiring safeguards that it insists upon nowhere else in the world.

The OECD's Financial Information Sharing Protocol

In spite of the fact that the EU has declared that only a few nations provide European data with "adequate" protection, it has not negotiated agreements comparable to the Privacy Shield with the rest of the supposedly inadequate world.[9] This is not because the rest of the world holds no European data: China, for example, is home to many firms that offer their online services in Europe.[10] Yet the European Commission, the European Parliament, and the ECJ have focused their ire almost exclusively on the intelligence agencies and businesses of the United States.

5. Regulation (EU) 2016/679 of the European Parliament and of the Council, paragraphs 103 and 104 of the preamble.
6. For the ECJ decision, see news release, "The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid," Court of Justice of the European Union, *Press Release* No. 117/15, October 6, 2015, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (accessed December 14, 2017).
7. Stewart Baker, "Time To Get Serious About Europe's Sabotage of U.S. Terror Intelligence Programs," *The Washington Post*, January 5, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/01/05/time-to-get-serious-about-europes-sabotage-of-us-terror-intelligence-programs/?utm_term=.94f4fc836595 (accessed December 14, 2017).
8. News release, "The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid." For an explanation of Section 702, see Paul Rosenzweig, Cully Stimson, and David Shedd, "Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program," Heritage Foundation *Backgrounder* No. 3122, http://www.heritage.org/defense/report/maintaining-americas-ability-collect-foreign-intelligence-the-section-702-program.
9. Outside Europe and the U.S.–EU Privacy Shield, the EU has certified only Argentina, Canada, Israel, New Zealand, and Uruguay as having adequate data-protection standards. See European Commission, "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries," 2017, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed December 14, 2017).
10. Stewart Baker, "Let China and Europe Fight it Out Over Data-Privacy Rights," *The Wall Street Journal*, April 5, 2017, https://www.wsj.com/articles/let-china-and-europe-fight-it-out-over-data-privacy-rights-1491410676 (accessed December 14, 2017). See also Stewart Baker, "The Europocrisy Prize–Coming Soon!" *The Washington Post*, January 22, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/01/22/the-europocrisy-prize-coming-soon/?utm_term=.6c8a5f245ce0 (accessed December 14, 2017).

Curiously, in other contexts, the EU strongly supports data sharing with autocratic regimes, without any meaningful safeguards at all. For example, the OECD, with the support of the EU, is encouraging all nations—not only the members of the OECD—to adopt a regime of financial information sharing.[11] This regime purportedly seeks to discourage tax evasion. It does so by requiring the routine, automatic sharing of bulk taxpayer information—including private tax, banking, brokerage account, and insurance information—of almost all foreign individuals or businesses, or of Americans with foreign bank accounts, to other participating foreign governments.

These governments include China, Russia, Nigeria, and many other regimes that are corrupt, hostile to Western democracy, or both. In short, the EU is backing the creation of a system that would transfer sensitive information about European citizens with dual nationalities or foreign bank accounts, or on refugees, dissidents, or political exiles, to foreign regimes that have every incentive to abuse this information to target individuals—regimes that are unrestrained by their meaningless promises to avoid such abuse.[12]

The EU's hypocrisy in criticizing the U.S. while supporting the OECD regime demonstrates that the point of its data-protection crusade is not to protect European data. It is to play the anti-American card in order to justify giving EU institutions more power at the expense of Europe's nation-states, and—along the way—to do as much damage to successful U.S. firms as possible.

The Coming Challenges of the GDPR

The GDPR and the associated Directive 2016/680 pose four distinct challenges to the U.S. First, the directive appears to clear the way for European data sharing with U.S. authorities for the purposes of fighting crime. But the directive authorizes this sharing only if the nation that is to receive the data has "adequate" safeguards—and the ECJ has already found that the U.S. lacks such controls. The directive also makes provision for international agreements, such as Privacy Shield, which might meet the ECJ's objections. But the GDPR imposes new requirements on the treatment of European data, and it is not yet clear if Privacy Shield meets these requirements. Given the history of politically motivated litigation against the U.S. in the ECJ, it is likely that the GDPR will form the basis for a new legal challenge against Privacy Shield—and if this challenge is successful, European data sharing will come to an end.

Second, the financial penalties that the EU could, as a result of the GDPR, impose on U.S. firms are very large. To take one case, Apple's financial turnover in its 2017 fiscal year was $230 billion. An EU fine of 4 percent would therefore amount to approximately $9.2 billion. This is more than the fine that French bank BNP paid in 2014 as a result of its egregious violations over 10 years of U.S. sanctions on Iran and Sudan, sanctions that derived in part from U.N. Security Council Resolutions.[13] It would be grossly disproportionate for the EU to treat purported misuses of the data of European consumers—data that those consumers willingly provided to the firms that the EU seeks to sanction—to be punished more severely than money-laundering that aided the illicit Iranian nuclear weapons and ballistic missiles programs or Sudan's genocide in Darfur. But that is the result contemplated by the GDPR. Not only will these fines damage U.S. businesses—they will also encourage some businesses to move from the U.S. to the EU, an outcome that the EU would surely welcome.

