The American Journal of Bioethics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uajb20

The Ethical Data Practices Framework and Its Implications for Data Privacy Relations between the United States and the European Union

Vasiliki Rahimzadeh

To cite this article: Vasiliki Rahimzadeh (2023) The Ethical Data Practices Framework and Its Implications for Data Privacy Relations between the United States and the European Union, The American Journal of Bioethics, 23:11, 29-33, DOI: 10.1080/15265161.2023.2256618

To link to this article: https://doi.org/10.1080/15265161.2023.2256618

Published online: 25 Oct 2023.

protection legislation, it can learn from the experiences of other governments and become a worldwide leader in laws that appropriately balance corporate interests and consumer protections. Creating a federal Data Protection Agency is a step in that direction.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

FUNDING

The author(s) reported there is no funding associated with the work featured in this article.

ORCID

Efthimios Parasidis http://orcid.org/0000-0002-8565-119X

REFERENCES

Alder, S. 2023. Revised American Data Privacy and Protection Act due to be released. *The HIPAA Journal*, April 14.

Barnes, L. G. 2015. How mandatory arbitration agreements and class action waivers undermine consumer rights and why we need Congress to Act. *Harvard Law & Policy Review* 9 (2):329–54.

Childress, J. F., R. R. Faden, R. D. Gaare, L. O. Gostin, J. Kahn, R. J. Bonnie, N. E. Kass, A. C. Mastroianni, J. D. Moreno, and P. Nieburg. 2002. Public health ethics: Mapping the terrain. *The Journal of Law, Medicine & Ethics* 30 (2):170–8. doi: 10.1111/j.1748-720x.2002.tb00384.x.

Godlasky, A. 2022. Data Privacy Act has Bipartisan support. But … *National Press Foundation*, November 30.

H.R. 8152. 2021–2022. American Data Privacy and Protection Act, 117th Congress.

McCoy, M. S., A. L. Allen, K. Kopp, M. M. Mello, D. Patil, P. Ossorio, S. Joffe, and E. J. Emanuel. 2023. Ethical responsibilities for companies that process personal data. *The American Journal of Bioethics* 23 (11):11–23. doi: 10.1080/15265161.2023.2209535.

Parasidis, E., E. Pike, and D. McGraw. 2019. A Belmont Report for health data. *The New England Journal of Medicine* 380 (16):1493–5. doi: 10.1056/NEJMp1816373.

Pike, E. R. 2020. Defending data: Toward ethical protections and comprehensive data governance. *Emory Law Journal* 69 (4), 687–743.

S.2134. 2021–2022. Data Protection Act of 2021, 117th Congress.

S.3300. 2019–2020. Data Protection Act of 2020, 116th Congress.

THE AMERICAN JOURNAL OF BIOETHICS
2023, VOL. 23, NO. 11, 29–33
https://doi.org/10.1080/15265161.2023.2256618

Taylor & Francis
Taylor & Francis Group

OPEN PEER COMMENTARIES

Check for updates

The Ethical Data Practices Framework and Its Implications for Data Privacy Relations between the United States and the European Union

Vasiliki Rahimzadeh

Baylor College of Medicine, Center for Medical Ethics and Health Policy

Private companies are data-rich. But market pressures to collect more, store more, and analyze more consumer data can often make them ethically bankrupt in the way of proactively protecting consumer data privacy rights. The recognized need to codify data privacy rights into law as global commerce and compute power exploded in the 2000s were foundational motivations for establishing a new privacy regime within the European Union (EU). Since its enforcement in 2018, the General Data Protection Regulation (GDPR) has since become a beacon for omnibus data privacy and protection law (Dove 2018). While only applicable to processing and controlling data involving citizens of EU Member States (Becker et al. 2022), the GDPR has nevertheless shaped privacy policies and norms worldwide, including in the United States. Indeed,

CONTACT Vasiliki Rahimzadeh Vasiliki.Rahimzadeh@bcm.edu Center for Medical Ethics and Health Policy, Baylor College of Medicine, Houston, TX, USA.

GDPR's legislative influence is evident in State-based consumer privacy laws in California, Virginia, Connecticut, and Colorado, among others (US State Privacy Legislation Tracker 2023). Some have argued a GDPR-inspired regulation in the U.S. should be endeavored (Nayyar 2023), and that establishing "one comprehensive privacy standard worldwide for the collection and processing of personal data" (Voss and Houser 2019) should be an international regulatory priority. Yet differences in regulatory approaches to federal data privacy, protection, and security between the United States and the EU have grown starker since GDPR, and at times have significantly strained the transatlantic transfer of personal data.

