CONSENT AS FRICTION

NIKOLAS GUGGENBERGER[1]

Abstract: The leading technology platforms generate several hundred billion dollars annually in revenue through algorithmically personalized advertising—with pernicious effects on our privacy, mental health, and democracy. To fuel their data-hungry algorithms, these platforms have long conditioned access to their services on far-reaching authorizations, embedded in boilerplate terms, to extract their users' data. Until recently, privacy-sensitive alternatives were unavailable—even for a premium. Users faced a stark choice: submit to surveillance or forgo digital participation. I term this business practice 'surveillance by adhesion.'

In July 2023, however, the European Court of Justice ruled in *Meta v. Bundeskartellamt* that surveillance by adhesion violated the European Union's General Data Protection Regulation. To comply with the EU's new regulatory paradigm, the leading (predominantly American) platforms must fundamentally revise their business models by either abandoning personalized advertising or obtaining individuals' informed consent. In practice, the EU's stringent guardrails—which mandate providing users with 'real choice' beyond mere consent pop-ups and granular control—may render user consent so onerous to secure, precarious to sustain, restrictive to operationalize, and prone to litigation that they undermine the commercial viability of personalized advertising. Rather than empowering users to exercise control over their data, the consent mechanism may thus manifest as a vehicle for welcome friction, prompting a shift towards less invasive contextual advertising.

Building on these insights, this Article contends that U.S. policymakers and regulators should, and indeed can, likewise leverage consent as friction to undermine the economic viability of personalized advertising and other harmful surveillance-driven business models. This approach offers a pragmatic alternative to failed notions of user control over data, especially as democratic data governance too often remains beyond reach. Although the EU's new regulatory paradigm offers one model, there are multiple avenues to harness consent as a

[1] Assistant Professor of Law, University of Houston Law Center, with courtesy appointment at the Cullen College of Engineering's Electrical and Computer Engineering Department, and Affiliated Fellow, Yale Information Society Project. For valuable thoughts, conversations, and feedback, thanks to Jack Balkin, Emily Berman, Darren Bush, Anupam Chander, Leah Fowler, Urs Gasser, Leonid Guggenberger, Michael Froomkin, Chris Hoofnagle, Daniel Markovits, Sari Mazzurco, Andrew Miller, James Nelson, Przemysław Pałka, Artur Pericles, Neil Richards, Eleanor Runde, Peter Salib, Alicia Solow-Niederman, Thomas Streinz, and Lex Zardiashvili, and the participants of the Consumer Law Scholars Conference, Privacy Law Scholars Conference, University of Houston Law Center Work in Progress Workshop, Yale Jackson School of Global Affairs Governing Algorithms Workshop, and Yale Law School Private Law Clinic. For excellent research assistance, thanks to David Strumeyer, Katherine Szymanski, and Elizabeth Zietz.

source of friction across different legal contexts. In fact, state-level biometric privacy laws exemplify this strategy's efficacy domestically. Their qualified consent requirements have thrown so much sand in the gears of biometric data collection and use that several leading technology companies have refrained from launching intrusive facial recognition applications altogether. By adopting this friction-based strategy, the Federal Trade Commission and state privacy enforcers can effectively establish potent data usage limitations.

INTRODUCTION

"Senator, we run ads," a smirking Mark Zuckerberg, CEO of Facebook, told Senator Orrin Hatch (R-UT) during the 2018 congressional inquiry into the Facebook-Cambridge Analytica scandal.[2] Senator Hatch had asked how the company "sustain[ed] a business model in which users do not pay for [the company's] service."[3] Indeed, since then, the tech giant, now known as Meta, has generated over $500 billion in advertising revenue and extracted $170 billion in profits.[4] Its core business model has remained unchanged.[5] Like Alphabet, Amazon, TikTok, X (formerly Twitter), and similar platforms,[6] Meta algorithmically personalizes advertisements and other content, based on individuals' characteristics or behaviors.[7] This practice enhances users' engagement and advertisements' effectiveness, thereby boosting these

[2] *Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on Com., Sci., and Transp. and the Comm. on the Judiciary*, 115th Cong. 21 (2018) (statement of Mark Zuckerberg, CEO, Facebook Inc.). In 2018, the data analytics firm Cambridge Analytica used improperly harvested data from around eighty-seven million Facebook users to create targeted advertisements used to influence votes in the 2016 United States presidential election. Joanne Hinds et al., *"It Wouldn't Happen to Me": Privacy Concerns and Perspectives Following the Cambridge Analytica Scandal*, 143 INT'L J. OF HUM.-COMPUT. STUD. 1, 1 (2020).

[3] *Facebook, Social Media Privacy*, supra note 2, at 21 (statement of Sen. Orrin Hatch, Member, Comm. on the Judiciary).

[4] Meta Platforms, Inc., Annual Report (Form 10-K) 90, 103 (Feb. 2, 2024); Facebook, Inc., Annual Report (Form 10-K), 66 (Jan. 27, 2021).

[5] *See Facebook's Business Model: Unlocking Financial Success*, DIGITAL ENTERPRISE, https://digitalenterprise.org/models/facebook/ (explaining that Facebook's revenue is primarily earned through advertising as opposed to users, who engage with the platform for free).

[6] This Article uses the term 'platform' in a broad sense, including for websites and mobile applications.

[7] FTC Staff Report, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services 14, 38 (Sep. 2024), https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services [https://perma.cc/4RGN-QWXK]. *See also* James Ball, *Online Ads Are About to Get Even Worse*, THE ATLANTIC (June 1, 2023), https://www.theatlantic.com/technology/archive/2023/06/advertising-revenue-google-meta-amazon-apple-microsoft/674258/ [https://perma.cc/ZC7C-KM2L] (explaining the process by which websites collect identifying information from users to create targeted advertisements).

platforms' revenues[8]—with pernicious effects on our privacy, mental health, and democracy.[9]

Platforms rely on vast troves of users' behavioral data to fuel their algorithms.[10] Aiming to amass as much data as possible, platforms had long conditioned access to their services on far-reaching authorizations, embedded in boilerplate terms, to extract users' data, infer individuals' preferences, and personalize advertisements and other content accordingly.[11] Users faced a stark choice: submit to extensive surveillance to participate in the digital economy or preserve their privacy by forgoing these services entirely.[12] Privacy-sensitive alternatives were unavailable—even for a premium.[13] Most users submitted to surveillance despite holding largely negative sentiments

---

[8] *See e.g.* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 63–92 (2019); Alexander Bleier & Maik Eisenbeiss, *Personalized Online Advertising Effectiveness: The Interplay of What, When, and Where*, 34 MKTG. SCI. 669, 686 (2015). *See also* Bo Guo & Zhi-bin Jiang, *Influence of Personalised Advertising Copy on Consumer Engagement: A Field Experiment Approach*, ELEC. COM. RSCH. (2023) (observing an increase in consumer engagement where ads are personalized); Claire M. Segijn et al., *The Role of Ad Sequence and Privacy Concerns in Personalized Advertising: An Eye-Tracking Study into Synced Advertising Effects*, 50 J. OF ADVERT. 320, 326 (2021) (emphasizing the effectiveness of ad personalization and "synced advertising"— repeated display of the same message). *But see* TIM HWANG, SUBPRIME ATTENTION CRISIS: ADVERTISING AND THE TIME BOMB AT THE HEART OF THE INTERNET 75–91 (2020) (doubting the effectiveness of online advertising due to public indifference, ad blocking, and fraud).

[9] *See* I.A.

[10] *See* FTC Staff Report, *supra* note 7 , at 15–20 (listing sources of data collection including user metrics, demographics, personal information, privacy preferences, and more); Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. ___ manuscript at 10 (forthcoming 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713111 [https://perma.cc/SY4A-686Y] [hereinafter Solove, *Artificial Intelligence*] (describing the process by which algorithms extract patterns from data). *See also* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018).

[11] *See, e.g.*, Facebook Inc., *Terms of Service* § 2, https://www.facebook.com/legal/terms (last visited Jan. 5, 2024). ("Instead of paying to use Facebook and the other products and services we offer, by using the Meta Products covered by these Terms, you agree that we can show you personalized ads and other commercial and sponsored content that businesses and organizations pay us to promote on and off Meta Company Products. We use your personal data, such as information about your activity and interests, to show you personalized ads and sponsored content that may be more relevant to you.")

[12] Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1397 (2000).

[13] News outlets in the EU offer choices between a 'free' version with tracking and a paid data-sensitive alternative see e.g. DER SPIEGEL, https://www.spiegel.de/ (last visited Jul. 11, 2023) (choice in pop-up window). *See also* Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 119–20 (2019) (observing that some services have offered data-sensitive premium subscriptions).

towards personalized advertising.[14] I term this business model 'surveillance by adhesion.'[15]

In July 2023, however, the European Court of Justice (ECJ) ruled in *Meta v. Bundeskartellamt* that surveillance by adhesion violated the EU's General Data Protection Regulation (GDPR),[16] challenging the entire industry's mode of operation. The court held that Meta lacked a valid justification—as required by the GDPR—for collecting and using personal data to target advertisements and other content.[17] Specifically, the ECJ rejected Meta's boilerplate terms of service as an adequate legal basis for the company's extensive data exploitation, constraining platforms' ability to define their data relations with users.[18] To comply with the EU's new regulatory

---

[14] *See* Sophie C. Boerman et al., *When is Personalized Advertising Crossing Personal Boundaries?: How Type of Information, Data Sharing, and Personalized Pricing Influence Consumer Perceptions of Personalized Advertising*, 4 COMPUT. HUM. BEHAV. REP. 1, 8–9 (2021) (observing negative sentiments and avoidance techniques and identifying higher personal prices as likely tipping point in users' acceptance); M. Leszczynska & D. Baltag, *"Can I Have It Non-Personalised?: An Empirical Investigation of Consumer Willingness to Share Data for Personalized Services and Ads,"* 47 J. CONSUM. POL'Y 345, 362 (2024) (finding that "most [consumers] are hesitant to share personal data for any form of personalization").

[15] On contracts of adhesion see Friedrich Kessler, *Contracts of Adhesion—Some Thoughts about Freedom of Contract*, 43 COLUM. L. REV. 629, 632 (1943) ("standardized contracts are frequently contracts of adhesion; they are *à prendre ou à laisser*"). On the related question whether privacy policies themselves are enforceable contracts see WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 310–311 (2d ed. 2023); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 DICK. L. REV. 587 (2007). For discussions of the dominant economic system online *see generally* ZUBOFF, *supra* note 6; JULIE E. COHEN, BETWEEN TRUTH AND POWER (2019); Amy Kapczynski, *The Law of Informational Capitalism, Review*, 129 YALE L.J. 1460 (2020) (emphasizing the nexus between data surveillance, capitalism, and legal ordering); Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 2015 J. OF INFO. TECH. 75 (2015) [hereinafter Zuboff, *Big Other*] (discussing data extraction in computer-mediated transactions).

[16] Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶ 155 (July 4, 2023). *See generally* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1–88 [hereinafter GDPR].

[17] *Meta*, ECLI:EU:C:2023:537, at ¶¶ 97–139.

[18] *Id.* ¶¶ 97–104. For critiques of the expansion of contractual imperatives *see generally* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2014); BRETT M. FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 71 (2018) (identifying electronic contracting as "an illustration of techno-social engineering of humans"); Danielle D'Onfro, *Contract-Wrapped Property*, 137 HARV. L. REV. 1058, 1075–1125 (2024) (developing the concept of "[i]mperial contract doctrine" — describing the way modern contract usage can undermine property values — and detailing its enormous costs); David A. Hoffman, *Defeating the Empire of Forms*, 109 VA. L. REV. 1367, 1368 (2023) (noting the expansion of governing by contract); Kessler, *supra* note 15, at 640 (observing authoritarian and feudal tendencies of governance by boilerplate); Michael Simkovic & Meirav Furth-Matzkin, *Proportional Contracts*, 107 IOWA L. REV. 229, 237 (2021) (emphasizing the attentional toll overreliance on contractual ordering imposes on consumers).

paradigm, leading advertising-funded platforms must fundamentally revise their business models by either entirely forgoing personalized advertising or by securing individuals' informed consent to process their personal data.[19]

Moreover, the EU has a stringent definition of what counts as valid consent.[20] Neither accepting platforms' boilerplate terms of service nor perfunctory consent pop-ups will suffice. Instead, platforms must ensure that individuals have 'real choice,' free from coercion.[21] According to the ECJ, this involves offering equivalent data-sensitive alternatives for minimal fees that lead to actual uptake and granting users granular control over their data.[22] Providing an advertising-free option for, say, five dollars per month would presumably not meet this standard.[23] The EU's new Digital Markets Act (DMA), enacted in 2022, additionally mandates an opt-in mechanism for any cross-platform data sharing within the same company.[24] Even after securing valid consent, the GDPR encumbers consent's utility to platforms as a continuing legal basis for data processing.[25] Individuals retain an unfettered right to withdraw consent at any time,[26] while platforms remain boxed into the original purpose of data processing, unable to modify it without obtaining consent anew.[27]

---

[19] *Meta*, ECLI:EU:C:2023:537, at ¶¶ 140–154.

[20] GDPR art. 4(11) (defining consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"), 7, recital 32, 42–3. On consent more generally *see* NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 9 (2019); RADIN, *supra* note 18, at 21 (contrasting "informed consent" in the medical context and contractual boilerplate as opposites).

[21] Case C-252/21, *Meta*, ECLI:EU:C:2023:537, ¶¶ 147–153 (July 4, 2023); European Data Protection Board (EDPB), *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms* ¶¶ 67–71 (Apr. 17, 2024), https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en [https://perma.cc/9Q3X-FVZD]. *See* Cohen, *supra* note 12, at 1393–94 (describing the theory of privacy as choice).

[22] *Meta*, ECLI:EU:C:2023:537, ¶ 150. On the peculiarities of "Pay-for-Privacy Models" *see* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1400–1428 (2017) (articulating concerns about unequal access to privacy, illusory control, and predatory and discriminatory behaviors).

[23] Infra pages 35-36

[24] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) art. 36 [hereinafter DMA].

[25] GDPR art. 1(43).

[26] GDPR art. 7(3) ("The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."). Marcu Florea, *Withdrawal of Consent for Processing Personal Data in Biomedical Research*, 13 INT'L DATA PRIV. L. 107, 108–11 (2023).

[27] GDPR art. 5(1)(b) ("Personal data shall be:… collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes… ['purpose limitation'].").

Rigorously enforced, these obligations and constraints insert significant friction[28] into surveillance-based business models—like sand in the gears of an engine. Indeed, they render consent so onerous to secure, precarious to sustain, restrictive to operationalize, and prone to litigation that they undermine the commercial viability of personalized advertising.[29] The new regulatory paradigm could finally herald the demise of the intrusive business model,[30] prompting a shift towards less harmful contextual advertising;[31] that is, advertising attached to specific content or keywords without relying on personal data, like TV commercials for chicken wings during the Super Bowl.[32] Instead of facilitating user control over personal data, consent may thus primarily manifest as a source of welcome friction, establishing soft yet potent data usage limitations.[33]

Drawing on these insights from Europe, this Article contends that U.S. policymakers and regulators can and should leverage consent into friction to undermine the economic viability of personalized advertising and similarly harmful surveillance-driven business models.[34] By adopting this friction-based strategy, the Federal Trade Commission (FTC) and state privacy enforcers can implement soft yet potent limitations on data usage—for instance,

---

[28] Economically, friction represents transaction costs.

