Forget You! And Forget Me, Too

Written by Taliah Coe, WWU International Business Student
December 7, 2021

Introduction

In an increasingly technologically-dominated world, consumers and firms alike struggle to regulate this dynamic landscape. Every industry relies on international data flows, which enable everything from online communication to global supply chain management. Highly globalized and interconnected economies, however, demand serious consideration of the potential for government surveillance and corporate abuse. Data brokerage and personal information sales have become lucrative industries directly affecting consumers who desire greater protection.[1] As a result, corporations grapple with the increasing frequency of cyberattacks and the growing demand for ethical information management.[2] The newly introduced "right to be forgotten" is one manifestation of expanding data privacy legislation in Europe. The importance of data protection in international trade deals grows exponentially, thus the lack of uniformity across EU-US privacy regulation requires immediate attention. Nationally, the US must accept Europe as a first-mover in data regulation and create federal policies that reflect the level of protection afforded to EU users. US state governments must also initiate and pass their own consumer data protection legislation rather than waiting for Congress to lead.

Europe's General Data Protection Regulation

Privacy regulations are evolving with a marked shift toward safeguarding consumers and the historic right to be forgotten legislation reflects this. The concept was first introduced by the European Union in 2014 but the General Data Protection Regulation (GDPR) and Article 17 were created and implemented in May 2018.[3] Also known as the right to erasure, this provision within Europe's new data privacy and security law affords data subjects the right to request that search engine operators delist URLs that contain "inaccurate, inadequate, irrelevant, or excessive information through searches with a person's name."[4] It defines a data subject as a person who can be distinguished by reference to a name, number, location, or by identity factors.[5] It is important to note that the GDPR does not provide a general right to erasure but rather a limited right under specific circumstances.[6] Companies like Google, Bing, and Yahoo must grant erasure when one of the following applies: personal data is no longer necessary concerning the reason it was collected; personal data has been unlawfully processed; or the data subject withdraws consent upon which the processing is based, among a few others.[5] It also stipulates that data collectors—entities possessing personal information—verify the data subject's identity then promptly erase information. The GDPR entitles consumers to a greater degree of accessibility and control over their data, but also creates a bureaucratic nightmare with significant gray areas.

By the same token, an organization's right to process someone's data may override their right to be forgotten. The GDPR outlines several situations that eclipse an individual's right to erasure: the data is being used to exercise freedom of expression and information; the data is being used to comply with a legal ruling; the data represents important information that serves

[1] Fast Company, "The data brokers buying and selling information," Melendez and Pasternack, March 2, 2019
[2] FORBES, "Alarming Cybersecurity Stats for 2021," Chuck Brooks, March 2, 2021
[3] GDPR.EU, "Everything you need to know about the 'Right to be forgotten'"
[4] Media Laws, "Google and the Right to be Forgotten," Giacomo Bertelli, April 2, 2020
[5] Lexology, "Data Privacy and cybersecurity in global dealmaking," Polk and Wardell, October 20, 2021
[6] BLG, "The right to erasure of personal information," Gratton, Nagy, and Du Perron, May 28, 2021

the public interest, scientific or historical research, or statistical purposes; or the data is being used for the establishment of a legal defense, to name a few.[3] This opens the door to conflicting ideas regarding meaning and interpretation, as well as assumptions about intention. The GDPR fails to outline a correct procedure for submitting erasure requests, leaving a crucial part of implementation open-ended. In like manner, a determination is left to search engine operators as to whether an individual's right to privacy outweighs the public's right to access information when delisting URLs.[4] This allowance is reminiscent of countries' ability to self-determine developed or developing status in the World Trade Organization and creates similarly heated debate.

These issues point to ongoing conflict regarding the extent of oversight that search engines and tech companies require and how best to regulate them. While the right to be forgotten provides a glimmer of hope for greater consumer data protection within the EU, questions remain about how to achieve desired transparency on the GDPR. In typical ambiguous fashion, Google Reports only states that "each request is manually reviewed and assessed on a case-by-case basis" with no further detail.[7] Some data privacy experts have made the case for requests to be reviewed by an independent authority as well.[8] Human rights and civil liberties organizations are demanding clarity on how search engine operators arrive at decisions to grant or refuse requests for erasure. This month, allegations were made that the right to be forgotten was wielded inappropriately by former billionaire Seán Quinn to delist family press coverage in Ireland.[9] Wealthy public figures appear to have seized the opportunity to use Article 17 for reputation management.