Third, the GDPR, as trade expert Shanker Singham of the Legatum Institute puts it, is an example

11. The OECD regime has four parts: (1) the amended multilateral Convention on Mutual Administrative Assistance in Tax Matters (the Protocol); (2) the Competent Authority Agreement on Automatic Exchange of Financial Account Information; (3) the OECD Standard for Automatic Exchange of Financial Account Information in Tax Matters; and (4) the OECD Base Erosion and Profit Sharing (BEPS) project.

12. David Burton, "Two Little Known Tax Treaties Will Lead to Substantially More Identity Theft, Crime, Industrial Espionage, and Suppression of Political Dissidents," Heritage Foundation *Backgrounder* No. 3087, December 21, 2015, http://www.heritage.org/taxes/report/two-little-known-tax-treaties-will-lead-substantially-more-identity-theft-crime (accessed December 14, 2017). For the EU's backing, see Organization for Economic Co-operation and Development, Meeting of the OECD Council at Ministerial Level, "Declaration on Automatic Exchange of Information in Tax Matters," May 6, 2014, p. 3, http://www.oecd.org/mcm/MCM-2014-Declaration-Tax.pdf (accessed December 14, 2017).

13. "U.S. Imposes Record Fine on BNP in Sanctions Warning to Banks," Reuters, June 30, 2014, https://www.reuters.com/article/us-bnp-paribas-settlement/u-s-imposes-record-fine-on-bnp-in-sanctions-warning-to-banks-idUSKBN0F52HA20140701 (accessed December 14, 2017). The relevant U.N. Security Council sanctions included Resolution 1591 (2005) on Sudan and Resolutions 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), and 1928 (2010) on Iran.

of regulation that "is disproportionate to its objectives; it is highly prescriptive and imposes substantial compliance costs for business that want to use data to innovate."[14] Around the world, anti-competitive practices and behind-the-borders barriers to trade are on the rise.[15] Indeed, the EU's reaction to the fact that its online businesses have by and large faltered in the face of U.S. competition has not been to improve European competitiveness. Instead, as Singham notes, "the EU has sought to force its regulatory system on the rest of the world (the GDPR is an example of this). If it succeeds, the result would be the kind of wealth destruction that pushes more people into poverty."[16] The GDPR, in short, is not just anti-American: It is anti-innovation, and represents part of the concerted EU effort to reduce regulatory competition between itself and the U.S., and to impose its high-regulation, low-growth model on its most efficient competitors in the United States.

Fourth, the GDPR assumes that the EU has the right to control what everyone around the world does with data that originates from EU citizens, and to subject firms based in other nations to the EU's legal and judicial system. If the U.S. demanded a comparable right, it would be howled down—not least in Europe—as engaging in egregious legal imperialism. Indeed, European authorities have greeted even the U.S.'s financial penalties on European banks for engaging in conduct inside the U.S. that violated U.S. law—and, on occasion, U.N. sanction —with extreme displeasure. Yet the EU is now asserting that it has the right to fine companies that are based in the U.S., which hold their data in the U.S., and which are subject to U.S. law, on the basis of EU rules, and that the EU approach to data protection must be adopted around the world.

What the U.S. Should Do

It is time for the U.S. to end its attempts to satisfy the EU, and to treat the EU with the same firmness and uncompromising clarity that the EU has displayed in its relations with the U.S.

- **The flag must govern data.** The fundamental issue at stake between the U.S. and the EU is whether, as the EU has it, the flag follows the data. The U.S. principle is that data is governed by the flag of the country where it is held, and U.S. courts have upheld this principle.[17] If the EU's approach prevails, the U.S. will have given away part of its legal sovereignty, for it will have conceded that there are in effect two laws for firms dealing with private data in the U.S.—a U.S. law and an EU law. The EU would never concede that U.S. law should operate in the EU, and the U.S. should not concede the reverse. The U.S. should therefore bar the payment by U.S. firms of fines imposed on them for violations (real or purported) of EU data-protection rules pending a comprehensive settlement of this international dispute on the basis of the principle that data is governed by the flag under which it rests. This bar should be imposed on the basis that EU financial penalties are excessive, and that the EU has no right to exert extraterritorial jurisdiction in the United States.[18]

