The executive order, Secretary of the Treasury Janet L. Yellen, chair of CFIUS, noted, "highlights CFIUS's increasing attention to national security risks in several key areas and sharpens the Committee's focus on protecting America's national security, while maintaining the U.S. open investment policy."[48] Together with the new enforcement and penalty guidelines, the order, according to the White House, "send[s] a very clear message, a public message, to the private sector . . . about what are some factors that we as an administration are very focused on."[49] It also sends a message to "the public as a whole, as well as foreign governments, allies, and partners around the world."[50] Part of a broader set of actions, the order "explicitly ties CFIUS's role, actions, and capabilities with the Administration's overall national security priorities."[51] It is a part, as well, of a transnational proliferation of heightened investment screening.[52]

International Human Rights and Humanitarian Law

The United States and the European Union Begin Implementation of the European Union-U.S. Data Privacy Framework

doi:10.1017/ajil.2023.17

On October 7, 2022, President Joseph R. Biden, Jr. signed Executive Order 14,086 on Enhancing Safeguards for United States Signals Intelligence Activities[1] to implement the EU-U.S. Data Privacy Framework (DPF) that was "agreed in principle" on March 27, 2022.[2] The DPF seeks to address issues identified by the Court of Justice of the European Union (CJEU) in *Schrems II* (2020), which struck down the European Commission's adequacy decision approving the Privacy Shield, the prior legal framework for transferring EU personal data

[48] U.S. Dep't of the Treasury Press Release, Statement by Secretary of the Treasury Janet L. Yellen on President Biden's Executive Order on the Committee on Foreign Investment in the United States (Sept. 15, 2022), *at* https://home.treasury.gov/news/press-releases/jy0951 [https://perma.cc/AL6P-ZFZD].

[49] White House Press Release, Background Press Call on President Biden's Executive Order on Screening Inbound Foreign Investments (Sept. 14, 2022), *at* https://www.whitehouse.gov/briefing-room/press-briefings/2022/09/15/background-press-call-on-president-bidens-executive-order-on-screening-inbound-foreign-investments [https://perma.cc/7RVG-QXRN].

[50] *Id.*

[51] Fact Sheet, *supra* note 2.

[52] *See, e.g.*, National Security and Investment Act 2021 (c. 25) (UK); Regulation 2019/452 Establishing a Framework for the Screening of Foreign Direct Investments into the Union, 2019 OJ (L 79) I; Foreign Investment Reform (Protecting Australia's National Security) Act 2020 (Austl.).

[1] Enhancing Safeguards for United States Signals Intelligence Activities, Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022) [hereinafter EO 14,086]. Separately, on December 14, 2022, the United States and other governments agreed to the OECD's Declaration on Government Access to Personal Data Held by Private Sector Entities, *at* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487 [https://perma.cc/4AAR-54A4].

[2] White House Press Release, Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (Oct. 7, 2022), *at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework [https://perma.cc/B5LZ-RN3N] [hereinafter Fact Sheet]. When the framework was first announced, it was called the Trans-Atlantic Data Privacy Framework. *See* note 3 *infra*.

to the United States.[3] The European Commission anticipates issuing an adequacy decision concluding that U.S. law now achieves the standards required by EU law (a draft decision was published in December). After that decision enters into force, U.S. entities will be permitted to transfer personal data from the EU to the United States under clear rules, unless the CJEU rejects the decision when it is inevitably challenged. According to the White House, the "EU-U.S. DPF [when implemented] will restore an important legal basis for transatlantic data flows," which is "critical to enabling the $7.1 trillion EU-U.S. economic relationship."[4]