The *Ethical Data Practices Framework* advanced in the target article by McCoy et al. (2023) is timely in the political history of data privacy relations between the EU and U.S. The authors take a pragmatic approach to helping companies respect substantive - minimizing harm, fairly distributing benefits and burdens, and respecting individual autonomy - as well as procedural - transparency, accountability, and inclusion - ethical principles in routine company operations that involve processing and sharing personal data. Five imperatives activate these principles in practice, including

- Minimize collection and retention of personal data;
- Offer fewer but more meaningful choices about data;
- Provide meaningful disclosure;
- Assess the social impact of data practices; and
- Ensure meaningful stakeholder engagement (McCoy et al. 2023).

In what follows, I provide a brief historical accounting of the past 20 years of data privacy negotiations between the U.S. and EU. I weave in commentary about the implementation potential and challenges of self-governing frameworks like the *Ethical Data Practices Framework* to sustaining healthy data privacy relations between these economic powers moving forward. I draw on findings from ongoing empirical work to justify why accountability mechanisms, in specific, are needed to orient companies toward the ethical data practices we know individuals want and care about.

SAFE HARBOR (2000–2014)

Regulation (EU) 2016/6792 sets out the rules for the transfer of personal data from controllers or processors in the EU to other countries. Legislators further acknowledged that such data flows are "essential for the expansion of cross-border trade and international cooperation," insofar as "the level of protection afforded to personal data in the Union must not be undermined by transfers to third countries or international organisations." Article 45(3) of the same Regulation grants the European Commission the authority to determine whether "a third country, a territory or *one or more specified sectors* (emphasis added) within a third country, ensure(s) an adequate level of protection" that is functionally equivalent to the protections afforded under the GDPR. The adequacy of protections for inbound personal data transfers from the EU to the US has been legally challenged no fewer than three times, and the U.S. has struggled to maintain its adequacy status ever since.

The Safe Harbor arrangement was among the earliest official data privacy agreements between the U.S. and EU. It was enacted in July 2000, and was administered by Department of Commerce and enforced by the U.S. Federal Trade Commission (FTC). Under Safe Harbor, U.S. companies could voluntarily sign onto the arrangement if they self-certified with the Department of Commerce that company privacy policies incorporated the Safe Harbor Privacy Principles and agreed to make these policies transparent. After more than a decade in effect, the EU Parliament invalidated Safe Harbor in March 2014. In that instance, private U.S. companies were chiefly to blame. U.S. intelligence agencies that unlawfully processed personal data on account of national security were also found to violate the Safe Harbor terms.

Parliament's decision to end Safe Harbor rested in part on the ineffectiveness of self-certification and the FTC's failure to hold companies accountable for Safe Harbor violations among private U.S. companies. The events that led to Safe Harbor's dissolution is consequential, in my view, for the implementation potential of the *Ethical Data Practices Framework* because the *Framework* similarly relies on companies to self-monitor their activities according to the practices outlined therein. History could be a prophetic tool here. If U.S. companies were willing to violate legally binding privacy terms overseen and enforced by their own national regulators then, what has changed to compel companies to adopt voluntary data ethics practices and track their own progress on them now? It is therefore skeptical that ethically rigorous and practically-informed frameworks, which I consider the *Ethical Data Practices Framework* to be, can fully achieve their goals without strong accountability measures attached.

EXPECTATION OF ACCOUNTABILITY

A practical imperative that helps keep firms accountable to the social impacts of their data practices seem to be absent from the list McCoy and colleagues suggest. An embedded mechanism for accountability could be a natural outgrowth of practical imperative (4) *Assess the social impact of data practices* and would ideally establish penalties for, as well as track progress on the corrections made when firms "burden, exclude, exploit, or discriminate against members of disadvantaged groups."

The authors identify data access committees (DAC) as one oversight body that could counteract this exploitation, exclusion, and discrimination in a company's data practices. Companies that establish their own DAC would be borrowing from oversight models that are more typified in the public sector, including research institutions like the NIH (see for example (Data Access Committee - National Institute of Allergy and Infectious Diseases 2023; Database of Genotypes and Phenotypes (dbGaP) - Data Access Committee 2023; NIMH Data Archive - CCF 2023). DACs are charged with ensuring only authorized users access appropriately permissioned data for ethically approved purposes (Cheah and Piasecki 2020). I found in my own stakeholder-engaged research with data access committees and institutional stewards of genomic data that DACs rarely solicit "input from users or affected groups" or include community representatives in decisions related to data access and use (manuscript forthcoming). Nor would adding such representatives to DAC membership necessarily guarantee ethical secondary use for all data accessed. US- and EU-based DACs are commonly misunderstood as ethics and inclusion bodies when they are actually compliance bodies (Lawson et al. 2023), for better or for worse. At present, DACs are less than ideal sites for stakeholder engagement, and tasking them with holding companies accountable for the social impacts of company data practices may be misplaced.