[29] *See* III.B.

[30] *See* David Dayen, *Ban Targeted Advertising*, NEW REPUBLIC (Apr. 10, 2018), https://newrepublic.com/article/147887/ban-targeted-advertising-facebook-google [https://perma.cc/5XCG-XTUL].

[31] *See* III.C. On the potential for harm reduction see FTC, *Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* iii, 29–30 (Feb. 2009). Shifting to contextual advertising, however, is no panacea to all online harms. *See* Julie E. Cohen, *Infrastructuring the Digital Public Sphere*, 25 YALE J.L. & TECH SPECIAL ISSUE 1, 30 (2023) (expressing concern about "flows of disinformation and ethnonationalism" facilitated by content-based targeting) [hereinafter Cohen, *Infrastructuring the Digital Public Sphere*]; Przemysław Pałka, *Harmed While Anonymous*, TECH. & REGUL. 22, 22 (2023) (identifying the harms of processing non-personal data).

[32] Cohen, *Infrastructuring the Digital Public Sphere*, *supra* note 31 at 30.

[33] FRISCHMANN & SELINGER, *supra* note 16, at 141, 283–88.

[34] On deliberate friction as a regulatory tool *see id*.; HARTZOG, *supra* note 8, at 253 (lauding friction's capacity to strike a "balance between people's valued obscurity and the public's ability to learn"); Brett Frischmann & Susan Benesch, *Friction-In-Design Regulation as 21st Century Time, Place, and Manner Restriction*, 25 YALE J.L. & TECH. 376, 388 (2023) (advocating for friction as a regulatory tool in the digital economy); Brett M. Frischmann & Moshe Y. Vardi, *Better Digital Contracting With Prosocial Friction-in-Design*, Jurimetrics 38–46 (forthcoming 2025) https://papers.ssrn.com/abstract=4918003 [https://perma.cc/U3ZE-MZQD] (proposing prosocial friction-in-design for digital contracting); Ellen Goodman, *Digital Fidelity and Friction*, 21 NEV. L.J. 623, 648–52 (2021) (proposing communication delays, virality disruptors, and taxes as deliberate frictions); *see generally* William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 49–50 (2013) (detailing the impact of friction on data sharing); Paul Ohm & Jonathan Frankle, *Desirable Inefficiency*, 70 FLA. L. REV. 777, 822–38 (2018) (exploring the desirable effects of friction as a regulatory tool); Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 715–18 (2013) (discussing the ways in which frictionless sharing can be harmful); Zahra Takhshid, *Wearable AI, Bystander Notice, and the Question of the Privacy Frictions*, 104 B.U. L. REV. 1087, 1097–1105 (2024) (suggesting "privacy frictions" for wearable AI devices to alert bystanders).

by challenging surveillance by adhesion as an unfair trade practice. This approach can work, even without a GDPR-style consent requirement.

Although emulating the EU's regulatory framework offers one model, there are other avenues to harness consent as a source of friction across different legal contexts.[35] In fact, Illinois' Biometric Information Privacy Act (BIPA) and Texas' Capture or Use of Biometric Identifier Act (CUBI) provide compelling domestic examples[36] that illustrate the efficacy of friction from consent in the U.S., albeit limited to a niche aspect of privacy. These laws mandate explicit and informed consent for biometric data collection.[37] In practice, the consent requirement has created substantial operational challenges—imagine, for example, obtaining informed consent for facial recognition from strangers passing a smart door bell—and violations have proven costly.[38] In July 2024, Meta entered the biggest state privacy settlement ever and agreed to pay $1.4 billion to resolve a lawsuit brought by the Texas Attorney General over the company's Tag Suggestion, a discontinued social media feature that relies on users' biometric information.[39] Effectively, consent has manifested as friction: It has deterred numerous major technology companies from deploying potentially intrusive facial recognition applications.[40] If extended beyond core biometric data, this type of consent-based friction could serve as a powerful instrument to check the excesses of informational capitalism.[41]

The argument to leverage consent as friction adopts a realpolitik approach to privacy—one that pragmatically works within existing political

---

[35] See, e.g., 740 ILL. COMP. STAT. 14/15(b) (2008); TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017).

[36] 740 ILL. COMP. STAT. 14/15(b) (2008); TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017).

[37] 740 ILL. COMP. STAT. 14/15(b) (2008); TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017).

[38] *See* Fredric D. Bellamy & Ashley N. Fernandez, *Illinois Court Decisions Acknowledge Biometric Privacy Act's Damages a Potential Business Killer*, REUTERS (Apr. 17, 2023), https://www.reuters.com/legal/legalindustry/illinois-court-decisions-acknowledge-biometric-privacy-acts-damages-potential-2023-04-17/ [https://perma.cc/A76Z-5SRC] (calling the Illinois Biometric Information Privacy Act a "potential business killer").

[39] Agreed Final Judgement, Texas v. Meta Platforms, Inc., No. 22-0121 (Tex. Dist. Ct. 2024); Mike Scarcella & Jody Godoy, Meta to Pay $1.4 Billion to Settle Texas Facial Recognition Data Lawsuit, REUTERS (Jul. 31, 2024), https://www.reuters.com/technology/cybersecurity/meta-platforms-pay-14-bln-settle-texas-lawsuit-over-facial-recognition-data-2024-07-30/ [https://perma.cc/92L7-WBUK].

[40] Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1, 41 (2020); Ally Marotti, *Google's Art Selfies Aren't Available in Illinois. Here's Why,*, CHI. TRIB. (Jan. 17, 2018), https://www.chicagotribune.com/2018/01/17/googles-art-selfies-arent-available-in-illinois-heres-why/ [https://perma.cc/QDR4-3GBU].

[41] *See* COHEN, *supra* note 13; ZUBOFF, *supra* note 6 at 21; *see generally* Kapczynski, *supra* note 15; Zuboff, *Big Other*, *supra* note 15.

realities rather than idealized scenarios.[42] U.S. privacy enforcement, led at the federal level by the FTC, would ideally move beyond flawed illusions of individual control and towards democratic data governance to distinguish legitimate from illegitimate data usage.[43] Yet, this vision appears unlikely to come to fruition soon. Despite the FTC's recent criticism of the dominant 'notice and choice' regime and shifts in enforcement strategies,[44] individual control will presumably remain the agency's primary regulatory tool.[45] The

---

[42] *See* Alicia Solow-Niederman, *The Overton Window and Privacy Enforcement*, 37 HARV. J.L. & TECH. 1007, 1013–34 (2023) (identifying the FTC's practical enforcement boundaries).

[43] *See* III.A. For shortcomings of control-based privacy individualism *see* LEONID GUGGENBERGER, IRRWEG INFORMATIONELLE PRIVATAUTONOMIE: GRENZEN DES MARKTBASIERTEN DATENSCHUTZES (2023) (detailing how individual control over data, as idealized in the GDPR, is ill-suited to provide adequate privacy protection); Ben-Shahar, *supra* note 13 at 106 (analogizing "data emissions" to pollution); Dirk Bergemann et al., *The Economics of Social Data*, 53 RAND J. ECON. 263 (2022) (analyzing and formalizing data externalities); Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1930 (2013) [hereinafter Cohen, *What Privacy is For*] (observing that the "emphasis on privatized regulation and control of information flows [] reinforces precisely those aspects of modulation that are most troubling and most intractable"); A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1717–45 (2015) (analogizing surveillance to pollution); Joshua A. T. Fairfield, & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2015) (arguing that privacy represents as public, not just a private good); Sari Mazzurco, *Democratizing Platform Privacy*, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 792, 811–21 (2021) (criticizing privacy law's lack of consideration for social dynamics and democratic governance); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1660 (1999) (citing privacy-as-control's inability to "promote democratic self-rule"); Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U.L. REV. 357, 394 (2022) [hereinafter Solow-Niederman, *Information Privacy*] (demonstrating that inferences drawn from large data sets can impact individuals similarly as information from personal data); Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 638 (2021) (identifying the shortcoming of individual control over personal data and proposing democratic data governance). On the ineffectiveness of data control see e.g. FRISCHMANN & SELINGER, *supra* note 16, at 314–15; HARTZOG, *supra* note 8, at 62–67 (observing a manufacturing of consent); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) (discussing the First Amendment in the context of data control); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543, 563 (2008) (noting the steep time costs of reading privacy policies word-for-word); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 426–27 (2018) (discussing the illusory nature of control); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 444 (2016) (characterizing privacy controls as an illusion of choice); Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 605 (2024) (observing a notion of false legitimacy) [hereinafter Solove, *Murky Consent*]; Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1452 (2001) [hereinafter Solove, *Privacy and Power*] (identifying limits on individuals' ability to make informed decisions about their data).

[44] FTC, Remarks of Chair Lina M. Khan, As Prepared for Delivery IAPP Global Privacy Summit 2022, 6 (Apr. 11, 2022), https://www.ftc.gov/news-events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022 [https://perma.cc/G26Z-NWP9]; Luke Herrine, *Unfairness, Reconstructed*, YALE J. ON REG. (forthcoming 2024) (observing a shift away from consumer sovereignty).

[45] *See* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 6 (2021).

political economy remains favorable to notions of control, as evidenced by the most promising recent federal privacy bills.[46] Further, any fundamental changes to the FTC's regulatory strategy would face a high risk of judicial overturn.[47] At the state level, new privacy laws largely confine enforcers to control-based frameworks,[48] further entrenching the conceptual *status quo*. Consequently, the core challenge of privacy realpolitik lies in identifying effective mechanisms within control-based frameworks to curtail harmful business models.[49]

This Article develops the concept of consent as friction and its implications for privacy regulation in four parts. Part I introduces surveillance by adhesion and shows how the EU's new regulatory paradigm has outlawed this mode of operation.[50] Part II unravels the legal ramifications of shifting the foundation of data processing from contractual imperatives (promise)[51] toward consent (permission).[52] Part III reveals how this shift, especially the real choice requirement, disrupts the mechanics of personalized advertising.[53] More broadly, it reveals that seemingly toothless control-based privacy frameworks can effectively transform into powerful data usage limitations, when consent generates sufficient friction.[54] Finally, Part IV argues that consent-based friction provides an effective and pragmatic tool for U.S. policymakers and regulators to end personalized advertising and can prompt an overdue shift toward less harmful contextual advertising, particularly where comprehensive democratic data governance remains unattainable or impractical.[55]

---

[46] *See, e.g.*, American Privacy Rights Act, S. ___, 118th Cong. (2024); American Privacy Rights Act, H.R. 8818, 118th Cong. (2024).

[47] *See* West Virginia v. EPA, 597 U.S. 697, 723–24 (2022) (formally recognizing the "major questions doctrine"); Utility Air Regulatory Group v. EPA, 573 U.S. 302, 324 (2014); Loper Bright Enters. v. Raimondo, 144 S.Ct. 2244, 2263 (2024) (rejecting agency deference for questions of law, overruling the *Chevron*-doctrine).

[48] Viljoen, *supra* note 43, at 592–97.

[49] *Id.* at 598.

[50] *See infra* XX and accompanying text.

[51] On contractual imperatives in privacy law see IGNACIO N. COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY, 11 (2023). On the core of contracts *see generally* CHARLES FRIED, CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION (2d ed. 2015).

[52] *See infra* XX and accompanying text. Note that "consent" features prominently in contract law, Nancy Kim, Relative Consent and Contract Law, 18 Nev. L. J. (2017) (clarifying the "meaning of contractual consent"). *See generally* Randy E. Barnett, A Consent Theory of Contract, 86 Colum. L. Rev. 269, 291-309 (1986). This Article distinguishes between contractual assent and data consent.

[53] *See infra* XX and accompanying text.

[54] *See infra* XX and accompanying text.

[55] *See infra* XX and accompanying text.

I. ENDING SURVEILLANCE BY ADHESION IN THE EU

Personalizing advertising and other content builds on vast troves of individuals' personal data.[56] The more data platforms can aggregate, the more capable their algorithms become, and the more granularly they can personalize advertisements and other content.[57] Platforms' algorithms rely on information that is deliberately shared or extracted through behavioral surveillance.[58] The extracted information may stem from keystrokes while typing, eyeball movements while scrolling through news feeds, granular location data while traveling, and detailed expense reports from shopping sprees.[59] Aggregating this "behavioral exhaust" can be enormously valuable to advertising-based platforms because it enables them to finetune their messages to our presumptive tastes and preferences.[60] Finetuning messages serves to increase engagement with advertisements.[61] This enhanced engagement, in turn, boosts these platforms' revenue streams.[62]

The characteristics that render data so valuable to businesses, however, also threaten individuals' privacy.[63] This is because the same data enables inferences and predictions about everything in our lives, from medical history to personality traits and sexual desires and from mood swings to political affiliations.[64] These inferences and predictions are indeed used to manipulate and deceive individuals, exploit their weaknesses, and extract attention and engagement—thereby deepening power asymmetries between platforms and their users.[65] This may create wants that we don't really want, inducing

---

[56] *See* FTC Staff Report, *supra* note 7 , at 15–20 (identifying numerous sources of personal data collection).

[57] Solove, *Artificial Intelligence and Privacy*, *supra* note 10, at 10. *See also* HARTZOG, *supra* note 8, at 5.

[58] *See* FTC Staff Report, *supra* note 7, at 55–58 ; WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 400 (2d ed. 2023) (distinguishing active and passive data collection).

[59]

[60] ZUBOFF, *supra* note 6 at 63–92; Zuboff, *supra* note 13.

[61] Zuboff, *supra* note 13 at 79.

[62] *Id.*

[63] Derek E. Bambauer, *Target(ed) Advertising* 58 U.C. DAVIS L. REV. _26–41_ (forthcoming 2024); Balkin, *supra* note 43, at 1187–90.

[64] *Id.*; Clemens Stachl et al., *Predicting Personality from Patterns of Behavior Collected with Smartphones*, 117 PROC. NAT'L ACAD. SCI. 17680 (2020); Rae Nudson, *When Targeted Ads Feel a Little Too Targeted*, VOX (Apr. 9, 2020), https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus [https://perma.cc/8W4M-6TT7]; Sylvie Douglis, Ad Targeting Gets Into Your Medical File, NPR (Jan. 9, 2024), https://www.npr.org/transcripts/1197960899.

[65] *See* Rowe, *supra* note 40, at 24–34 (describing concerns associated with facial recognition); Elise Hu, *Facebook Manipulates Our Moods For Science And Commerce: A Roundup*, NPR (June 30, 2014), https://www.npr.org/sections/alltechconsidered/2014/06/30/326929138/facebook-manipulates-our-moods-for-science-and-commerce-a-roundup [https://perma.cc/LXW2-4LRZ].

overconsumption and even addiction.[66] It may also facilitate discrimination and exclusion.[67] Ultimately, surveillance may jeopardize our civil liberties[68] and mental health.[69] Individual privacy, however, is not the only value at stake. Behavioral surveillance and personalized advertising can also undermine democracy, diminish public trust, obscure public discourse and markets, and even implicate national security, as evidenced by jogging soldiers who inadvertently revealed the boundaries of military bases in conflict regions when tracking their run via the fitness app Strava.[70]

---

[66] Vikram R. Bhargava & Manuel Velasquez, *Ethics of the Attention Economy: The Problem of Social Media Addiction*, 31 BUS. ETHICS Q. 321, 323–28, 339–42 (2021) (linking social media's business model to addiction); James Niels Rosenquist et al., *Addictive Technology and Its Implications for Antitrust Enforcement*, 100 N.C. L. REV. 431, 442–52 (2022). *See generally*, ADAM L. ALTER, IRRESISTIBLE: THE RISE OF ADDICTIVE TECHNOLOGY AND THE BUSINESS OF KEEPING US HOOKED (2017). On the role of wants and their creation see JOHN KENNETH GALBRAITH, THE AFFLUENT SOCIETY 124–31 (40th anniversary ed. 1998) (coining the dependence effect and observing advertising as a link between production and wants); Frank H. Knight, *Social Science and the Political Trend*, 3 U. TORONTO Q. 407, 422 (1934) (identifying the "excessive tendency to produce wants for goods" as a "fundamental weaknesses of the market system").