EU law restricts the transfer of personal data outside of the European Union absent assurances that the data will be protected abroad in accordance with the conditions established by the General Data Protection Regulation (GDPR).[5] One method for providing such assurances is an "adequacy decision," in which the European Commission certifies that rules and procedures are in place in a given third country that "ensure[] an adequate level of protection" for the EU personal data that is to be transferred.[6] Provided a third-country company follows its country's approved rules (in the United States this would be by committing to comply with specified privacy principles through annual self-certification to the Department of Commerce), they may transfer personal data from the European Union. An adequacy decision thus simplifies and creates certainty for companies whose data transfers are regulated by EU law. But an adequacy decision requires not just the Commission to conclude that the third country's rules meet the required threshold for data protection set by the GDPR. If the Commission's decision is challenged, the CJEU must do so as well. As will be explained below, the CJEU has twice determined that U.S. law does not meet EU legal requirements, invalidating the Commission's adequacy decisions.

In the absence of an adequacy decision, there are other ways for third-country companies to comply with the GDPR's data transfer rules.[7] They may, for example, establish Binding Corporate Rules (BCR) that are approved by the competent EU data protection authority.[8] And they may use EU-issued Standard Contractual Clauses (SCC), as many companies do.[9] But these mechanisms may be deemed insufficient for much the same reason that the adequacy decisions were faulted: that U.S. law does not match EU standards and the SCCs (and the other methods that could demonstrate that the transfers were subject to

[3] White House Press Release, Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (Mar. 25, 2022), *at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework [https://perma.cc/CRP5-EYL4]; Eur. Comm'n Press Release, European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework (Mar. 25, 2022) *at* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 [https://perma.cc/8F87-VT8V].

[4] Fact Sheet, *supra* note 2.

[5] *See* General Data Protection Regulation, Art. 44, 2016 OJ (L 119) 1, at 41, *at* http://data.europa.eu/eli/reg/2016/679/2016-05-04 (effective 2018) [hereinafter GDPR]. The GDPR replaced the Data Protection Directive, 1995 OJ (L 281) 31 (effective 1998) [hereinafter DPD]. The Data Protection Directive also required that third countries ensure an adequate level of protection of EU personal data. *See id.* Art. 25(1).

[6] GDPR, *supra* note 5, Art. 45(1); *see also* DPD, *supra* note 5, Art. 25(6).

[7] *See* GDPR, *supra* note 5, Arts. 46–47.

[8] Eur. Comm'n, Binding Corporate Rules (BCR), *at* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en [https://perma.cc/6TM9-LG2N].

[9] Eur. Comm'n Press Release, European Commission Adopts New Tools for Safe Exchanges of Personal Data (June 4, 2021), *at* https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847 [https://perma.cc/48AE-6ULC].

https://doi.org/10.1017/ajil.2023.17 Published online by Cambridge University Press

appropriate safeguards) do not include sufficient "additional measures" to compensate for the deficiencies.[10] Many European national data protection authorities, for example, have so concluded in complaints brought against European companies for their use of Google Analytics.[11] It is anticipated that a pending decision against Meta Industries in Ireland will come to the same conclusion.[12] This means that there may be no workable legal basis for EU-U.S. personal data transfers under EU law.

While some companies, like Microsoft, might be able to allow their European customers to store their data locally (data localization) and therefore avoid transfers out of the European Union,[13] that is not possible for Meta Industries, Inc. (Facebook), Alphabet, Inc. (Google), and many other U.S. companies, large and small, that depend on transatlantic data transfers to sell online ads or measure web traffic or simply manage their businesses from abroad.[14] This explains why the European Commission and the U.S. government have worked for years to establish a sound legal foundation for an adequacy decision. "The stakes are too high—and international trade between Europe and the U.S. too important to the livelihoods of millions of people—to fail at finding a prompt solution to this imminent problem," Google's President of Global Affairs Kent Walker wrote in January 2022.[15]

The DPF is the third attempt by the United States and the European Union to agree on a U.S. legal framework that would satisfy EU requirements. In cases brought by Austrian privacy activist Max Schrems, the CJEU invalidated two previous adequacy decisions approving prior agreements. The first pertained to the Safe Harbor Framework, in place from 2000 until it was undone in October 2015 by *Schrems I*.[16] In that case, the CJEU found that the Commission's 2000 decision endorsing Safe Harbor[17] was invalid because U.S. law did not "ensure[] . . . a level of protection of fundamental rights [related to data protection] essentially equivalent to that guaranteed in the EU legal order."[18] In particular, U.S. law "permit[ted] the public authorities [through surveillance programs] to have access on a generalised

[10] *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd, ECLI:EU:C:2020:559, para. 135 (July 16, 2020) [hereinafter *Schrems II*].