History, again, may provide important insight. When leadership and organizational changes were announced at Twitter and Facebook, ethics teams were first to be let go (Knight 2023).

The literature on AI ethics and related algorithmic justice initiatives exemplify how difficult implementation is proving to be (Jobin, Ienca, and Vayena 2019). This implementation gap in AI ethics ties directly to an accountability gap whereby just identifying what is ethical practice is a substantial task for companies, let alone strategizing how to embed them into workflows post hoc.

U.S. – EU PRIVACY SHIELD (2016–2020)

It took more than two years for the EU and U.S. to strike a new transatlantic data transfer agreement after the fall out of Safe Harbor. The resulting U.S.-EU Privacy Shield (EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield 2023) strengthened data protection obligations for U.S. companies and established stricter monitoring protocols for the U.S. regulators. It also clarified the conditions of use, limitations, and oversight of EU personal data on behalf of U.S. public authorities and established new redress possibilities for Europeans to levy civil complaints against unlawful data processing or controlling by U.S. offenders. In the absence of a formal adequacy decision, U.S. based companies could benefit from data transfer privileges *as if* they had an adequacy designation. Using standard contractual clauses allowable under the U.S.-EU Privacy Shield, U.S. companies that self-certified could receive, transfer and process personal data from the EU insofar as they honored the rights of EU citizens to know, correct and delete personal information collected about them, among other requirements. The Privacy Shield furthermore codified the *de minimis* principle and eliminated indefinite storage, whereby only information that was necessary and proportionate for a specific business purpose could be stored.

These restricted data transfer privileges were, however, short-lived when, in July 2020, the Court of Justice of the European Union suspended the Privacy Shield. Legislators argued the Privacy Shield inadequately protected EU citizens from unlawful surveillance by U.S. federal intelligence and law enforcement agencies. The U.S. had been without a recognized EU data transfer agreement until July 10, 2023.

EU-U.S. DATA PRIVACY FRAMEWORK (2023-)

According to the European Commission's latest decision, the US ensures an "adequate level of protection—comparable to that of the European Union—for personal data transferred from the EU to US companies under the new EU-U.S. Data Privacy Framework (Commission Implementing Decision: Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework 2023). The new Privacy Framework enables safe data flows safely from the EU to US companies participating in the Framework, without requiring additional data protection safeguards (Adequacy decision for safe EU-US data flows 2023)

but instead introduces new binding safeguards. It also restricts access to EU data for US intelligence services only to what is "necessary and proportionate," and establishes a new legal remedy for EU individuals through the Data Protection Review Court (DPRC). Legislators claim the "new safeguards in the area of government access to data will complement the obligations that US companies importing data from EU will have to subscribe to" (Adequacy decision for safe EU-US data flows 2023) and will order the immediate deletion of personal data found to be in violation of the new Framework.

In this way, McCoy and colleagues could use new EU-U.S. Data Privacy Framework as a complementary source for practical guidance as it offers a U.S. translation of sorts for general data protection principles.

WRITING THE NEXT CHAPTER OF PRIVACY RELATIONS BETWEEN THE U.S. AND EU

While *Ethical Data Practices Framework* would have no legal bearing on transatlantic data transfers, it could result in reputational gains for companies that overall make the U.S. a more trustworthy destination for EU data.

Demonstrating why firms should treat regulatory compliance with data privacy laws as the floor, rather than the ceiling of good business practice is critical to aligning those practices with public values on ethical data sharing and use. The *Ethical Data Practices Framework* provides a starting point for firms in this regard, but additional tools are needed to substantiate this value proposition. For example, what effect does the adoption of a *de minimis* approach to consumer data collection and processing have on revenues? Do improved transparency practices improve consumer retention or confer specific advantages in a competitive market space? Clearer answers to these questions will help firms marshal support around the practices McCoy and colleagues propose, enriching opportunities for the public and firms to benefit proportionately.

ACKNOWLEDGEMENT

I wish to thank Adrian Thorogood for his conceptual and editorial support while drafting earlier versions of this article.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

FUNDING

This study is funded by National Human Genome Research Institute (No. 1K01HG013112).

ORCID

Vasiliki Rahimzadeh http://orcid.org/0000-0003-3537-7601

REFERENCES

Adequacy decision for safe EU-US data flows. 2023. Text. *European Commission - European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721. (Accessed August 17, 2023).

Becker, R., D. Chokoshvili, G. Comandé, E. Dove, A. Hall, F. Molnár-Gábor, P. Nicolas, S. Tervo, and A. Thorogood. 2022. Secondary use of Personal Health Data: When is it "Further Processing" under the GDPR, and what are the Implications for Data Controllers? https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4070716

Cheah, P. Y., and J. Piasecki. 2020. Data Access Committees. *BMC Medical Ethics* 21 (1):12. doi:10.1186/s12910-020-0453-z.