[67] SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 64–109 (2018); Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, Yale L.J. F. 907, 913–28 (2022) (observing discriminatory exclusion, oversurveillance, and predation of African Americans online); Dakota Kim, *A Constant Barrage: US Companies Target Junk Food Ads to People of Color*, GUARDIAN (Nov. 11, 2022), https://www.theguardian.com/environment/2022/nov/11/junk-food-marketing-children-of-color; Martin Moore, *How the Online Business Model Encourages Prejudice*, GUARDIAN (Oct. 28, 2018), https://www.theguardian.com/technology/2018/oct/28/how-target-ads-threaten-the-internet-giants-facebook. Algorithms may perpetuate prejudices entrenched in the real world and represented in data sets. *See* Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023, 1036 (2017); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 680–92 (2016).

[68] Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data [https://perma.cc/F8GV-K2SG]; Sara Morrison, *What Police Could Find out about Your Illegal Abortion*, VOX (June 24, 2022), https://www.vox.com/recode/23059057/privacy-abortion-phone-data-roe [https://perma.cc/W43X-CSP2].

[69] Gillian Brockell, *Dear Tech Companies, I Don't Want to See Pregnancy Ads after My Child Was Stillborn*, WASH. POST (Dec. 12, 2018), https://www.washingtonpost.com/lifestyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn/ [https://perma.cc/4H8L-E4JR]; Georgia Wells et al., *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sep. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 [https://perma.cc/PV9A-9NQ4].

[70] Ben-Shahar, *supra* note 13, at 113–14 (identifying public harm, including to national security); Chris Jay Hoofnagle, *Swindling and Selling Revisited* 5, 43–44 (2024) (observing the capacity to obscure transactions and distribute misinformation) (on file with author); Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 336–37 (2014) (discussing "digital gerrymandering" as a tool to influence elections); Liz Sly, *U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging*, WASH. POST (Jan. 29, 2018), https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html; Catherine

Section A of this Part discusses the pervasive practice of businesses conditioning digital services on consent to sweeping authorizations granting access to individual data, introducing the concept of surveillance by adhesion. Section B identifies surveillance by adhesion's secondary role, that of a compliance strategy under the GDPR. Section C analyzes the recent landmark case from the European Court of Justice, *Meta v. Bundeskartellamt*, which rejected surveillance by adhesion as incompliant with the GDPR, and Section D considers the Digital Markets Act as an additional source of disruption for surveillance by adhesion.

A. Surveillance by Adhesion as a Business Practice

Given these privacy risks, users may hesitate to share personal information with platforms.[71] This context gives rise to a business practice I call *surveillance by adhesion*: Platforms condition access to their services on users' submission to extensive surveillance. Specifically, platforms include far-reaching authorizations in their boilerplate terms to extract users' data, infer individuals' preferences, and personalize advertisements and other content accordingly.[72] Like other elements of boilerplate terms, these authorizations are not negotiable. Platforms do not offer privacy-sensitive alternatives—even for a premium.[73] All this occurs in a situation of grave power asymmetry between platforms and users, leaving individuals with a stark "choice": submit to extensive surveillance to participate in the digital economy or preserve their privacy by forgoing these services entirely.[74] This "choice," however, lacks any meaningful expression of autonomy.[75] It is not the type of consent that is said to do "moral magic," that is, "to make an action right when it would otherwise be wrong."[76] Rather, it resembles our acquiescence to boilerplate contracts or contracts of adhesion.[77]

Thorbecke, *Lawmakers Question Facebook over Targeted Ads for Military Gear in Wake of Capitol Riot*, ABC NEWS (Mar. 8, 2021), https://abcnews.go.com/Business/lawmakers-question-facebook-targeted-ads-military-gear-wake/story?id=76325413 [https://perma.cc/2TYQ-TT28].

[71] ZUBOFF, *supra* note 6, at 79–80; Generating user information for use in targeted advertising, Registration No. US9235849B2, col. 4 ll. 47–59 (emphasizing the need for surveillance by citing that user "information [] may be limited to what is needed for the service [] because of privacy considerations").

[72] *See, e.g.*, Facebook Inc., *Terms of Service*, *supra* note 9, § 2.

[73] News outlets in the EU offer users a choice between a "free" version with tracking and a data-sensitive alternative for a fee see e.g. DER SPIEGEL, *supra* note 11 (choice in pop-up window). *See also* Ben-Shahar, *supra* note 13, at 119–20 (observing that some services have offered data-sensitive premium subscriptions).

[74] *See, e.g.*, Facebook Inc., *Terms of Service*, *supra* note 9, § 2.

[75] RADIN, *supra* note 18, at 89–90.

[76] Heidi M. Hurd, *The Moral Magic of Consent*, 2 LEG. THEORY 121, 123–24 (1996).

[77] WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 474 (2d ed. 2023); RADIN, *supra* note 18, at 89–90.

Scholars have long and fiercely criticized boilerplate contracting.[78] It "enables enterprisers to legislate by contract . . . in a substantially authoritarian manner without using the appearance of authoritarian forms," Friedrich Kessler famously observed in his 1943 critique of adhesive contracts.[79] For Kessler, boilerplate could create a "new feudal order" that ironically inverts contract law's historic role in dismantling feudal involuntary servitude.[80] More recently, Margaret Jane Radin detailed the corrosive effects of recognizing boilerplate as legally binding despite insufficient expressions of autonomy: normative degradation by deleting rights without consent and—in Kessler's tradition—democratic degradation by enabling private governance of the marketplace.[81]

Scholars have distinguished four categories of objections to contracts of adhesion: (1) the 'No Reading Thesis,' suggesting that due to time and attention constraints, no one reads terms of service; (2) the 'No Market Discipline Thesis,' contending that unacknowledged terms do not meaningfully impact supply and demand; (3) the 'Online Disadvantage Thesis' proposing that (1) and (2) are even more pronounced online; and (4) the 'Feedback Loop Thesis' arguing that the lack of market discipline encourages ever worse terms for consumers.[82]

These critiques are all well-founded and become even more acute when companies hold monopoly power.[83] Subjecting our future selves to coercive enforcement demands some justification beyond our general participation in society.[84] Leveraging state power to enforce terms that do not result from any meaningful expression of autonomy would be profoundly unjust. Furthermore, it would appear perverse to subsidize exploitive practices by letting businesses access public infrastructure in the form of the judicial system.

---

78 *See generally* RADIN, *supra* note 16; Andrea J. Boyack, Abuse of Contract: Boilerplate Erasure of Consumer Counterparty Rights, Iowa L. Rev. 3 (forthcoming 2025) (showing "that the overwhelming majority of consumer contracts contain multiple categories of abusive terms"); Hoffman, *supra* note 18, at 1388 (pointing to a hundred-year tradition of criticizing mass contracting); Przemyslaw Palka, *Terms of Injustice*, 126 W. VA. L. REV. 133, 169–82 (2023) (arguing against consumer unfriendly terms).

79 Kessler, *supra* note 15, at 640.

80 *Id.* at 641.

81 RADIN, *supra* note 18, at 19, 33.

82 Hoffman, *supra* note 18, at 1377–78. *See also* Simkovic & Furth-Matzkin, *supra* note 18, at 243–54 (observing the potential for lemons markets).

83 *See* H.R. Rep. No. 117-8, 35–61 (2020) (detailing concerns related to monopolies' coercive powers); Mark Glick et al., *Big Tech's Buying Spree and the Failed Ideology of Competition Law*, 72 U.C. HASTINGS L.J. 465, 486–504 (2021) (identifying contemporary merger doctrine as a contributor to Meta's monopoly power); Nikolas Guggenberger, *Moderating Monopolies*, 38 BERKELEY TECH. L.J. 119, 141–51 (2023) (discussing the lack of constraints on speech platforms' terms of service)..

84 *See* Kaiponanea T. Matsumura, *Binding Future Selves*, 75 LA. L. REV. 71, 83–84 (2014) (delineating different selves rationales to explain contractual choice architecture).

Concerns about contractual overreach, however, are broader. They do not merely take issue with a certain form of contracting but with the role of contract law in our lives.[85] Contract doctrine's "imperial" tendencies disrupt private law's delicate equilibrium by, for example, undermining ownership.[86] To an alarming extent, contractual logic, as applied in practice,[87] drowns out competing legal principles from property to tort law and captures ever more unclaimed territory, with detrimental effects on liberty and modularity.[88] This perpetuates domination and deepens complexity, evidenced by consumers and small businesses entangled in terms of service too extensive to ever be read, constrained by waivers without viable alternatives, or bound by obligations that they never meant to assume.[89]

Others agree that contractual logic overreaches, warranting efforts to contain its influence.[90] This holds especially true for overreliance on written terms, as an "empire of forms has conquered products, procedure, and employment law."[91] Trivial relationships and low-value, everyday transactions are increasingly codified in text because the internalized costs of doing so

---

[85] D'Onfro, *supra* note 18, at 1075–1111

[86] *Id.*; *see also* David A. Hoffman, *Defeating the Empire of Forms*, *supra* note 18, at 1368 (2023) ("Contract's empire of forms, on a generations-long march, continues to conquer new territory. Not content with dominating the worlds of commercial law and finance, written contracts now govern the most common consumer and employment relationships").

[87] See RADIN, *supra* note 18, at 3, 8 (distinguishing between a world of agreements, representing how contract law should work, and a world of boilerplate, representing how contract law does work).

[88] D'Onfro, *supra* note 18, at 1111–25 (laying out the costs associated with contractual overreach). On the concept and value of modularity as a mechanism to govern complex systems efficiently by breaking them down into manageable semi-independent parts *see* Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L.J. 1, 24 (2000) (providing a transaction cost justification for limited forms of property); Henry E. Smith, *Property as the Law of Things*, 125 HARV. L. REV. 1691, 1700–1720 (2012) (presenting a modular theory of property); Henry E. Smith, *Toward an Economic Theory of Property in Information*, *in* RESEARCH HANDBOOK ON THE ECONOMICS OF PROPERTY LAW (Kenneth Ayotte & Henry E. Smith eds., 2011); Henry E. Smith, *Intellectual Property as Property: Delineating Entitlements in Information*, 116 YALE L.J. 1742, 1751–82 (2007) (describing modularity as an efficient information management architecture).

[89] D'Onfro, *supra* note 18, at 1064–75 (focusing on property in chattel bound by servitudes); Simkovic & Furth-Matzkin, *supra* note 18, at 236–54 (emphasizing the attentional toll overreliance on contractual ordering imposes on consumers). *See also, e.g.*, Rukmini Callimachi & Derek M. Norman, *Lured by Luxury Vacations, They Were Stuck With Debt*, N.Y. TIMES (Oct. 31, 2024), https://www.nytimes.com/2024/10/31/realestate/unlimited-vacation-club-hyatt-contracts-deception.html (reporting on consumers who were duped into expensive, long-term vacation club memberships that offered little value); Anna Tims, *Homeowners Trapped by 25-Year Solar Panel Contracts*, GUARDIAN (Nov. 25, 2018), https://www.theguardian.com/money/2018/nov/25/homeowners-trapped-solar-panels [https://perma.cc/D6VH-YDEY](reporting that homeowners have found themselves trapped in long-lasting contracts for rooftop solar panels binding potential buyers for years and thus rendering these homes hard to sell).

[90] Hoffman, *Defeating the Empire of Forms*, *supra* note 18 at 1395–96 (2023).

[91] *Id.*

have diminished in the wake of the digital revolution.[92] The public costs of excessive reliance on written terms have not, however.[93] Building on this analysis, some scholars propose to render all low-value written contracts unenforceable.[94] Others foreground the attentional strain modern contractual ordering imposes on consumers and recommend Pigouvian taxes to mitigate contacts' attentional externalities.[95] This would increase contracting costs to the parties and presumably reduce businesses' reliance on contractual ordering.[96] Lawmakers and courts, however, have mostly ignored the side effects of contractual imperatives' triumph and refrained from decisive action against contractual overreach.[97]

Against this background, some courts in the U.S. have expressed suspicion about adhesive terms' validity and held businesses, particularly insurance companies, to their customers' reasonable expectations instead of the boilerplate's wording.[98] The EU has even implemented a comprehensive regulatory framework that expressly renders "unfair" terms unilaterally provided to others unenforceable.[99] By and large, however, courts on both sides of the Atlantic have enforced boilerplate terms with minimal requirements for expressions of autonomy—some going as far as letting ignorance suffice to infer binding contracts.[100] The courts' deference to contractual ordering has enabled surveillance by adhesion.[101]

---

[92] *Id.* at 1399.

[93] *Id.* at 1406 (explaining that arbitration clauses "reduc[e] the incidence of mass adjudication [] weaken[ing] the deterrent force of the law" and steering consumer behavior through unenforceable terms can lead to a deterioration of the quality of products and services).

[94] *Id.* at 1409–14.

[95] Simkovic & Furth-Matzkin, *supra* note 18 at 234–35, 236–42, 254–65.

[96] *Id.* at 235.

[97] *Id.* at 233–34.

[98] *See e.g.* C & J Fertilizer, Inc. v. Allied Mut. Ins. Co., 227 N.W.2d 169, 176 (Iowa 1975) (applying a doctrine of reasonable expectations to insurance contracts). *But see* Deni Assocs. of Fla., Inc. v. State Farm Fire & Cas. Ins. Co., 711 So.2d 1135, 1140 (Fla. 1998) (declining to adopt the doctrine of reasonable expectations).

[99] Council Directive 93/13/EEC on unfair terms in consumer contracts, OJ (L 095) art. VII (Apr. 5, 1993).

[100] *See e.g.* B.D. v. Blizzard Entertainment, Inc., 76 Cal. App. 5th 931, 943–47 (2022) (discussing methods of assent to an online contract, including browsing, clicking "I agree", and signaling that one read the terms and conditions); DeFontes v. Dell, Inc., 984 A.2d 1061, 1071 (R.I. 2009) (holding that contract formation occurs when a consumer has time to review the terms and accepts them); Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1148 (7th Cir. 1997) (holding that a contract "need not be read to be effective"); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452–53 (7th Cir. 1996) (finding that, under the UCC, a buyer accepts delivered goods after they have had meaningful time to review the product); RADIN, *supra* note 18, at 21–23.

[101] *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1248 (2002) ("The transformation of personal information into property allows people to bargain over it and make binding transfers of it through contracts.").