[11] *See, e.g.*, Datenschutzbehörde, Teilbescheid, Datenschutzbeschwerde (Art. 77 Abs. 1 DSGVO) (Apr. 22, 2022), *at* https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt.pdf [https://perma.cc/3Q7K-27Y3] (Austria); Commission nationale de l'informatique et des libertés, Décision No. [. . .] du [. . .] mettant en demeure [. . .] (Feb. 10, 2022), *at* https://www.cnil.fr/sites/default/files/atoms/files/med_google_analytics_anonymisee.pdf [https://perma.cc/3QX4-EEXP] (France).

[12] Stephanie Bodoni, *Meta, Google Face Data Doomsday as Key EU Decision Looms*, BLOOMBERG (Feb. 18, 2023), *at* https://www.bloomberglaw.com/product/blaw/bloomberglawnews/bloomberg-law-news/XCJM6HTO000000.

[13] Andrea Vittorio, *Microsoft to Keep European Data Locally Amid Policy Uncertainty*, BLOOMBERG (May 6, 2021), *at* https://www.bloomberglaw.com/product/blaw/bloomberglawnews/bloomberg-law-news/X1KPGVU4000000.

[14] As Meta Platforms, Inc. explains in its 2022 SEC filing, "if no adequacy decision is adopted by the European Commission and we are unable to continue to rely on SCCs or rely upon other alternative means of data transfers from the European Union to the United States, we will likely be unable to offer a number of our most significant products and services, including Facebook and Instagram, in Europe, which would materially and adversely affect our business, financial condition, and results of operations." Meta Platforms, Inc., Form 10-K for the Fiscal Year Ended December 31, 2022, at 10 (Feb. 1, 2023), *at* https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/e574646c-c642-42d9-9229-3892b13aabfb.pdf [https://perma.cc/Z3QP-6L32].

[15] Kent Walker, *It's Time for a New EU-US Data Transfer Framework*, GOOGLE: THE KEYWORD (Jan. 19, 2022), *at* https://blog.google/around-the-globe/google-europe/its-time-for-a-new-eu-us-data-transfer-framework [https://perma.cc/9BVQ-XEY3].

[16] Case-C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015) [hereinafter *Schrems I*].

[17] Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7, *at* http://data.europa.eu/eli/dec/2000/520/oj.

[18] *Id.*, para. 96.

https://doi.org/10.1017/ajil.2023.17 Published online by Cambridge University Press

basis to the content of electronic communications."[19] U.S. law also did "not provid[e] for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him [collected by the government], or to obtain the rectification or erasure of such data."[20] The EU and the United States swiftly replaced Safe Harbor with Privacy Shield, which came into effect in July 2016.[21] Privacy Shield sought to cure Safe Harbor's defects through the issuance of "written assurances [by the United States] that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms"[22] and the creation of a Privacy Shield Ombudsperson at the State Department to "review . . . allegations that the U.S. Intelligence Community has engaged in signals intelligence activities that do not comply with applicable restrictions."[23]

In July 2020, in *Schrems II*, the CJEU invalidated the Commission's adequacy decision on the Privacy Shield.[24] The Court found that U.S. laws pertaining to government surveillance programs did not provide EU persons with data protection that was "essentially equivalent" to that provided under EU law.[25] They did not establish "minimum safeguards" and were not "limited to what is strictly necessary."[26] The Court also found that U.S. law did not provide an effective remedy for data protection violations because they did "not grant data subjects actionable rights before the courts against the US authorities."[27] The Privacy Shield's Ombudsperson was insufficient.