Commission Implementing Decision: Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. 2023. Available from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf. (Accessed August 17, 2023).

Data Access Committee - National Institute of Allergy and Infectious Diseases. 2023. March 15.

Database of Genotypes and Phenotypes (dbGaP) - Data Access Committee. 2023. https://www.ncbi.nlm.nih.gov/projects/gap/cgi-bin/about.cgi#dac. (Accessed August 17, 2023).

Dove, E. S. 2018. The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *Journal of Law, Medicine & Ethics* 46 (4):1013–30. doi:10.1177/1073110518822003.

EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. 2023. Text. *European Commission - European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216. (Accessed August 17, 2023).

Jobin, A., M. Ienca, and E. Vayena. 2019. The global landscape of AI ethics guidelines. *Nature Machine Intelligence* 1 (9)Nature Publishing Group :389–99. doi:10.1038/s42256-019-0088-2.

Knight, W. 2023. Elon Musk Has Fired Twitter's 'Ethical AI' Team. *Wired*. https://www.wired.com/story/twitter-ethical-ai-team/. (Accessed August 18, 2023).

Lawson, J., V. Rahimzadeh, J. Baek, and E. S. Dove. 2023. Achieving Procedural Parity in Managing Access to Genomic and Related Health Data: A Global Survey of Data Access Committee Members. *Biopreservation and Biobanking* bio.2022.0205. doi:10.1089/bio.2022.0205.

McCoy, M. S., A. L. Allen, K. Kopp, M. M. Mello, D. J. Patil, P. Ossorio, S. Joffe, and E. J. Emanuel. 2023. Ethical responsibilities for companies that process personal data. *The American Journal of Bioethics* 23 (11): 11–23. doi:10.1080/15265161.2023.2209535.

Nayyar, S. 2023. Is It Time For A U.S. Version Of GDPR? *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/02/01/is-it-time-for-a-us-version-of-gdpr/. (Accessed August 29, 2023).

NIMH Data Archive - CCF. 2023. https://nda.nih.gov/ccf/data-access-committee.html. (Accessed August 17, 2023).

US State Privacy Legislation Tracker. 2023. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/. (Accessed August 17, 2023).

Voss, W. G., and K. A. Houser. 2019. Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal* 56 (2):287–344. doi:10.1111/ablj.12139.

THE AMERICAN JOURNAL OF BIOETHICS
2023, VOL. 23, NO. 11, 33–35
https://doi.org/10.1080/15265161.2023.2256254

Taylor & Francis
Taylor & Francis Group

OPEN PEER COMMENTARIES

Responsible Processing and Sharing of Genomic Data: Bringing Health Technologies Industries to the Table

Bartha Maria Knoppers[a], Shane Chase[b], Yann Joly[a], Ma'n Zawati[a], and Adrian Thorogood[c]

[a]McGill University; [b]Illumina; [c]Terry Fox Research Institute

The article "Ethical Responsibilities for Companies that Process Personal Data" (McCoy et al. 2023) provides a principled and pragmatic ethical framework for companies collecting, sharing, and using personal data in the United States. Filtered through the classical Belmont Report ethical principles for research with human subjects, the framework offers a concrete and flexible basis for industry self-regulation, consumer awareness and activism, and eventual government regulation. The authors also helpfully translate the principles into a concise and practical checklist to support ethics (self-assessments) with general applicability. Practical recommendations include minimizing data processing to only what is necessary to achieve defined purposes; providing consumers with more compact and meaningful choices about how their data are processed; providing plain language disclosures to inform consumers; conducting social impact assessments that consider risks beyond individual privacy; and ensuring meaningful involvement of stakeholders in data governance.

McCoy et al.'s ethical framework shares a common purpose with the recent *International Genomic Data Sharing by Health Technologies Industries: Points to Consider* (Knoppers et al. 2023) developed by McGill University's Center of Genomics and Policy, in consultation with 11 international companies from diverse industry sectors (listed in Table 1). This framework for industry highlights similar principles and practice guidance, albeit focused on the processing and sharing of human genomic and related health data internationally by health technologies industries (HTI). HTI include pharmaceutics, sequencing platforms, clinical genomics, direct-to-consumer genetic testing, digital health data management, cloud computing, advanced analytics and AI, and digital health and engagement platforms.

McCoy et al.'s ethical framework builds on the principles of the Belmont Report and is directed at US companies processing personal data. The PtC, by contrast, has an international grounding and seeks to apply to the activities of HTI globally. The PtC builds on the international *Framework for Responsible Sharing of Genomic and Health-Related Data* of the Global Alliance for Genomics and Health (GA4GH 2014). The GA4GH is an international alliance that

CONTACT Bartha Maria Knoppers bartha.knoppers@mcgill.ca Centre of Genomics and Policy, McGill University, Montreal, Canada.