B. Surveillance by Adhesion as a Compliance Strategy

In the EU, however, surveillance by adhesion was not only a business practice — counterintuitively, it also was a central element of platforms' GDPR compliance strategy.[102] At the core of the EU's comprehensive data protection framework lies a general prohibition of data usage, or, in the GDPR's terminology, "data processing," without proper justification.[103] Effectively, personal data may only be processed based on one of the six legitimate bases enumerated in GDPR art. 6(1).[104] This requirement leads to two separate relationships between platforms and users: the services contract and the data relation, the latter of which includes the justification to process users' data.[105]

First on the list of potential justifications stands the data subject's consent.[106] With its envisioned capacity to operationalize control over data, consent arguably provides the prototypical permission to process personal data in private relations.[107] EU data protection law provides stringent requirements for obtaining valid consent, however.[108] GDPR art. 4(11) defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes."[109] The data controller bears the burden of demonstrating all conditions for valid consent are met.[110]

The European Data Protection Board's (EDPB) most recent guidelines explain consent's four elements as follows.[111] First, consent must be freely

---

[102] GDPR recital 40.

[103] GDPR art. 6(1) (Data processing is defined in GDRP art. 4(2) as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction")

[104] GDPR art.6(1). These lawful purposes include the user giving consent; data processing that is necessary to contract performance; processing that is necessary to fulfill legal obligations; processing that is necessary to protect the interests of the user; processing that is necessary to comply with the public interest; processing that is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. *Id.*

[105] *See* Przemysław Pałka, *Data Management Law for the 2020s: The Lost Origins and the New Needs*, 68 BUFF. L. REV. 559, 614 (2020) ("Unlike the 'notice and choice model' [in the U.S.,] the GDPR does not see the relationship regarding data as a market transaction.").

[106] GDPR art. 6(1)(a).

[107] *See e.g.* GDPR recital 40 ("[P]ersonal data should be processed on the basis of the consent of the data subject concerned or *some other* legitimate basis" [emphasis added]). For the inadequacies of control see III.A.

[108] GDPR art. 4(11).

[109] GDPR art. 4(11).

[110] GDPR art. 7(1), recital 42.

[111] EDPB, *Guidelines 05/2020 on Consent under Regulation 2016/679* ¶ 11 (May 4, 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en. The EDPB is tasked with ensuring consistent interpretation of the GDPR by data protection authorities throughout the European Economic Area. *See Tasks and*

given, which "implies real choice and control,"[112] absent any "risk of deception, intimidation, coercion or significant negative consequences (e.g., substantial extra costs) if he/she does not consent."[113] With the emphasis on real choice, the EDPB clarifies that physical or legal pressure is not necessary to invalidate consent; feeling compulsion suffices.[114] This interpretation aligns with GDPR recital 43, which recommends against relying on consent as a justification for processing personal data in situations of clear power imbalances.[115] Data processing by government and employers—both entities wielding outsized power over their citizens and employees, respectively—often falls into this category, for example.[116] Most importantly for platforms, however, GDPR art 7(4) extends the protection of choice against coercion and limits tying consent to data processing to the provision of a service.[117]

Second, the granting of consent must be specific, not general.[118] As part of the effort to provide sufficient transparency for freely exercised choices, the requirement limits consent to identified and prescribed types and purposes of data processing.[119]

Third, only informed consent provides a basis for lawful data processing.[120] The concept of informed consent is the GDPR's core pillar to protect data subject autonomy.[121] It is the controller's responsibility to ensure information provided to data subjects is sufficient to exercise their autonomy.[122] Rooted in structural information asymmetries between the data controller and the data subject, informed consent builds on notions of consent in the health sector, which is in stark contrast to general contract law doctrine.[123] To comply with informed consent requirements, the data processor must disclose the identity of the controller, the purpose of data processing, the type of data processed, and the right to withdraw consent at any time.[124] Only clear and precise language that is tailored to the targeted audience and

---

Duties, EUROPEAN DATA PROTECITON BOARD, https://edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en.

[112] *Id.* ¶ 13.

[113] *Id.* ¶ 13, 24.

[114] *Id.* ¶ 13.

[115] GDPR, rec. 43.

[116] EDPB, *Guidelines 05/2020 on Consent*, *supra* note 111 at ¶¶ 16–24.

[117] GDPR art. 7(4), rec. 43. *See also* II.C.

[118] EDPB, *Guidelines 05/2020 on Consent*, *supra* note 111, at ¶ 55.

[119] *Id.*

[120] GDPR art. 4(11).

[121] EDPB, *Guidelines 05/2020 on Consent*, *supra* note 111, at ¶ 62.

[122] *Id.* at ¶ 3.

[123] *See* RADIN, *supra* note 18, at 21 (contrasting "informed consent" in the medical context and contractual boilerplate as opposites); Balkin, *supra* note 43, at 1200–1203.

[124] EDPB, *Guidelines 05/2020 on Consent*, *supra* note 111, at ¶ 64.

distinguishable from other terms—such as community standards or terms of service—can fulfill the disclosure requirement.[125]

Fourth and finally, GDPR art. 4(11) demands that the data subject's wishes are unambiguously indicated "by a statement or by a clear affirmative action."[126] Only deliberate action can establish valid consent.[127] Add to all this that individuals retain an unfettered right to withdraw consent for the future at any time,[128] and it becomes clear that these requirements and limitations complicate platforms' business model.

Meta sought a different, less burdensome legal basis for data processing that would allow the company to condition the provision of its social media services on its ability to exploit its users' personal data.[129] As of the GDPR's entry into force in 2018, Meta switched the legal basis for processing users' personal data from consent to contractual necessity.[130] GDPR art. 6(1)(b) allows data processing to the extent it "is necessary for the performance of a contract to which the data subject is party."[131] Instead of asking individuals for consent to use their data, Meta included far-reaching permissions to infer individuals' preferences and personalize advertisements and other content in its terms of service.[132]

Meta's logic was simple. By including the delivery of personalized advertisements and other content in its terms of service, processing users' data became necessary to perform its contract with users.[133] Compliance with the GDPR's core requirement, therefore, demanded nothing but an update of the company's boilerplate, and Meta could continue to condition its services on its ability to exploit its users' personal data.[134] Despite the GDPR's goal of enhancing individual control and autonomy over data, users could only 'choose' between Meta's digital services with extensive surveillance and no access to the largest social network. Surveillance by adhesion, a practice that would have been highly suspicious under the GDPR's thick conceptualization of consent, became magically possible under contractual logic. For five years, Meta's tactic had paid off.[135]

---

[125] *Id.* ¶¶ 66–75.

[126] GDPR art. 4(11).

[127] EDPB, *Guidelines 05/2020 on Consent*, *supra* note 111, at ¶ 77.

[128] GDPR art. 7(3).

[129] Lex Zard, *Five Years of Illegitimacy of Surveillance Advertising*, *in* CRITICAL REFLECTIONS ON THE EU'S DATA PROTECTION REGIME, manuscript at 2 (Róisín Á. Costello & Mark Leiser eds., forthcoming 2024) (on file with author) (describing how Meta's justification for data processing switched from consent to contractual necessity).

[130] *Id.*

[131] GDPR art. 6(1)(b).

[132] Zard, *supra* note 129, at 2.

[133] *Id.* at 15.

[134] *Id.* at 2, 15.

[135] Zard, *supra* note 129, at 8–9.

C. Meta v. Bundeskartellamt

On July 4, 2023, however, the ECJ declared in *Meta v. Bundeskartellamt*, that surveillance by adhesion is incompatible with the GDPR, dealing a significant blow to Meta's business model.[136] *Meta* is set to become one of the most consequential privacy rulings yet. Its practical impact stands to eclipse that of the ECJ's 2014 decision in *Google Spain SL v. Agencia Española de Protección de Datos*, recognizing the right to be forgotten against search engines,[137] and *Schrems I* and *Schrems II*, limiting transatlantic dataflows.[138] Though hallmarks of EU privacy jurisprudence, these decisions imposed ultimately negligible compliance costs.[139] Platforms easily adjusted their practices without changing their business models. *Meta* stands to be different. This Section discusses the impact of *Meta* on data privacy protection in the EU.

The transformative potential of *Meta* challenging personalized advertising rests in the ECJ's mere seven-paragraph interpretation of GDPR art. 6(1)(b), the contractual necessity of data processing.[140] Recall Meta's core compliance strategy: The company included the provision of personalized advertisements in its terms of service, aiming to establish its data processing as a contractual necessity.[141] The ECJ obliterated Meta's argument.[142] The court found that the company could have provided social media services without personalizing advertisements and other content.[143] In other words, the court found that Meta's data collection and analysis to personalize advertisements and other content were not necessary for the performance of its

---

[136] Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶ 104 (July 4, 2023). Deviating from the Advocate General's opinion and far exceeding the German Federal Cartel Office's initial order, the ECJ did not limit itself to the data exchange between Meta's various platforms and tools.

[137] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 ECLI:EU:C:2014:317, ¶ 94 (May 13, 2014) (establishing that search engines are data controllers responsible for the processing of personal information through website indexing and recognizing individuals' right to request, under certain conditions, the de-indexing of search results linking to their personal information that is inaccurate, irrelevant, or no longer necessary).

[138] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015) (Schrems I); Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020) (Schrems II).

[139] *See generally Google Spain SL*, ECLI:EU:C:2014:317; *Schrems I*, ECLI:EU:C:2015:650; *Schrems II*, ECLI:EU:C:2020:559.

[140] Case C-252/21, *Meta*, ECLI:EU:C:2023:537, ¶¶ 97–104 (July 4, 2023).

[141] Zard, *supra* note 129, at 2.

[142] *See Meta*, ECLI:EU:C:2023:537 at ¶¶ 97–104 (rejecting Meta's argument that processing user data is a necessary function of the platform).

[143] *Id.*

contract with users.[144] Whether user experience would be better or worse without personalization remained irrelevant.[145]

The court explained that for data processing to be considered necessary, "it must be objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject."[146] The court added a but-for qualification: "the main subject matter of the contract cannot be achieved if the processing in question does not occur."[147] When judging whether a service can be provided, the data controller must consider all available "workable, less intrusive alternatives."[148] In accordance with general principles, the burden of proof to establish contractual necessity lies with the entity invoking the justification.[149]

Applying these standards, the ECJ limited the data controllers' power to define the contractual obligation in their terms of service.[150] Referencing certain data usages in platforms' terms of service does not automatically fulfill the contractual obligation requirement for the purpose of GDPR art. 6(1)(b).[151] Furthermore, the court demanded that the necessity of data usage be assessed individually for every service, even where services are bundled together in one contract.[152] Meta failed on both fronts.[153] Its express qualification of personalized advertisements as consideration for digital services did not meet the benchmark of necessity.[154] And although personalization of content might have been useful to some users, the company could alternatively have provided social media services without personalization.[155] The availability of this alternative was sufficient for the court to reject Meta's attempt to tie social media services with the personalization of advertisements and other content.[156] On the same grounds, the ECJ also dismissed the data exchange between Meta's several different platforms—the core objection to Meta's business practices in the German FCO's original order that gave rise to the case.[157]

The *Meta* opinion consolidated an emerging regulatory consensus in the EU. In 2021, Luxembourg's National Commission for Data Protection fined

---

[144] *Id.* at ¶ 104.
[145] *Id.* at ¶ 102.
[146] *Id.* at ¶ 98.
[147] *Id.*
[148] *Id.* at ¶ 99.
[149] *Id.* at ¶¶ 95, 98.
[150] *Id.* at ¶¶ 97–104.
[151] *Id.* at ¶ 99.
[152] *Id.* at ¶¶ 100–102.
[153] *Id.* at ¶ 102, 104.
[154] *Id.* at ¶ 104.
[155] *Id.* at ¶ 102.
[156] *Id.* at ¶¶ 102–104.
[157] *Id.* at ¶¶ 103–104.

Amazon for using customers' data to personalize advertisements without their consent.[158] In late 2022, the EDPB concluded that Meta's contract with its users provided insufficient justification to process personal data for behavioral and personalized advertisements.[159] Shortly thereafter, the Irish Data Protection followed the EDPB's decision, fined Meta, and ordered the company not to rely on its contracts with users as justification for data processing to personalize content.[160]

Next, the ECJ turned to Meta's legitimate interests in personalizing advertisements and other content,[161] which could justify the company's data usage. GDPR art. 6(1)(f) requires three cumulative conditions: (1) the controller's interest in processing the data must be legitimate, (2) the data processing must be necessary to achieve these interests, and (3) countervailing "interests or fundamental rights and freedoms of the data subject" do not take priority.[162] The referring court considered a slew of plausibly legitimate interests, ranging from the provision of personalized advertisements and marketing tools to network security, innovation for the social good, and product improvement, to name only a few.[163]

When applying the balancing test to personalizing advertising, the court first referenced GDPR recital 47, which mentions direct marketing as a possible legitimate interest.[164] Without much attention to the second prong, the ECJ then balanced Meta's interests in personalized advertising against the

---

[158] Nat'l Comm'n for Data Prot. (CNPD), *Decision Regarding Amazon Europe Core S.à r.l.* (Jun. 8, 2021), http://cnpd.public.lu/en/actualites/international/2021/08/decision-amazon-2.html [https://perma.cc/YMB6-MAUB] (Luxembourg law prevents the CNPD from "publish[ing] any decision before the deadlines for appeals have expired."); Taylor Telford, *E.U. Regulator Hits Amazon with Record $887 Million Fine for Data Protection Violations*, WASH. POST (Jul. 31, 2021), https://www.washingtonpost.com/business/2021/07/30/amazon-record-fine-europe/.

[159] EDPB, *Binding Decision 4/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Instagram Service (Art. 65 GDPR)* ¶ 128 (Dec. 5, 2022), https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-42022-dispute-submitted_en [https://perma.cc/J8KJ-DAKJ].

[160] Data Prot. Comm'n, Decision *In re.* TSA (Inquiry 18-5-7), ¶¶ 202, 206, 209, 212, 348 (Dec. 31, 2022), https://edpb.europa.eu/system/files/2023-01/instagram_inquiry-18-5-7_final_decision_en.pdf [https://perma.cc/QN4E-XYYX]; Data Prot. Comm'n, Decision *In re.* LB (Inquiry 18-5-5) (Dec. 31, 2022), https://edpb.europa.eu/system/files/2023-01/facebook-18-5-5_final_decision_redacted_en.pdf [https://perma.cc/88B5-R4J6].

[161] Case C-252/21, *Meta*, ECLI:EU:C:2023:537, ¶¶ 105–126 (July 4, 2023).

[162] GDPR art. 6(1)(f). *See also Meta*, ECLI:EU:C:2023:537 at ¶ 106; Case C-597/19, *Mircom Int.'l Content Mgmt. & Consulting (MICM) Ltd. v Telenet BVBA*, ECLI:EU:C:2021:492, ¶ 106 (June 17, 2021); Case C-40/17, Fashion ID v. Verbraucherzentrale NRW e.V., ECLI:EU:C:2019:629, ¶ 95 (Jul. 29, 2019) (delineating the equivalent predecessor of GDPR art. 6(1)(f), Data Protection Directive 95/46 art. 7(f)). *See also* EDPB, *Guidelines 8/2020 on the Targeting of Social Media Users*, ¶¶ 50–55 (Apr. 13, 2021), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en [https://perma.cc/Z8MG-DD3F].

[163] Case C-252/21, *Meta*, ECLI:EU:C:2023:537, ¶ 113 (July 4, 2023).