The DPF, as implemented through the executive order and related actions, seeks to address the two shortcomings in U.S. law identified in *Schrems II*. But the privacy principles that U.S. companies must adhere to under the DPF and the processes that U.S. companies use to self-certify and re-self-certify their adherence will remain substantively the same as under Privacy Shield.[28] This is because *Schrems II* did not call into question the substantive safeguards that

[19] *Id.*, para. 94.

[20] *Id.*, para. 95.

[21] *See* Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 OJ (L 207) 2, at 7, *at* http://data.europa.eu/eli/dec_impl/2016/1250/oj; *see also* Kristina Daugirdas & Julian Davis Mortenson, *Contemporary Practice of the United States*, 110 AJIL 346, 360 (2016).

[22] Eur. Comm'n Press Release, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016), *at* https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216 [https://perma.cc/22FG-ZEMZ].

[23] Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure 1, *at* https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf [https://perma.cc/NU8G-GJPR].

[24] *Schrems II*, *supra* note 10.

[25] *Id.*, paras. 181–82, 185.

[26] *Id.*, para. 184.

[27] *Id.*, para. 181; *see also id.*, paras. 191–92.

[28] *See* Privacy Shield Framework, FAQs – EU-U.S. Data Privacy Framework Updates (1–4) (last updated Jan. 11, 2023), *at* https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update [https://perma.cc/59EL-AD88] [hereinafter Privacy Shield Framework FAQs]. *Compare* EU-U.S. Data Privacy Framework Principles Issued by the U.S. Department of Commerce, *in* Commission Implementing Decision of XXX 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, Annex I (Dec. 13, 2022), *at* https://commission.europa.eu/document/download/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en?filename=Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf [https://perma.cc/8UWN-6AZS] [hereinafter Draft Adequacy Decision], *with* EU-U.S. Privacy Shield Framework Principles Issued by the Department of Commerce, *at* https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [https://perma.cc/88ZJ-M94K].

https://doi.org/10.1017/ajil.2023.17 Published online by Cambridge University Press

the Privacy Shield offered to EU individuals.[29] As a result, U.S. companies will be able to subscribe to the DPF through compliance with an existing set of privacy obligations, including "the requirement to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties."[30] More than 5,000 U.S. companies self-certified under Privacy Shield.[31]

The executive order, together with the Justice Department regulations and Intelligence Community Directive that were issued subsequently,[32] institute novel limitations on U.S. signals intelligence mass data collection for criminal law enforcement and national security purposes and provide new means of redress for EU persons who believe their rights have been breached.[33] Specifically, the order requires signals intelligence activities to "take into consideration the privacy and civil liberties of all persons" and "be conducted only when necessary to advance a validated intelligence priority and only to the extent and in a manner proportionate to that priority."[34] The order "[m]andates handling requirements for personal information collected through signals intelligence activities and extends the responsibilities of . . . officials to ensure that appropriate actions are taken to remediate non-compliance."[35] And it requires "U.S. Intelligence Community elements to update their policies and procedures to reflect the new privacy and civil liberties safeguards" in the order.[36]

The executive order also establishes a "multi-layer mechanism for individuals from qualifying states and regional economic integration organizations . . . to obtain independent and binding review and redress of claims."[37] The Civil Liberties Protection Officer (CLPO) in the Office of the Director of National Intelligence will provide the first level of review to determine whether U.S. laws were violated and, if so, the "appropriate remediation."[38] The CLPO's decisions will be subject to binding review by the Data Protection Review Court (DPRC), created under Article II of the Constitution, whose judges "have relevant experience in the fields of data privacy and national security, review cases independently, and enjoy protections against removal."[39] The DPRC will appoint a "special advocate" to "assist the panel in its consideration of the application for review, including by advocating regarding the

[29] *See* Privacy Shield Framework FAQs, *supra* note 28.