Implications for Trade

Article 17 has escalated tensions between the United States and the European Union over how to regulate data privacy because regulations in the two economies differ greatly. The original 2016 EU-US Privacy Shield outlined data protection requirements when transferring personal data and supported regularity in Trans-Atlantic commerce.[10] In July 2020, the Court of Justice of the EU (CJEU) invalidated the privacy shield, citing the fact that protection for US consumers was not equivalent to that of European citizens under the EU Charter of Fundamental Rights.[11 and 12] The CJEU took issue with the allotted scope of national intelligence and collection of foreign intelligence via communications systems.[13] The original EU-US privacy shield also lacked a right to redress through oversight or compliance enforcement in the form of an independent and impartial body. When the European court struck down the agreement, it reopened data privacy tensions between the US and the EU and placed the $6.2 trillion EU-U.S. trade relationship in jeopardy.[13] In March, the Biden Administration announced an effort to

[7] Google Transparency Report, "Requests to delist content under European privacy law," November 14, 2021
[8] Independent.ie, "Right to erasure brings as many questions as answers," November 8, 2021
[9] The articles delisted from the search engine included past coverage of the family's lifestyle and their involvement in extensive court battles in the fallout of the financial crash. The URLs requested to be removed were granted by Google. Irish Times, "Right to be forgotten should be reviewed after use by Quinns," Jack Power, November 7, 2021
[10] ITA, U.S. Department of Commerce, "Privacy Shield Overview"
[11] The court determined that the Privacy Shield transfer mechanism did not comply with the level of protection required by European Union law. European Commission. "EU-US Privacy Shield"
[12] Bloomberg Law, "Seeking Smooth Sailing for Data Flows Across the Pond," Mark Smith, November 1, 2021
[13] Brookings, "Trans-Atlantic data flows," Emily Skahill, July 29, 2021

"intensify negotiations" on an updated EU-U.S. Privacy Shield but concrete action remains forthcoming.[14]

Recommendations

Two possible solutions present themselves concerning the precedent set by the right to be forgotten. The first is congressional legislation similar to the General Data Protection Regulation in order to address digital privacy at the national level. As aforementioned, the European Union is a major economic partner, and the passage of a federal consumer privacy law between two powerful economies would set a precedent in data protection standards globally.[12] Such a deal would also build confidence about the durability of data transfer between businesses on each side of the Atlantic. While the United States missed the chance to be the leader in data protection, it still can signal the importance of ethical technology use to other G20 countries. The downside to an American GDPR equivalent would be the surveillance reforms that the CJEU desires and the humility this would require from the U.S. government. The CJEU striking down the US-EU Privacy Shield could easily be viewed as a threat to U.S. autonomy and might cause lawmakers to fume over requests from an international court. While most ideal, this option is unlikely since Congress failed to advance many holistic data privacy and security proposals over the past few years.[15] The US federal government generally relies on a sector-based approach to data regulation that focuses on high-risk industries, like healthcare and financial services, rather than broad reform.[16 and 17]

The second solution is policy reform at the state government level, such as the 2018 California Consumer Protection Act. The CCPA is similar to the GDPR in many regards and includes the right to be forgotten, along with expanded protections for California residents, and severe civil penalties and statutory damages for violations.[15] This option is much more feasible, as legislation moves faster and is passed at higher frequencies at the state level.[18] It is also possible that stringent state regulatory standards adopted in one state could spread to others, motivating multinational tech companies to adjust all jurisdictions to a higher standard. It is often costly and complicated to treat consumers differently in various locations.[19] This "California Effect," the shift of regulation towards economic jurisdictions with stricter standards, is a double-edged sword since it can exasperate consumers who prefer low standards of protection to keep costs down.[20 and 21]

Conclusion

In summation, there are several actionable steps that the US and EU governments can take today that will amplify the economic benefits of cross-border data transfers. US political leaders must accept that the EU leads the data privacy charge, but more importantly that the

---

[14] U.S. Department of Commerce, "Intensifying Negotiations on Trans-Atlantic Data Privacy Flows," Gina Raimondo, March 25, 2021

[15] Lexology, "Data Privacy and cybersecurity in global dealmaking," Polk and Wardell, October 20, 2021

[16] The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

[17] The Gramm-Leach-Bliley Act of 1999 (GLBA) or The Financial Services Modernization Act of 1999

[18] State legislatures introduce 23x more bills than the U.S. Congress does. Quorum, "State Legislatures Vs. Congress"

[19] ScienceDirect, "Exporting Standards," Anu Bradford, June 2015

[20] California Effects are situations where stringent regulatory standards adopted in one jurisdiction spread to other jurisdictions, increasing consumer protection everywhere. The term was coined by David Vogel in his 1997 book *Trading Up*.

[21] ProMarket, "Is there a California Effect in Data Privacy Law?," Jens Frankenreiter, October 21, 2021

American economy only stands to benefit from finding common ground on privacy protections. There is demonstrable value in the US creating GDPR-adjacent legislation and has to begin with the Biden Administration making good on its promise to negotiate a new US-EU Privacy Shield. Due to Congress' sluggish legislative pace, using executive orders to compose a new data agreement and to address the CJEU's national security concerns would be far more effective. The US government must recruit and seek the council of leading American economists and lawyers in this process, and also work with European experts to author a Privacy Shield replacement. In turn, the EU and its many governments must be open to collaborative, democratic efforts to develop a new consumer data protection agreement. Presidents and prime ministers must lead by example and inform the public that federal consumer privacy standards are the best strategy to preserve Trans-Atlantic trade relationships. They ensure that both the American and European economies maximize competitiveness in the global economy.