[164] *Id.* at ¶ 115.

interests, freedoms, and rights of users.[165] The court foregrounded users' reasonable expectations.[166] Irrespective of whether social media operators charge monetary fees, the court reasoned, users could not reasonably expect the usage of their data for personalized advertisements without their prior consent.[167] Further tipping the balance, Meta's extensive data usage could profoundly affect users by engendering a sense of constant surveillance.[168] The court expressed severe doubts about whether other purposes, including network security, product improvement, protecting minors, and research and innovation for social good, could justify the type and scope of Meta's data processing.[169]

Having rejected the two most plausible bases for Meta's data processing, the ECJ considered the necessity of data processing[170] "for compliance with a legal obligation" and "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."[171] Lacking essential details for a final ruling, the court limited itself to formulating abstract guidelines for fact-finding courts, demanding an explicit legal requirement for the data processing in question.[172] That said, no reasonable interpretation of these guidelines leaves room to accommodate Meta's personalization of advertisements or its extensive cross-platform data exchange. Lastly, the court dismissed the idea that GDPR art. 6(1)(d), the provision permitting data processing "to protect the vital interests" of individuals could, even in the abstract, justify Meta's practices.[173]

D. The Digital Markets Act

The ECJ's ruling is not the only source of disruption for surveillance by adhesion. The competition-focused Digital Markets Act (DMA) places additional obligations on some of the largest platforms considered 'gatekeepers.'[174] Gatekeepers are defined as undertakings with a significant impact on the EU's internal market that provide an important gateway for businesses to

---

[165] *Id.* at ¶¶ 115–118.

[166] *Id.* at ¶ 116.

[167] *Id.* at ¶ 117.

[168] *Id.* at ¶ 118.

[169] *Id.* at ¶¶ 119–123.

[170] *Id.* ¶¶ 119–126. Due to a lack of relevant information, the court ultimately remanded back to the national courts which presented questions concerning the interpretation of EU law to the ECJ. *Id.* at ¶ 130.

[171] *Id.* at ¶ 127; GDPR art. 6(1)(c), (e).

[172] Case C-252/21, *Meta*, ECLI:EU:C:2023:537, ¶ 130-132 (July 4, 2023).

[173] *Id.* at ¶¶ 135–138.

[174] European Commission Press Release IP/23/4328, Digital Markets Act: Commission Designates Six Gatekeepers (Sep. 6, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.

reach users and enjoy an entrenched, durable position.[175] On this basis, the European Commission has designated several companies, including Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft, as gatekeepers of their respective core platform services.[176] These include, among others, social networking platforms such as TikTok, Facebook, Instagram, and LinkedIn; intermediation platforms such as Google Maps and Amazon Marketplace; the video-sharing platform YouTube; and the search engine Google.[177]

Besides obligations to grant competitors access to core services, the new regulation also establishes additional explicit consent requirements for gatekeepers.[178] According to DMA art. 5(2), platforms designated as gatekeepers must obtain end users' consent if they "process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper" or combine personal data across different platforms.[179] On substance, these guardrails overlap with the requirements stipulated in *Meta*.[180] The DMA, however, does not speak to personalized advertising based on data solely collected from individuals using the gatekeepers' core platform. In this regard, *Meta* goes beyond the DMA's requirements. Yet, despite *Meta*'s broader scope, the European Commission relied on DMA art. 5(2) when it recently notified Meta of its preliminary finding that the company has failed to implement the conditions to obtain valid consent for personalized advertising properly.[181] The Commission's choice may have been motivated by the DMA's explicit language or its potentially larger fines compared to those of the GDPR.[182]

* * *

Together, the ECJ's ruling in *Meta* and the DMA's additional explicit consent requirements define a new regulatory paradigm in the EU. They limit the ability of data controllers to define their data relations with their users via boilerplate terms. Practically, this ends surveillance by adhesion as a business practice in the EU, challenging the core of the entire industry's mode of

---

[175] Commission Regulation 2022/1925 of the European Parliament and of the Council of 14 Sept. 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), art. 3(1)(a – c), 2022 O.J. (L 265), 30 [hereinafter DMA].

[176] European Commission Press Release, *supra* note 176.

[177] *Id.* (providing a complete list).

[178] DMA art. 5(2).

[179] *Id.* at art. 5(2)(a).

[180] *See supra* Part I.C.

[181] European Commission Press Release IP/24/3582, Commission Sends Preliminary Findings to Meta Over its "Pay or Consent" Model for Breach of the Digital Markets Act (Jul. 1, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582 [https://perma.cc/384Q-WTWT].

[182] *See* DMA recital 37 (specifying consent requirements for gatekeepers); *see also* DMA art. 30(1) (allowing for fines of up to 10% of worldwide turnover for first offenders).

operation. To personalize advertisements and other content, platforms like Meta will need to obtain individuals' valid consent to data usage for that purpose. This task, however, will be thorny, as the following Part will detail: Under the GDPR's stringent guardrails, valid consent is incomparable to contractual assent to boilerplate.[183]

II. From Promise to Permission: Data Protection as Anti-Contract Law

The new regulatory paradigm set forth by *Meta* and the new DMA heralds a profound conceptual transformation of commercial data relations. To be clear, neither *Meta* nor the new DMA decommodifies data—that is, they don't remove data's status as a tradable asset.[184] Rather, the new paradigm shifts the governance of data relations from a model tracking contractual promises to one grounded in explicit and separate permissions. Under surveillance by adhesion, individuals' control over their data was intermediated by a thin concept of binding contractual assent to a boilerplate service contract. This contract then justified data processing and, thus, also governed users' data relations with platforms. The new paradigm establishes two separate and independent relationships: the service contract and the data relation. In doing so, it elevates individuals' control over their data to the GDPR's thicker notion of momentarily permissive consent, based on "real choice."[185] This transition redefines the appropriate boundaries of contractual logic and

[183] See infra XX and accompanying text. The GDPR's conditions for valid consent also apply to the DMA's consent requirements, *see* DMA art. 5(2).

[184] *See* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. Rev. 423, 475–500 (2018) (critiquing privacy frameworks that enable data commodification); James Grimmelmann & Christina Mulligan, *Data Property*, 72 Am. U.L. Rev. 829, 859–62 (2023) (identifying different conceptualizations of data as property). *But see* Beschwerde nach Artikel 77(1) DSGVO [Complaint under Article 77(1) GDPR] *In re.* Meta Platforms Ireland Ltd. §§ 19–22 (Nov. 28, 2023), https://noyb.eu/de/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay [https://perma.cc/5PHC-4R8Q] (noting that providing data protection for a premium would limit exercise of a fundamental right only to those who can afford to pay). On decommodification generally *see* Rethinking Commodification: Cases and Readings in Law and Culture (Martha M. Ertman & Joan C. Williams eds., 2005); Kieran Healy & Kimberly D. Krawiec, *Repugnance Management and Transactions in the Body*, 107 Am. Econ. Rev. 86, 86–89 (2017) (conceptualizing and criticizing repugnance from the public as a constraint on exchange); Kimberly D. Krawiec, *Markets, Repugnance, and Externalities*, 19 J. Inst'l Econ. 944, 949–51 (2023) (delineating and criticizing the limitations on egg donations and kidney exchanges). On taboo trades and prohibited markets *see generally* Kimberly D. Krawiec, *Markets, Morals, and Limits in the Exchange of Human Eggs*, 13 Geo. J. L. & Pub. Pol'y 349 (2015); Kimberly D. Krawiec, *The Dark Side of Commodification Critiques: Politics and Elitism in Standardized Testing*, 35 Wash. U. J.L. & Pol'y 349 (2011); Kimberly D. Krawiec, *No Money Allowed*, 2022 U. Chi. Legal F. 221 (2022).

[185] *See* II.C.

provides a powerful example of successful pushback against the suffocating overreach of contractual imperatives in the digital sphere.[186]

With this change in the nature of data relations, the EU's new privacy paradigm positions data protection as anti-contract law in two core ways: first, by limiting platforms' ability to define their data relations with users via terms of service and, second, by unbundling permissive consent to data processing from contractual assent to boilerplate. The following sections demonstrate the extent to which these two elements elevate dignitarian autonomy over contractual imperatives, as applied in practice.[187]

Section A discusses limitations on the relevant subject matter of contracts implicitly resulting from *Meta*. Section B distinguishes data consent from assent to circumstantial contracts. Section C explores the further unbundling consent from contract, including privacy price control and granular decision making.

A. Limiting Contracts' Relevant Subject Matter

Recall that under the GDPR, a contractual relationship justifies all data processing necessary to fulfill the contractual obligations.[188] Data protection law *prima facie* follows the contract. With few exceptions for extreme cases, promise and consideration govern the data relation, not *vice versa*.[189] Contractual assent replaces the otherwise necessary consent or weighing of interests.[190] Inevitably, this invites contractual imperatives into the realm of data protection law. These imperatives range from minimal conditions for expressions of individual autonomy to the very ability to subject our future selves

---

[186] *See generally* Omri Ben-Shahar & Lior Jacob Strahilevitz, Contracting over Privacy: Introduction, 45 J. LEGAL STUD. 1 (2016) (observing that "[p]rivacy law has an uneasy relationship with contract").

[187] See infra XX and accompanying text. On the different emphases of human dignity and market-based liberty in the EU and the US *see* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 664–69, 682–84 (2014) (distinguishing permissive U.S. privacy rules with the EU's more restrictive approach); Pałka, *supra* note 105, at 572–88, 602–24 (contrasting the roots of data protection regulation in the EU and the US); Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1988 (2013) ("Europe has long sought both data trade and privacy protection."); Joel Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1342–52 (2000) (contrasting market liberty in the U.S. and social protection in Europe); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151, 1160–64 (2004) (observing a transatlantic divide over the roles of dignity and liberty in privacy law).

[188] GDPR art. 6(1)(b).

[189] Contractual supremacy requires a valid contract. Egregious privacy intrusions, like spying on tenants or misuse of photographs for explicit purposes, may invalidate the contractional relation under unconscionability and public policy doctrines. In these extreme cases privacy norms define contractual relations.

[190] *See* GDPR art. 6(1)(a), (f).

to state-sanctioned enforcement.[191] At a more abstract level, contractual supremacy also imports reasoning predominantly informed by economic considerations, such as transaction costs and, in the EU, facilitating cross-border commerce.[192] By establishing *prima facie* contractual supremacy, GDPR art. 6(1)(b) creates a significant risk of undermining individuals' dignitarian autonomy and fundamental rights.

In *Meta*, the ECJ, however, emphasized the *necessity* of data processing for the performance of a contract.[193] What appears to merely repeat the statutory text effectively confines platforms' ability to govern data relations via terms of service.[194] Rather than applying the necessity criterion to the contract as stipulated by Meta's terms of service, the ECJ constructed the content of the bargain objectively. That is, the court substituted its own interpretation of the core exchange for that of the parties—defined by Meta—and then applied the necessity criterion to this revised understanding.

Like the ECJ, the EDPB's regulatory guidance also emphasizes the *necessity* of data processing for the performance of a contract.[195] The Board expressly attributes "independent meaning" to the concept of necessity beyond a mere mirror image of the contractual terms.[196] The EDPB bases that conclusion on a 2008 ECJ decision, delineating the meaning of necessity in the context of the performance of a task carried out in the public interest as a basis for data processing.[197] Instead of relying on the contract to fill the concept of necessity with meaning, this approach relies on an objective analysis, the starting point of which is "the purpose of the processing . . . in the context of a contractual relationship."[198]

This is remarkable because, generally, the parties to a contract—or, in actuality, the drafters of the terms of service—determine the contract's objective. By extension, this determination would then govern the contextual data relations.[199] Even the EU's 1993 Directive on Unfair Terms in Consumer

---

[191] *See* Matsumura, *supra* note 84, at 79–92 (identifying the ability to bind our future selves as one critical dimension of expressing autonomy).

[192] *See, e.g.*, Council Directive 93/13/EEC on unfair terms in consumer contracts, OJ (L 095) 29 (Apr. 5, 1993) (even referencing "distortions of competition").

[193] Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶¶ 97–104 (July 4, 2023).

[194] Id.

[195] EDPB, *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects - Version 2.0* ¶¶ 23–39 (Oct. 8, 2019), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

[196] *Id.* at ¶ 23.

[197] Case C-524/06, Heinz Huber v. Bundesrepublik Deutschland, ECLI:EU:C:2008:724 (Dec. 16, 2008), ¶ 52.

[198] EDPB, *Guidelines 2/2019*, *supra* note 196, at ¶ 24.

[199] GDPR art. 6(1)(b).

Contracts, which places significantly stricter limits on businesses than U.S. consumer protection, refrains from scrutinizing contracts' main subject matter.[200] In contrast to consumer protection law's restraint, the ECJ directly second-guessed the contract's objective.

But exactly how restrictive is the GDPR when assessing a contract's subject matter as a legal basis for data processing? The GDPR's recitals, which provide explanations of the rationales behind the law to guide future legal interpretation, offer no meaningful insights.[201] Reading the ECJ's reasoning in *Meta* closely, however, reveals a court with no doubts that personalizing advertisements and other content could not reasonably be considered part of a social network's contractual barter justifying data usage. Indeed, taking data protection law seriously demanded these restrictions. Otherwise, platforms could simply bypass the stringent requirements for obtaining valid consent by doing exactly what Meta tried—incorporating the desired data processing in their terms of service.

The *Meta* opinion evinces several crucial guardrails for future application in this area. First and most importantly, the court endorsed the advocate general's opinion that contracts need to be disaggregated and the resulting services judged independently.[202] Tying services together in a package cannot expand the contours of contractual necessity under data protection law.[203] Furthermore, the ECJ treated a barter contract—social media services in exchange for exposure to personalized advertisements—as two separate relations. This interpretation of 'necessity' limits boilerplate's role in structuring data relations. Second, the court treated consent as first among equal legal justifications, warranting a restrictive interpretation of contractual necessity in the absence of consent.[204] Third, and building on consent as a leitmotiv, the new standard appears to consider whether relying on a contract merely serves to circumvent the heightened requirements for valid consent. Here, the court dismissed what it implicitly identified as a sham agreement. Fourth, the ECJ emphasized users' reasonable expectations in its application of GDPR art. 6(1)(f) and assessment of Meta's legitimate interests as a justification for

---

[200] Council Directive 93/13/EEC on Unfair Terms in Consumer Contracts, O.J. (L 095) 29, 30 (Apr. 5, 1993) (stipulating that the "assessment of unfair character shall not be made of terms which describe the main subject matter of the contract nor the quality/price ratio of the goods or services supplied").

[201] GDPR rec. 44 ("processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract").

[202] Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶¶ 100–102 (July 4, 2023); Case C-252/21 Opinion Advocate General Rantos, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537 (July 4, 2023), ¶ 54.

[203] *Meta*, ECLI:EU:C:2023:537, at ¶¶ 100–102.

[204] *Id.* at ¶¶ 91–63. *Cf.* MCGEVERAN, *supra* note 42, at 392.

data processing.[205] This could be read as a broader endorsement of individuals' reasonable expectations as a benchmark for acceptable data usage. In turn, this benchmark could also define a contract's suitability for structuring data relations.[206]

To operationalize the framework consistently, we should first ask whether the data usage is ancillary to a normatively accepted contractual obligation.[207] This prong is rooted in the fairness principle in GDPR art. (5)(a).[208] Second, we need to consider the intensity of the privacy invasion at stake—an aspect the ECJ emphasized in the context of Meta's legitimate interests.[209] Substantial interference with individuals' privacy requires granular, valid consent. The performance of a contract cannot suffice because promoting commerce would be outweighed by the impact on individuals' data autonomy. Third, we should disaggregate bundled services—including barter exchanges that can be settled in fiat—and apply the necessity criterion granularly.[210] Where all three conditions are satisfied, GDPR art. 6(1)(b) can provide a lawful basis.[211] This test would, for example, allow Amazon to compute addresses for delivery purposes: The data processing would be ancillary to an e-commerce purchase, and even a narrow understanding of Amazon's core obligations would demand the processing of address data. But services-for-data business models, whether advertisement-based or not, could generally not rely on GDPR art 6(1)(b); they would require consent.