[30] Eur. Comm'n Press Release, Data Protection: Commission Starts Process to Adopt Adequacy Decision for Safe Data Flows with the US (Dec. 13, 2022), *at* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631 [https://perma.cc/YJ2F-73BK].

[31] *See* Adam Satariano, *E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact*, N.Y. TIMES (July 16, 2020), *at* https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html.

[32] Data Protection Review Court, 87 Fed. Reg. 62,303 (Oct. 14, 2022), *at* https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22234.pdf [hereinafter DOJ Regulations]; Intelligence Community Directive 126 – Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14,086, *at* https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf [https://perma.cc/6XCW-3AA9].

[33] Fact Sheet, *supra* note 2.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

https://doi.org/10.1017/ajil.2023.17 Published online by Cambridge University Press

complainant's interest in the matter and ensuring that the [DPRC] is well informed of the issues and the law with respect to the matter."[40]

Although the executive order is designed to address the concerns of the CJEU regarding U.S. signals intelligence gathering and the provision of independent avenues of redress, it has a broader effect. The new rules apply "regardless of . . . nationality,"[41] and so they can be extended to any "qualifying state."[42] Thus, even though the United Kingdom will not be covered by the European Commission's adequacy decision, the British government announced on October 7, 2022, that it is also moving toward a data adequacy agreement with the United States based on the executive order.[43]

Full implementation of the DPF will take some time. The Commission's adequacy decision on the protection of personal data under the DPF will probably be adopted by the summer of 2023.[44] On December 13, 2022, the Commission published a draft decision, finding that "the United States ensures an adequate level of protection . . . for personal data transferred from the European Union to organisations certified under the EU-U.S. Data Privacy Framework."[45] Before the decision can go into force, it must be reviewed by the European Data Protection Board (EDPB), and then it must be approved by a committee of representatives of EU member states.[46] The European Parliament may also request that the Commission withdraw or amend the decision on the grounds that "its act exceeds the implementing powers provided for in the regulation" (right of scrutiny).[47] On February 28, 2023, the EDPB adopted a non-binding opinion on the draft adequacy decision.[48] The EDPB "welcome[d] substantial improvements [but] [a]t the same time, it expresse[d] concerns and request[ed] clarifications on several points . . . in particular, [relating] to certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the practical functioning of the redress mechanism."[49] In the United States, each element of the Intelligence Community must update their policies and procedures by October 7, 2023.[50] The Privacy and Civil Liberties Oversight Board can then conduct a

[40] EO 14,086, *supra* note 1, Sec. 3(d)(i)(C).

[41] *Id.*, Sec. 1.

[42] *Id.*, Sec. 3(a).

[43] UK Gov't Press Release, UK and US Meet to Make Positive Progress on Data and Tech (Oct. 7, 2022), *at* https://www.gov.uk/government/news/uk-and-us-meet-to-make-positive-progress-on-data-and-tech [https://perma.cc/SNA5-VKEK].

[44] *See* Sam Schechner & Kim Mackrael, *EU Advances Its Data-Flow Deal After U.S. Makes Surveillance Changes*, WALL ST. J. (Dec. 13, 2022), *at* https://www.wsj.com/articles/eu-to-advance-its-data-flow-deal-after-u-s-makes-surveillance-changes-11670927692.

[45] Draft Adequacy Decision, *supra* note 28, para. 196.

[46] *See* Eur. Comm'n, Adequacy Decisions, *at* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/2E2B-Y5K5].

[47] *Id.*

[48] Eur. Data Protection Bd., Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data Under the EU-US Data Privacy Framework (Feb. 28, 2023), *at* https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [https://perma.cc/3UT8-LE5L].