- **Any U.S.–EU trade agreement must respect U.S. sovereignty.** The proposed U.S.–EU trade area known as the Transatlantic Trade and Investment Partnership (TTIP) is on hold, and appears close to collapse. At the EU's insistence, and in another instance of U.S. deference to the EU, the EU's data protectionism was removed from the initial TTIP negotiations. Before negoti-

14. Shanker Singham, "A Narrow-Minded Brexit Is Doomed to Fail," CapX, December 4, 2017, https://capx.co/a-narrow-minded-brexit-is-doomed-to-fail/ (accessed December 14, 2017).
15. World Trade Organization, "Report Urges WTO Members to Resist Protectionism and 'Get Trade Moving Again,'" July 25, 2016, https://www.wto.org/english/news_e/news16_e/trdev_22jul16_e.htm (accessed December 14, 2017).
16. Singham, "A Narrow-Minded Brexit Is Doomed to Fail."
17. "Microsoft Wins Battle with U.S. Over Data Privacy," *Financial Times*, July 14, 2016, https://www.ft.com/content/6a3d84ca-49f5-11e6-8d68-72e9211e86ab (accessed December 14, 2017).
18. These are the same grounds that have led many foreign countries to object to U.S. judgments. The State Department notes that there is "no bilateral or multilateral convention in force between the United States and any other country on reciprocal recognition or enforcement of judgments." The U.S. therefore has no treaty obligation to enforce ECJ or European Commission judgments. See U.S. Department of State, Bureau of Consular Affairs, "Enforcement of Judgments," 2017, https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/internl-judicial-asst/Enforcement-of-Judges.html (accessed December 27, 2017).

ations resume, Congress should pass a joint resolution stating that it will reject any U.S.–EU trade agreement that is not based on the principle that only U.S. laws on data protection apply in the U.S.

- **End all designations under the Judicial Redress Act of 2015.** The Judicial Redress Act of 2015, though well-intentioned, was a unilateral concession that predictably failed to satisfy the EU. The U.S. should end the ability of Europeans (and all other nations) to use it against U.S. agencies by removing all designations made under it. Any future designations should come only as part of a comprehensive and final settlement of all data-protection disputes between the U.S. and the EU (or other nation or nations concerned).[19]

- **Establish a principle of share and share alike on counterterrorism data.** European counterterrorist agencies rely heavily on data collected by their U.S. counterparts. President Donald Trump should make it publicly clear that if the EU cuts off data sharing under the GDPR, or under Directive 2016/680, the U.S. will immediately end the routine sharing of counterterrorism data with European authorities, and will cooperate only at times, in cases, and with authorities of its own choosing. A public statement will make it clear to the European Parliament, the European Commission, and the ECJ—all of whom have few if any responsibilities for countering terrorism—that their actions will have wide-ranging consequences. The U.S. should help those who seek to collaborate honestly—but if the EU chooses to stand on its own in the realm of data, it should be left to confront its numerous Islamists without the benefit of U.S. assistance. Agreements such as the U.S.–U.K. Data Agreement should continue if U.S. data sharing is cut off as a result of EU actions.[20]

Conclusion

The true remedy for the EU's complaints is for it to undertake reforms that allow EU data firms to grow, to compete on price and service with U.S. companies, and thereby to build up a data industry that operates under EU law. There is no doubt that individual privacy is important, and that—subject to the need to detect and prevent crime, a process that must be supervised by warrants provided by legitimate authorities—personal data should belong to the individual. Equally, there is room for real and serious disagreement about how these principles should be embodied in law. For well over a decade, the U.S. has sought to reach a fair agreement with the EU about data protection that addresses these questions.

This effort has repeatedly failed because the EU has persistently and hypocritically raised the bar in its demands on the U.S.—and only on the U.S. The EU sees no problem when European data is transferred to China or Russia: It is only when the U.S. is concerned that the EU presses its demands for data protection. The U.S. has approached the EU as a friend, but it has been treated worse than China. It is therefore time for the U.S. to stop being played for a fool, to recognize the EU's hostility, and—before the GDRP takes effect—to take measures that will force the EU to recognize that the U.S. will not stand by as the EU exerts legal authority over U.S. firms that have the temerity to be commercially successful.

*—**Ted R. Bromund, PhD,** is Senior Research Fellow in the Margaret Thatcher Center for Freedom, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

19. To date, only the EU and 26 of its member nations have been designated. See U.S. Department of Justice, "Judicial Redress Act of 2015," 2017, https://www.justice.gov/opcl/judicial-redress-act-2015 (accessed December 14, 2017).
20. "UK–US Pact Will Force Big Tech Companies to Hand Over Data," *Financial Times*, October 23, 2017 https://www.ft.com/content/09153a74-b5bc-11e7-aa26-bb002965bce8 (accessed December 14, 2017). The EU directives do not bind the U.K. in certain areas of judicial cooperation in criminal matters or police cooperation.