This approach significantly differs from transparency-grounded limitations on boilerplate, rooted in consumer protection, both in the EU and the U.S. It almost inverts consumer protection law's paradigm: the more closely

---

[205] *Meta*, ECLI:EU:C:2023:537, at ¶¶ 116–117.

[206] Instead of these scattered guardrails, the court should have offered a positive framework delineating the boundaries of GDPR art. 6(1)(b). The best foundation for a such framework lies in the norm's purpose. That is, to lower transaction costs and promote commerce. By recognizing contracts as legal bases for data processing, the GDPR lowers the protections of individual autonomy over data relative to its stringent conditions for valid consent. The norm balances individual autonomy and business interests. The EDPB's pragmatic guidance reflects a similar understanding: some data processing is simply inevitable for commerce and GDPR art. 6(1)(b) is grounded in the EU Charter of Fundamental Rights' economic freedom. *See* EDPB, *Guidelines 2/2019*, *supra* note 196 at ¶ 2 (adding that contract-based data processing lies in the interest of both parties).

[207] This approach is inspired by the civil law artifact of a normatively defined contractual typology. It could, however, just as well be brought to fruition in common law jurisdictions. After all, common law jurisdictions also distinguish between different types of contracts, for example, to determine the scope of statutory laws like tenant or sales laws. To operationalize these distinctions, courts have developed tests like inquiries into the predominant purpose of transactions, which rely on a similar logic. On the exaggerated differences between civil and common law generally see Holger Spamann, Civil V. Common Law: The Emperor Has No Clothes (August 26, 2024). Harvard Public Law Working Paper No. 24-11, Available at SSRN: https://ssrn.com/abstract=4937647.

[208] *See also* EDPB, *Guidelines 2/2019*, *supra* note 196, at ¶ 12.

[209] *Meta*, ECLI:EU:C:2023:537, at ¶¶ 116–117.

[210] *Meta*, ECLI:EU:C:2023:537, at ¶¶ 100–102.

[211] GDPR art. 6(1)(b).

the data usage resembles contractual consideration, the less likely the GDPR is to accept 'performance of a contract' as a valid legal basis for processing that data.[212] The GDPR's benchmark is best understood to reflect normatively defined user expectations, derived from the GDPR's fairness principle, not expectations in the form of actual or typical user knowledge.[213] This standard shifts the relevant question from what (cynical) individuals expect from platforms—that is, market transparency[214]—to what they should expect—that is, normative transparency guided by the fairness principle.[215]

There is reason to believe that the ECJ's narrow understanding of contractual necessity in the context of personalized advertising reaches far beyond Meta as a company or social media as a sector. Search, shopping, video sharing, music, and gaming can be separated from personalized advertising just as easily as social media. Likewise, users generally do not seek out these services for advertising. There may, however, be some limits to the application of this understanding. First, one could imagine platforms that deliberately pitch themselves as intermediaries for paid personalized advertising content. Even under a normative concept of transparency, it remains unclear whether the court would go as far as categorically rejecting these contracts as valid bases for data processing. Second, the personalization of organic content may indeed be inseparable from the provision of certain services. Take a hypothetical algorithmic medical advice app. Not personalizing the automatically generated advice would, at least, significantly reduce its benefits and could even be outright dangerous by ignoring autoimmune reactions or drug interactions, for example. The same could be true of a 'personal shopper' site. But, under the *Meta* decision, neither the medical advice app nor the personal shopper site could embed within its display unrelated advertisements chosen based on users' personal data without their informed consent.

To summarize, the GDPR significantly limits platforms' ability to structure data relations contractually via boilerplate. This restriction safeguards the heightened requirements for valid consent—namely that it be freely given, informed, specific, and unambiguous.[216] In doing so, the GDPR functions as a form of anti-contract law, pushing back against overreaching contractual imperatives.

---

[212] *Id.*

[213] GDPR art. 5(1)(a).

[214] *See* Leonid Guggenberger, *Nebenentgelte im Bankgeschäft, AGB-Kontrolle und Markttransparenz [Ancillary Fees in Banking, Limits on Boilerplate, and Market Transparency]*, BKR 1 (2017) (Ger.).

[215] See RADIN, *supra* note 18, at 30–31 ("Because an expectation is widespread…doesn't necessarily make it right. Recipients [of boilerplate] have a right to expect justice, even in an unjust system").

[216] GDPR art. 4(11).

B. Distinguishing Consent from Contract

With surveillance by adhesion banned by the ECJ, all eyes are on consent as the sole remaining legal basis to personalize advertisements. The following sections show how the GDPR conceptually distinguishes, insulates, and decouples consent to data processing from assent to any circumstantial contract.[217] The separation of consent and contract aims to enable real choice, prevent coercion, and protect our continuous exercise of autonomy. That is, the autonomy of our future selves to remain unbound by our present selves' choices, as is familiar in the context of our bodily integrity and sexual self-determination.[218] At the same time, the GDPR's protections against coercion do not generally decommodify personal data.[219] Instead, platforms may still obtain consent as a form of consideration for their services and monetize users' data—provided they meet the conditions for valid consent. In other words, consent as momentary permission remains a marketable entitlement.[220] This principle comes with an exception, however. The new Digital Services Act (DSA) prohibits online platforms from personalizing advertisements based on profiling using sensitive personal data.[221]

The distinction between consent and contract becomes evident as the GDPR requires an articulation of the data subject's wishes separate from the assent to a circumstantial contract. The EDPB, for example, emphasizes that "consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service."[222] Where consent is obtained in text form within the same document as the circumstantial contract, the declaration of consent needs to be clearly separated from the terms and conditions of the contract. Merely proceeding with a service can establish a contractual, or at least quasi-contractual relationship, creating legal obligations and, potentially, providing the basis for damages. That same behavior, however, would be insufficient to constitute consent under the GDPR: Merely proceeding with a service does not establish valid consent to data processing.[223]

The requirements for legal capacity also vary between consent to data processing and assent to a contract. GDPR Art. 8(1) of the sets the age of

---

[217] See infra XX and accompanying text.

[218] *See* Matsumura, *supra* note 84, at 93.

[219] *See supra* note 128.

[220] *But see* EDPB, *Opinion 08/2024 on Valid Consent*, *supra* note 21, at ¶ 130.

[221] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 on a Single Market for Digital Services (Digital Services Act) 2022 O.J. (L 277), ¶ 69; GDPR art. 4(4), 9(1) (limiting user profiling and data processing).

[222] EDPB, *Guidelines 05/2020 on Consent*, *supra* note 111, at ¶ 81.

[223] *Id.* at ¶ 79.

consent for data processing to sixteen years.[224] This is three years higher than the thirteen-year threshold the EU Commission—inspired by the US Children Online Data Protection Act of 1998[225]—had originally proposed.[226] Section 3 of the same article then clarifies that the statutory definition of the age of consent does not affect the general principles of contract law in the Member States.[227] Although differing in the details, these general principles of contract law limit the legal capacity of minors under eighteen years in most Member States.[228] Whatever the reasons for the age difference for legal maturity might be, the divergence between the conditions for consent to data processing and assent to a contract shows that the two agreements are separate; they must be recognized as individually legally relevant acts.

Once established, the model outcomes of contract and consent reveal contrasting conceptualizations of autonomy.[229] On the one hand, contracts bind the promisor to their promise relating to marketable entitlements. Any future opposing will of the promisor becomes irrelevant. Contract freezes the promisor's exercise of autonomy in time. The state delegates its enforcement power to the promisor, enabling them to barter the resulting future limitation of autonomy for consideration. Granted, these principles have notable exceptions; various consumer protection frameworks allow promisors to back out, minors can disaffirm most contracts, contracts themselves can include immediate termination rights,[230] and unilateral contracts may collapse promise and performance entirely. None of that changes the archetypal binding nature of contracts, though.

---

[224] Art. 8(1) of the GDPR allows Member States to set age thresholds as low as thirteen years.

[225] *Commission Staff Working Paper—Impact Assessment*, at 107, SEC (2012) 72 final 68 (Jan. 25, 2012).

[226] *See* Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), at 45, COM/2012/011 final (Jan. 25, 2012). The former Data Protection Directive did not specify a minimum age for consent, *see* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (L 281) 31–50 (Oct. 24, 1995).

[227] GDRP art. 8(3). General contract law falls under the jurisdiction of the Member States. *Id.*

[228] *See* European Union Agency for Fundamental Rights, *Age of Majority*, http://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/age-majority [https://perma.cc/63R6-MJYR]. In Germany, for example, minors under the age of seven are deemed incapable of contracting and minors between the ages of seven and 18 are limited in their legal capacity, Bürgerliches Gesetzbuch [BGB] [Civil Code], § 104, no. 1, 105, no. 1, 106-113, http://www.gesetze-im-internet.de/englisch_bgb/index .html (Ger.).

[229] Matsumura, *supra* note 84, at 79–92 (distinguishing different selves and delineating our autonomy accordingly). Note that users can delete their accounts on Meta's platforms, thereby terminating the contract with the company.

[230] Meta, for example, allows its users to delete their profiles and, thus, terminate their social media contract at any time. Facebook Inc., *Terms of Service*, supra note 11, at § 3.

On the other hand, individuals can freely withdraw consent to data processing under the GDPR at any time. Unlike the assent to contracts, consent to data usage is not binding into the future.[231] The GDPR's emphasis of the right to remain unbound elevates privacy insofar to the level of bodily integrity and sexual self-determination—in line with privacy's dignitarian roots in the EU. Instead of trading away permissions, we continuously exercise autonomy by doing as we please—untainted by our prior permissions. This, of course, comes at a cost; it also reduces the commercial value of individuals' entitlements. Overall, the shift from contract to consent as a governance paradigm for data relations, following *Meta*, thus rebalances different notions of autonomy. It strengthens dignitarian self-determination at the expense of market-based liberty.[232]

C. Unbundling Consent from Contract

Even as consent and contract form distinct legal relationships under the GDPR, platforms may try to tie them together. Specifically, they might condition the provision of goods or services on individuals' consent to data processing for, say, personalized advertisement or market research. Deeply skeptical of the coercive impact of such conditioning, the GDPR limits this practice. GDPR art. 7(4) stipulates in admittedly convoluted terms that "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract . . . is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[233] The Regulation's recitals interpret this provision as a legal presumption against the validity of consent in these instances.[234]

The rationale behind the GDPR's skepticism of tying contract and consent is intuitive. Where consent to data processing beyond what is necessary for the performance of the contract is required to access goods or services, data subjects may feel coerced into consenting to that data processing. This coercion would be incompatible with the GDPR's goals of protecting human dignity and the vision of autonomy over personal data.[235] Power asymmetries vis-à-vis data subjects, the essential nature of their digital services, and market concentration among digital platforms all support the GDPR's

---

[231] *See* Matsumura, supra note 84, at, 79–92 (distinguishing different versions of selves and autonomy).

[232] *See* Whitman, *supra* note 188, at 1160–64.

[233] GDPR art. 7(4).

[234] GDPR rec. 43 ("Consent is presumed not to be freely given … if the performance of a contract … is dependent on the consent despite such consent not being necessary for such performance.").

[235] GDPR art. 1(2).

presumption of coercion.[236] Understandably, the GDPR's authors have addressed bundling in the same provision as power asymmetries. In both cases, individuals' choices would not be genuine or "real," as the EDPB puts it.[237] Applying these standards, the ECJ found in *Meta* that platforms may generally not condition social media services on consent to data processing for personalized advertisement and other content.[238] Similarly, the EDPB's regulatory guidance identifies a photo editing service that demands users to activate GPS geolocation and tolerate data processing for behavioral advertising as an example of prohibited tying.[239]

To practically operationalize real choice, platforms would need to offer their users equivalent data-sensitive alternatives.[240] That is, they would need to offer the same core application without data processing beyond what is necessary for the service, specifically personalized advertisements.[241] If a platform, for example, deliberately degraded security features or throttled functionalities for the data-sensitive option, this option would presumably not satisfy the court's equivalence standard.

1. Privacy Price Control

Excessive subscription fees for data-sensitive options, however, could reduce real choice to absurdity, and thus coerce users into submitting to surveillance. This is why the ECJ found in *Meta* that platforms may charge at most "an appropriate fee" for data-sensitive options, without defining these terms.[242] In reaction to this ruling and the recent decisions by the Irish Data Protection Commission,[243] in November of 2023, Meta switched to a 'pay-or-okay' model.[244] That is, the company relies on consent as a legal basis for

---

[236] Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶¶ 147–151 (July 4, 2023). *See generally* Nikolas Guggenberger, *Essential Platforms*, 24 STAN. TECH. L. REV. 237 (2021) (identifying digital platforms as essential infrastructure).

[237] EDPB, *Guidelines 05/2020 on Consent*, *supra* note 111, ¶ 13.

[238] *Meta*, ECLI:EU:C:2023:537 at ¶¶ 147–151.

[239] EDPB, *Guidelines 05/2020 on Consent*, *supra* note 111, ¶¶ 14–15.

[240] *Meta*, ECLI:EU:C:2023:537 at ¶ 150.

[241] *Id.* For cross-platform combination of users' data *see also* DMA rec. 37.

[242] *Meta*, ECLI:EU:C:2023:537 at ¶ 150. The controlling German version of the decision reads "gegebenenfalls gegen ein angemessenes Entgelt." This formulation does not establish a separate condition of necessity. *But see* EDPB, *Opinion 08/2024 on Valid Consent*, *supra* note 21, ¶¶ 130–132.

[243] *See generally*, *Meta*, ECLI:EU:C:2023:537; Data Prot. Comm'n, Decision *In re.* TSA (Inquiry 18-5-7) (Dec. 31, 2022), https://edpb.europa.eu/system/files/2023-01/instagram_inquiry-18-5-7_final_decision_en.pdf [https://perma.cc/XQU7-36EX]; Data Prot. Comm'n, Decision *In re.* LB (Inquiry 18-5-5) (Dec. 31, 2022), https://edpb.europa.eu/system/files/2023-01/facebook-18-5-5_final_decision_redacted_en.pdf [https://perma.cc/5RYF-ENLY].