[49] Eur. Data Protection Bd., Press Release, EDPB Welcomes Improvements Under the EU-U.S. Data Privacy Framework, But Concerns Remain (Feb. 28, 2023), *at* https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en [https://perma.cc/X9DE-6GJH].

[50] EO 14,086, *supra* note 1, Sec. 2(c)(iv)(B).

https://doi.org/10.1017/ajil.2023.17 Published online by Cambridge University Press

review of those policies and procedures "to ensure they are consistent with the enhanced safeguards contained" in the order.[51] The attorney general must also designate the European Union as a "qualifying state" and appoint judges and special advocates for the DPRC.[52] Separately, the Department of Commerce will need to adapt its existing Privacy Shield certification process to allow U.S. companies to commit to the required privacy principles under the DPF. Meanwhile, Schrems has already hinted that a legal challenge to the new adequacy decision is likely once it is adopted.[53]

The Department of Defense Issues Civilian Harm Mitigation and Response Action Plan

doi:10.1017/ajil.2023.16

On August 25, 2022, the Department of Defense issued the Civilian Harm Mitigation and Response Action Plan (CHMR-AP) "to improve how the Department of Defense (DoD) mitigates and responds to civilian harm resulting from military operations."[1] Secretary of Defense Lloyd J. Austin III stated in the memo approving the plan that "the protection of civilians is a strategic priority as well as a moral imperative" which "reflect[s] our values and also directly contribute[s] to achieving mission success."[2] While the CHMR-AP asserts that "[n]othing in this plan is intended to suggest that existing DoD policies or practices are legally deficient or that the actions to be implemented . . . are legally required, including under the law of war,"[3] and it seeks to preclude any contention that its issuance contributes to the development of customary international law,[4] the plan, if successfully implemented, will enhance U.S. compliance with its international obligations and set expectations for other militaries.

The Defense Department released the CHMR-AP only after years of pressure from Congress, non-governmental organizations, and newspaper reports and investigations. For two decades, human rights organizations criticized U.S. operations engaged in the "war on terror" for their civilian casualties and the military's failure to learn from those deaths and injuries, mitigate and prevent their recurrence, and properly investigate and prosecute those responsible.[5] In mid-2016, following a shift two years earlier in U.S. operations in

[51] *Id.*, Sec. 2(c)(v)(A).

[52] *Id.*, Sec. 3(f)(i); DOJ Regulations, *supra* note 32, at 62305-06 (28 CFR 201.3-201.4).

[53] *See* NOYB, Statement on US Adequacy Decision by the European Commission (Dec. 13, 2022), *at* https://noyb.eu/en/statement-eu-comission-adequacy-decision-us [https://perma.cc/4UX7-LYKM].

[1] U.S. Dep't of Defense, Civilian Harm Mitigation and Response Action Plan 1 (Aug. 25, 2022), *at* https://media.defense.gov/2022/Aug/25/2003064740/-1/-1/1/CIVILIAN-HARM-MITIGATION-AND-RESPONSE-ACTION-PLAN.PDF [https://perma.cc/6NQB-NT2L] [hereinafter CHMR-AP].

[2] Lloyd J. Austin III, Memorandum on Civilian Harm Mitigation and Response Action Plan (Aug. 25, 2022), *in* CHMR-AP, *supra* note 1, at I [hereinafter Austin Memorandum].

[3] *Id.* at 3 n. 1.

[4] *See id.* (explaining that the "U.S. military routinely implements heightened policy standards and processes that are more protective of civilians than, and supplementary to, law of war requirements, without such standards and processes modifying or creating new legal requirements").

[5] *See, e.g.*, NGO Letter to US Secretary of Defense Demands Accountability and Reform After 20 Years of Civilian Harm (Dec. 1, 2021), *at* https://civiliansinconflict.org/press-releases/ngos-demand-reform [https://perma.cc/Q8JG-KSQS] (letter to Secretary Austin from twenty-one organizations "urging him to account for