[244] Ignacio Cofone, *Meta Charging European Users to Remove Ads is a Privacy Red Herring*, CONVERSATION (Dec. 18, 2023), https://theconversation.com/meta-charging-european-users-to-remove-ads-is-a-privacy-red-herring-218893 [https://perma.cc/CMV6-WYMS].

data processing and offers a 'Subscription for no ads.'[245] The data-sensitive option was originally supposed to cost €9.99 ($10.92) on the web or €12.99 ($14.19) per month on iOS and Android.[246] Meta had planned to charge an additional €6 ($6.56) on the web and €8 ($8.74) per month on iOS and Android for every additional account managed in the same Account Center as of March 1, 2024.[247] Abandoning its original plans, the company then bowed to public pressure and offered to cut fees nearly in half to €5.99 ($6.44) per month.[248] But is Meta's new fee structure 'appropriate'?[249]

At least five distinct interpretations of the appropriateness condition appear plausible.[250] First, the condition may resort to the value of the data that platforms would otherwise extract from users, reflecting a direct extension of the equivalence requirement for data-sensitive alternatives.[251] Relying on the value of data as a benchmark, however, raises a host of follow-up questions. Users' personal data contains not only information about them. Platforms can aggregate the individual's data with millions, if not billions, of other profiles and draw inferences based on insights from this combination, capturing data's higher social value.[252] So, should the price cap reflect the exchange value of the data to the user or their social value to the platform?[253] Both are plausible. Platforms might argue that they aggregate the data and, thus, should be entitled to the resulting value. If, however, the social value became the decisive benchmark, more intrusive data analysis and more effective targeting would allow platforms to charge higher prices for their data-sensitive alternatives.[254]

---

[245] Meta Inc., *Facebook and Instagram to Offer Subscription for No Ads in Europe*, META NEWSROOM (Oct. 30, 2023), https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/ [https://perma.cc/6ZCY-EDN2]; Jacob Kastrenakes, *Facebook and Instagram Launch a Paid Ad-Free Subscription*, THE VERGE, https://www.theverge.com/2023/10/30/23938283/facebook-instagram-ad-free-subscription-eu [https://perma.cc/N9B3-JJU2](Oct. 30, 2023).

[246] Meta Inc., *Facebook and Instagram*, *supra* note 245.

[247] *Id.*

[248] Foo Yun Chee, *Meta Offers to Almost Halve Facebook and Instagram Monthly Fees*, REUTERS (Mar. 19, 2024), https://www.reuters.com/technology/meta-offers-cut-facebook-instagram-monthly-fees-599-euros-2024-03-19/ [https://perma.cc/8NHN-CHL5].

[249] *See* Beschwerde nach Artikel 77(1) DSGVO [Complaint under Article 77(1) GDPR] *In re.* Meta Platforms Ireland Ltd. ¶¶ 40–49 (Nov. 28, 2023), https://noyb.eu/de/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay (challenging Meta's compliance strategy).

[250] *See id.*

[251] *See* Cal. Civ. Code § 1798.125(a)(2).

[252] Ben-Shahar, *supra* note 13, at 114; Bergemann et al., *supra* note 43, at 264 ("The social dimension of the data generates a data externality."); Viljoen, *supra* note 43, at 603–16 (describing relationships between data subjects).

[253] Further differentiating data's social value, see Amanda Parsons & Salome Viljoen, *Valuing Social Data*, 124 COLUM. L. REV. 993, 1009–21 (2024) (distinguishing prediction and exchange value).

[254] Beschwerde nach Artikel 77(1) DSGVO [Complaint under Article 77(1) GDPR] *In re.* Meta Platforms Ireland Ltd., *supra*, ¶ 47.

Next, should the assessment focus on the value of individuals' data, granularly distinguishing between different users or group-based averages? Further complicating things, the marginal social value of a user's data varies with the platforms' data stock. To the extent practical considerations prevent granular assessments of value, the definition of relevant groups would decisively impact the outcome. Relying on averages, whatever the group's boundaries are inevitably undermines the goal of providing equivalent choices on an individual level. For some users, the data-sensitive option would present a great bargain. For others, it would be a prohibitively expensive alternative. It all depends on the commercial value of their personal data relative to that of their group.[255]

Second, one might try to approximate the barter exchange in its entirety when users pay with data. This barter is mainly defined by the value of data extracted by platforms discussed above. Pushing the equivalence criterion to the extreme, however, platforms might point out that data aggregation also aggregates the potential for privacy harm in the form of intrusive targeting with ads or more addictive content—a cost that users bear to some extent.[256] This inflates the "price" of paying with data, which, in turn, could affect the price cap implicit in the conditions for valid consent. Users would then—economically speaking—bear the same costs whether they choose the data-sensitive option or that with personalized advertisements. Yet, although considering these costs might satisfy an economic equivalence criterion, platforms cannot claim a legitimate interest in compensation for users' avoided privacy harms. These harms are costs to users but not consideration for platform services. The inclusion of avoided harms as part of the benchmark for determining valid consent would be inappropriate as part of an assessment that aims to approximate the barter between platforms and users.[257]

The first and second options would both inadvertently incentivize users to 'pay' with data rather than opting for the data-sensitive alternative. As sharing data about us often also reveals information about others, we trade away not only our own privacy but also the privacy of others.[258] Economically, this means that paying with data allows users to shift some of the price they pay for digital services onto third parties. If the value of data to the platform or the barter exchange—including the externalized costs—defines the benchmark for the price cap, the data-sensitive option would always be more

---

[255] *Id.* ¶ 48.

[256] *See* Rosenquist et al., *supra* note 66, at 442–52 (providing medical evidence for the addictive potential of digital technologies and its harm to users). Some privacy harms occur to third parties and society at large see III.A.

[257] These harms also do not represent intended benefits to third parties.

[258] For data's social or third-party effects see III.A.

expensive to individual users. This would, perversely, incentivize privacy harm to others.

Third, the value of platform services could provide the relevant benchmark. And yet, even within the narrow and reductive parameters of price theory—today's dominant approach to measuring value[259]—empirical evidence reveals significant differences depending on the valuation method employed. That is, specifically, differences emerge contingent on whether users are asked to buy (willingness to pay) or forgo platform services (willingness to accept).[260] To complicate things further, the value proposition of platforms changes with their content and growth over time. Larger platforms with more content and greater reach could charge comparatively higher prices for their data-sensitive options, as they tend to provide more value to users. This would likely nudge comparatively more users to consent to data processing for personalized advertising, putting larger platforms at a competitive advantage and magnifying market power's coercive potential in the context of obtaining consent.[261]

Fourth, regulators could limit fees to what sustainably supports the provision of platforms' services on a per-user basis. This approach could draw from a rich tradition of price-setting standards in regulated industries, such as railroad networks or electrical transmission. In these industries, prices are regularly limited to operational costs plus a reasonable return on investment.[262] Costs per user vary greatly among platforms and, generally, decrease with size due to economies of scale. Consequently, smaller platforms would be permitted to charge higher fees for data-sensitive alternatives than large ones. From a policy perspective, these differences could find their justification in the higher risk potential to individuals' autonomy when sharing data with large, powerful entities:[263] "[t]he more power you have, the more additional power you derive from the new data."[264] Drawing from price setting in

---

[259] MARIANA MAZZUCATO, THE VALUE OF EVERYTHING: MAKING AND TAKING IN THE GLOBAL ECONOMY 6–15, 21–74 (2018) (emphasizing that price theory is one of many possible and historically utilized conceptualizations of value and identifying its shortcomings).

[260] Cass R. Sunstein, *Valuing Facebook*, 4 BEHAV. PUB. POL'Y 370, 372–76 (2020) (identifying differences between the willingness to accept and the willingness to pay when measuring the benefits of social media).

[261] Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537 ¶¶ 147–149 (July 4, 2023).

[262] MORGAN RICKS ET AL., NETWORKS, PLATFORMS, AND UTILITIES 147–78 (2022).

[263] The GDPR applies regardless of the size of a company or the purpose of data processing but does establish stricter requirements for especially risky activities *see e.g.* GDPR art. 37. Contrast this with the DSA's tiers of supervisory scrutiny according anticipated risk potentials see DSA arts. 11-43.

[264] Bruce Schneier, *The Myth of the "Transparent Society,"* WIRED (Mar. 6, 2008), https://www.wired.com/2008/03/securitymatters-0306/ [https://perma.cc/KG5R-RTZA]. *See also* Bruce Schneier, *The Battle for Power on the Internet*, ATLANTIC (Oct. 24, 2013), https://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/

regulated industries would also be hard to reconcile with the general thrust of the GDPR and the particular purpose of the price cap; that is, to avoid coercion. If platforms doubt the commercial viability of a low price cap for the data-sensitive alternative, they can always pivot to contextual advertising.[265]

Fifth, and most convincingly, regulators could directly revert to the coercive potential of the platforms' fees.[266] There are at least two plausible approaches to defining coercive power. On the one hand, a realist perspective might suggest emphasizing the actual uptake of privacy-sensitive alternatives. Contentpass, a paywall provider, for example, reports that 99.9% of users consent to tracking instead of shelling out €2.99 ($3.27) for a cross-site subscription for digital content.[267] As activists have argued, it indicates a lack of real choice if almost everyone opts to pay with data despite stated preferences to the contrary.[268] Thus, for choice to be real, prices would need to be low enough that users actually switch, not just theoretically consider it. This method would shield the assessment from the potential pitfalls of a privacy paradox: Individuals may tend to value privacy in the abstract but not act accordingly.[269] Regulators and courts could then treat a data-sensitive alternative that receives barely any uptake as *prima facie* evidence that the associated fee is coercive.[270] Effectively, relying on users' real propensity to switch would cap the acceptable fees for data-sensitive alternatives at minimal levels.

[https://perma.cc/L5Y2-UZ7N](arguing that "technology magnifies power," and "the already-powerful big institutions…had more power to magnify").

[265] *See* III.C.

[266] EDPB, *Opinion 08/2024 on Valid Consent, supra* note 21, at ¶¶ 133–136 (emphasizing autonmy, fairness, and accountability).

[267] Victor Morel et al., *Legitimate Interest is the New Consent - Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls*, Proceedings of the 22nd Workshop on Privacy in the Electronic Society 153, 155–56 (ACM Nov. 2023).

[268] noyb, *Noyb Files GDPR Complaint against Meta over "Pay or Okay"* (Nov. 28, 2023), https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay [https://perma.cc/HP2A-U86N**]**.

[269] *See* Alastair R. Beresford, Dorothea Kübler & Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment*, 117 ECON. LETTERS 25, 26 (2012) (observing that most study participants were willing to share "information about their monthly income and date of birth for a 1 Euro discount"). *See generally* Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, 41 J. CONSUMER AFF. 100 (2007) (popularizing the term 'privacy paradox'); Bernardo Reynolds et al., *Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours*, Human-Computer Interaction – INTERACT 2011 204 (2011); Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S78 (2016) (describing the "privacy paradox"). For a critical account *see* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1 (2021).

[270] It remains possible that users reject the data-sensitive alternative because it lacks certain valued functionalities.

Some may criticize this approach for excluding the possibility of parallel but autonomous decisions in favor of personalized advertising.[271] Yet, both the built-in comparison to actual preferences and the nature of the limitation on tying as a presumption against free choice instead of a hard rule should provide sufficient safeguards. As a matter of policy, focusing on the actual exercise of choice by some percentage of users comes with the benefit of reducing third-party privacy harm. This is because the standard would, by definition, reduce the quota of users consenting to data processing for personalized advertising. Also, as the price would be set to an amount where enough people switch, it would remove the cost-advantage of paying with data in the form of externalizing privacy harm to others.[272]

On the other hand, regulators could rely on a normative definition of a non-coercive fee, representing the values enshrined in the GDPR, and explicitly define a Euro-amount they deem acceptable. The question would then turn from an empirical inquiry into the actual uptake of data-sensitive alternatives to a moral assessment of sufficient autonomy and its quantification. Regulators' and courts' views on morally acceptable barriers to the exercise of data autonomy are inherently hard to anticipate, especially for different types of applications. Based on the emphasis regulators and courts have put on securing data autonomy thus far, however, I would likewise expect a minimal fee cap under this approach.[273]

Objections grounded in concerns for the commercial viability of certain business models or even ongoing provision of specific services are ill-founded. Implicit privacy price control differs from utility price regulation insofar as it does not care about business models or services. It simply functions as a condition for the validity of consent. Platforms remain free to charge any price for their services; they just cannot invoke pricy alternatives to establish that individuals had real choice when consenting to data processing for personalized advertising.

Irrespective of the theory regulators and courts choose to adopt, the relevant comparison for the appropriateness of fees for data sensitive options is contextual advertising—not advertising-free alternatives.[274] This is because contextual advertising is the closest equivalent to personalized advertising,

---

[271] *See* Guohua Wu & Lei Xu, *Demystifying the Privacy-Personalization Paradox: The Mediating Role of Online Trust in Websites/Apps with Personalized Ads and Attitude Towards Online Personalized Advertising*, HCI Int'l 2023 480, 488–89 (2023) (observing increased user trust resulting from personalized advertising).

[272] For data's social effects see III.A.

[273] The 'appropriateness criterion' cannot be construed as a taking of property. Platforms remain free to charge higher prices; they only cannot rely on these higher-priced options to establish they have provided users with real choice.

[274] *Meta* does not compel sales or services; the decision only defines criteria valid consent to personalized advertising.

without the processing of personal data.[275] To the extent that regulators and courts invoke the value of data to platforms as a reference point, platforms could at most resort to the additional revenue generated by personalized over contextual advertising.[276] Relying on Meta's average annual revenue per user as a proxy—$44.60 globally and $75.57 in Europe for Facebook Blue, for example[277]—would thus greatly overestimate the value of users' personal data. To the extent that the fee's coercive impact directly controls the assessment, the relevant users' choice is between personalized advertisements and contextual advertising. After all this, Meta's all-or-nothing 'subscription for no ads' option[278] will presumably not meet the standard of providing real choice.

2. Granular Decision-Making

Although limitations on tying are core to ensuring real choice, providing a data-sensitive alternative for an appropriate fee will not suffice. Instead, users must be free to granularly "consent to particular data processing operations"[279] even if they choose the option with personalized advertising. This requirement applies to all platforms. For platforms designated as gatekeepers, the DMA expressly demands choices on the data sharing with third parties and any cross-platform combinations of data (even within the same company), including signing users in other services provided separately by the platform.[280] Meta's 'pay-or-okay' model likely also violates this requirement, as the European Commission just explained in its preliminary findings on the company's compliance with the DMA.[281]

Furthermore, sensitive categories of data receive special protections under the GDPR.[282] Granular choice must account for these protections.

---

[275] *See* EDPB, *Opinion 08/2024 on Valid Consent*, *supra* note 21, ¶ 121.

[276] European Commission Press Release IP/24/3582, Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act (Jul. 1, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582 [https://perma.cc/JRC3-5WT9]; Beschwerde nach Artikel 77(1) DSGVO [Complaint under Article 77(1) GDPR] *In re.* Meta Platforms Ireland Ltd. ¶ 46 (Nov. 28, 2023), https://noyb.eu/de/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay [https://perma.cc/TWT6-RA4A].

[277] Meta Inc., *Meta Earnings Presentation Q4 2023* 15, https://s21.q4cdn.com/399680738/files/doc_financials/2023/q4/Earnings-Presentation-Q4-2023.pdf [https://perma.cc/U2DE-ZW4P].

[278] *See* Meta Inc., *Facebook and Instagram*, *supra* note 245.

[279] Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537, ¶ 150 (July 4, 2023). *See also* CNIL, Deliberation of the Restricted Committee SAN-2019-001 pronouncing a financial sanction against GOOGLE LLC, ¶¶ 156–57 (Jan. 21, 2019), https://www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf [https://perma.cc/5LKK-FGY7].

[280] DMA art. 5(2).

[281] EC Press Release IP/24/3582, *supra* note 276.

[282] GDPR art. 9. Insofar, it is sufficient if an inseparable operation processes "at least one sensitive data item," Case C-252/21, *Meta*, ECLI:EU:C:2023:537, ¶ 89 (July 4, 2023). *See also* Case

Practically, this means that individuals must be able to separately and explicitly consent, a yet higher standard, to any usage of sensitive personal data that users provide.[283] Recall, however, that the DSA prohibits platforms from using sensitive personal data based on profiling for advertising purposes anyway. Moreover, the decision to personalize organic content in users' newsfeeds must be independent of their choices on advertising.

Finally, recall that each of these choices individually must comply with the standards for real choice, absent coercion. This has repercussions for the appropriateness of fees platforms may choose to charge for data-sensitive alternatives. Effectively, platforms have two options: either they mirror the various granular choices with a granular fee structure or they lower the fee to an amount that renders even the most granular choice possible non-coercive. The former is hardly practical and would invite endless litigation. The latter would reduce the fee to a negligible minimum.

* * *

To summarize, the EU's new regulatory paradigm tightly restricts the extent to which contracts for digital services can define data relations between platforms and users. Obtaining and relying on valid consent instead will be thorny, however. Specifically, platforms must offer equivalent data-sensitive alternatives and granular choice over data usage. Any fees for these alternatives must be appropriate; that is, not coercing users into consenting to personalized advertisements. All this is to say, shifting from contract to consent will insert significant friction into leading platforms' business models.

III. Consent Thicket as Privacy Protection

Dating back to at least Samuel D. Warren II's and Louis Brandeis' article on the "The Right to Privacy," informational privacy has been conceptualized as an individual entitlement resembling some notion of control over information.[284] Especially in the intellectually formative years of today's data protection frameworks, scholars and policymakers focused on individual rights as necessary and sufficient guarantors of privacy.[285] Even interventions like the visionary 1973 U.S. Department of Health, Education & Welfare (HEW) report, which keenly grasped the potential threats stemming from emerging big data analysis, mainly relied on individual entitlements to establish control

---

C-446/21, Maximilian Schrems v. Meta Platforms Ireland Ltd., anciennement Facebook Ireland Ltd. ECLI:EU:C:2024:834 ¶¶ 66-83.

[283] GDPR art. 9(2)(a).

[284] *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[285] *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 24–25 (Lowe & Brydone ed. 1967).

as remedies when it defined 'Fair Information Practices' (FIPs).[286] Starting in the last quarter of the 20th century, compliance regimes complemented individual entitlements with managerial processes and governance mechanisms.[287] Over time, these frameworks professionalized privacy compliance and transformed respect of individual entitlements into checklists.[288] This second wave of privacy law largely defines today's regulatory landscape and legislative proposals.[289] The GDPR operationalizes control most prominently via consent requirements.[290] Control, in turn, functions both as a mechanism to ensure adequate privacy protection and as an objective in its own right, embodying the notion of data autonomy.

Control, however, has remained a mirage, structurally inapt to express data autonomy and insufficient to safeguard privacy both at an individual and a collective level.[291] Demanding that a thick notion of real choice should govern data relations previously structured by contract might therefore be dismissed as naive reinforcement of a flawed concept. Yet, such a dismissal would miss the point. Asking whether real choice enables control and whether control protects privacy is important but not sufficient. Instead of facilitating control, real choice may create a consent thicket that gums up the works of personalized advertising in the EU. Friction can effectively transform consent requirements into a soft data usage limitation, inducing a shift toward less intrusive contextual advertising.

Section A considers to what extent "real choice" amounts to "real privacy." Section B identifies real choice as a source of welcome friction. Section C discusses the impact of friction from real choice on personalized advertising.

---

[286] U.S. DEP'T. OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS: RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, (OS)73-94, at 13–15, 53–57 (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/EV6L-XZD9](mostly relying on individual entitlements); Daniel Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 979–80 (2023) (identifying the HEW report as a milestone in the rise of individual privacy rights) [hereinafter Solove, *The Limitations of Privacy Rights*].

[287] ARI EZRA WALDMAN, ADVANCED INTRODUCTION TO U.S. DATA PRIVACY LAW 14 (2023).

[288] *See generally*, WALDMAN, *supra* note 45.

[289] WALDMAN, *supra* note 288, at 39.

[290] *See e.g.* GDPR arts. 4(11), 6(1)(a), 7(1) – (2), 9(2)(a) (requiring "explicit consent"), recs. 32–33, 42–43.

[291] Richards & Hartzog, *supra* note 43, at 444.

A. 'Real Choice,' Real Privacy?

Data protection frameworks primarily aim to protect individuals' control over personal data and, ultimately, privacy.[292] So, will real choice adequately protect privacy? Unfortunately, the answer is no[293]—and remains 'no' even when accounting for the GDPR's accompanying compliance framework, which includes data protection impact assessments, consultations, and requirements for designated data protection officers.[294]

First, the very idea of privacy as an individual entitlement fails to appreciate the social dimension of data.[295] No doubt, some level of control over one's intimate life is central to a free society.[296] Collecting, aggregating, and analyzing data about humans, however, can have severe consequences beyond specific individuals.[297]

Consider the now infamous example of individuals uploading their genetic information to databases that analyze their ancestry and might match them with relatives.[298] As people upload their genetic information, they not only disclose insights into their genomes but potentially also into their parents', siblings', and children's—even where these insights would not qualify as personal data of these relatives. Insurance companies with access to that information may be able to discriminate against family members who have never consented to the aggregation of that information in the first place. Law enforcement may identify these same family members based on nothing but a DNA sample. Individual entitlements do not account for these third-party effects.[299]

---

[292] GDPR art. 1(1), recitals 1–4 (foregrounding the fundamental right to data protection, whichin the U.S., constitute a privacy right). The GDPR also aims to protect other fundamental rights and to contribute to economic-wellbeing. GDPR recital 2(2).

[293] *See* FRISCHMANN & SELINGER, *supra* note 16, at 314–15; Balkin, *supra* note 43, at 1200; McDonald & Cranor, *supra* note 43, at 563 (arguing that it is impractical for internet users to thoroughly read online privacy policies); Hartzog, *supra* note 43, at 426 (arguing that control is illusory); Richards & Hartzog, *supra* note 43, at 444; Solove, *Privacy and Power*, *supra* note 43, at 1452.

[294] GDPR arts. 35–39.

[295] Viljoen, *supra* note 43, at 592–97, 603–16 (criticizing data protection law's conceptualization of "data as an individual medium"). *See also* Cohen, *What Privacy is For*, *supra* note 43, at 1908 (noting the expansive nature of data sharing).

[296] *See* WESTIN, *supra* note 211, at 24–25 (presenting an expansive understanding of control over privacy needed in a free society).

[297] Bergemann et al., *supra* note 43, at 265 (discussing data externalities); Ben-Shahar, *supra* note 13, at 114 (discussing the harms of data aggregation); Solove, *The Limitations of Privacy Rights*, *supra* note 286, at 990–93; Viljoen, *supra* note 43, at 603–16 (mapping social relations between data users).

[298] *See also* Viljoen, *supra* note 43, at 603–07 (providing a similar example of matching tattoos with a database).

[299] *See* Solove, *The Limitations of Privacy Rights*, *supra* note 286, at 990–93 (providing a similar example based on non-biometric inferences).

Negotiating limitations on how others share their personal data, which could indirectly expose our own information, is virtually impractical. This type of Coasean bargaining for privacy protections fails for several reasons: transaction costs would be disproportionately high, enforcement mechanisms illusionary, and information asymmetries immense. On top of that, even the revealing party regularly fails to appreciate the third-party effects caused by their disclosures.

Furthermore, excessively collecting, aggregating, and analyzing data can undermine social institutions and threaten collective goods. Scholars have analogized surveillance and compared data emissions to pollution, which effectively encapsulate these challenges[300] and underscores the need for democratic data governance that accounts for threats to collective self-governance.[301] The shift from contracts to consent fails to realign governance mechanisms with broader societal interests. Even with heightened protections for individual autonomy, platforms—and individuals—can still overexploit collective privacy for personal gain. The DSA attempts to address these concerns by implementing a tiered compliance framework, calibrating supervisory scrutiny based on platform size and potential systemic risks. Nevertheless, the effectiveness of this new regulation in safeguarding collective interests remains uncertain, as it does not fundamentally alter the underlying business models of digital platforms.

Data protection law's inherent focus on personal data as the object of control[302] exacerbates the problem. An entire industry is built on employing powerful algorithms to draw inferences from data.[303] These inferences enable precise behavioral predictions and probabilistic insights relating to individuals without having to identify them, questioning the very definition of personal data as a distinct category of information and a useful concept for regulation.[304] The new paradigm of real choice does not entail any steps to move beyond the limitations of personal data as the defining regulatory trigger. To the contrary, the shift toward consent and emphasis on dignitarian autonomy further strengthens the notion of a personal entitlement.

Second, even within the general constraints of individual entitlements, users lack the ability to manage their privacy effectively.[305] This mostly

---

[300] Froomkin, *supra* note 43, at 1717–45; *see generally* Ben-Shahar, *supra* note 13.

[301] Fairfield & Engel, *supra* note 43, at 422–24 (identifying the lack of privacy as a public bad, which, the authors argue, represents the flipside of a public good). *But see also* Meg Jones & Paul Ohm, *Voting for Consent*, 104 B.U. L. REV. 1107, 1125–28 (2024) (conceptualizing consent as voting to facilitate collective governance).

[302] *See* GDPR art. 4(11).

[303] Solow-Niederman, *Information Privacy*, *supra* note 43, at 380–81.

[304] *See* IGNACIO N. COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY, 47–49 (2023).

[305] FRISCHMANN & SELINGER, *supra* note 16, at 314–15.

results from structural information asymmetries between platforms and individuals and thinly stretched human attention. To make matters worse, companies have taken full advantage of these asymmetries. Relying on 'dark patterns,' or "deceptive user interfaces,"[306] they obscure privacy harms and lure individuals into over-using digital services and over-sharing information.[307] Regulators and courts may well find some if not most of these deceptive practices illegal under the new paradigm of real choice.[308]

The substantive shortcomings with real choice run deeper, however. One study, for example, estimated that internet users, on average, would have to spend 244 hours or about thirty workdays per year reading the privacy policies of the websites they visit.[309] Dedicating this much time to comprehending privacy policies is not just impractical but also constitutes an excessive waste of resources. This does not even consider that individuals would need to read several policies to compare the provisions and, in the aggregate, create market pressure to level up privacy protections for users. Unsurprisingly, only nine percent of Americans indicated that they always read privacy policies partially or in whole before accepting the terms and consditions.[310] And even adequately informed users may underestimate the consequences of their privacy losses, especially in seemingly banal everyday situations.[311] Meaningful choices about privacy will consequently remain illusionary in most circumstances.[312] Real choice, ironically, suffers from limitations similar to those of boilerplate agreements—a legal framework considered inadequate for protecting individual autonomy.[313]

Critics might respond that individuals' assessments of platforms' data usage are not the only channel of control over privacy. An alternative theory of control could build on experts as intermediaries. Under this theory, not individuals, but public authorities—empowered by the mandates to conduct

---

[306] Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A LIST APART (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/ [https://perma.cc/2MWC-ZTJZ]. For a compliation of bad practices *see Hall of Shame*, DECEPTIVE PATTERNS, https://www.deceptive.design/hall-of-shame.

[307] HARTZOG, *supra* note 8, at 161–62.

[308] CNIL, Deliberation of the Restricted Committee SAN-2019-001, *supra* note 279, at ¶¶ 90–103, 145 (setting forth guidelines for avoiding deceptive practices).

[309] McDonald & Cranor, *supra* note 43, at 563.

[310] Brooke Auxier et al., *4. Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RESEARCH CENTER: INTERNET, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/ [https://perma.cc/4N6L-X7VA].

[311] On the warning function of even minimal requirements of consideration, however, *see e.g.* Keaster v. Bozik, 623 P.2d 1376, 1380, (1981) (finding sufficient consideration in $5 for an option to buy land for $200,000); Wyatt v. Pezzin, 589 S.E.2d 250, 252 (treating one dollar as sufficient consideration for a right of first refusal on a land sale).

[312] Richards & Hartzog, *supra* note 43, at 444.

[313] *See* II.A.

risk assessments and demand mitigation—would analyze platforms' data use and disclosures.[314] Journalists, activists, and academics could take on this role as well, albeit without governmental investigative powers. These experts would then flag problematic platform behavior. Individuals could rely on the experts' analyses and adjust their behavior accordingly.

One might even further extend this critique and question whether control-based frameworks are, in fact, unable to account for third-party effects and exhaustion of collective goods. Public discussion and resulting awareness of privacy harms might influence social norms around the disclosure of personal information and thus affect individual choices. For instance, internalizing the privacy risks to relatives might make us think twice before uploading our genetic information to a database. Social norms around the public health impacts of secondhand smoke, for example, transformed dramatically within a generation. Social structures that sustainably manage our privacy commons might evolve similarly.[315]

These are worthy hopes. As the twenty-fifth anniversary of Google's embrace of surveillance-based advertising approaches, however, the prospect of witnessing meaningful shifts in social norms, enforced only through individual control over data, becomes increasingly implausible. 'Data pollution' resembles greenhouse gas emissions more closely than it does second-hand smoking. Like greenhouse gases, privacy harms are largely invisible, difficult to trace, and possess a global impact.[316] Even well-intentioned individuals may leave digital footprints, not realizing their contribution to third-party or collective privacy harms. All this suggests that the very nature of privacy and surveillance provides ample reason to doubt the emergence of sufficiently harm-mitigating social norms.

B. 'Real Choice,' Real Friction

Rather than empowering users or changing social norms, real choice may primarily function as a vehicle for friction,[317] impeding surveillance-based business models.[318] Enabling real choice, as demanded by the GDPR,

---

[314] *See* Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689) undefined 27; DSA arts. 34-37; GDPR art. 35–39 (describing the designation and responsibilities of data protection officers).

[315] *See* Sari Mazzurco, *Privacy Law's Role in an Information Economy*, 46 CARDOZO L. REV. 123, 175 (2024) (delineating the potential of social norms for privacy protection).

[316] Ben-Shahar, *supra* note 13, at 129.

[317] *See* Richards, *supra* note 34, at 722 (contrasting conscious and frictionless choices about privacy).

[318] *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE 81–100 (2008) (elaborating on the concept of choice architecture and its impact on outcomes).

renders consent onerous to secure, precarious to sustain, restrictive to operationalize, and prone to litigation.[319]

To appreciate how much consent as a legal basis complicates platforms' data extraction, it is worth examining recent regulatory enforcement actions. The French data protection authority (CNIL), for instance, fined Google €50M ($55M) for processing personal data without a valid legal basis.[320] Google had relied on individuals' consent to personalize advertising. The CNIL found users' consent was neither informed nor specific and unequivocal.[321] Beyond the substance of the information, which the CNIL characterized as incomplete, the authority emphasized the importance of how information is presented. The regulator characterized Google's practice of linking documents with more in-depth information as excessively scattering it across multiple documents, which makes the information hard to find.[322] One could, however, come to the opposite conclusion as well: A single, lengthy document might make it harder to find relevant information than smaller pieces connected via hyperlinks. Platforms may invite challenges, no matter how they structure the information.

Additionally, users' consent was deemed not sufficiently specific and unequivocal because granular choices about personalized advertising were located behind a "more options" button, which could be skipped.[323] In doing so, the CNIL set much higher transparency standards for valid consent than enforceable contracts would ever require. The decision, which was upheld in court, illustrates the inherent compliance risk associated with consent as a legal basis. The regulatory framework allows regulators to impose hefty fines—up to 4 % of the annual worldwide turnover under the GDPR and 10% under the DMA, respectively.[324] Future regulatory assessments will all but certainly continue to find deficiencies in the platforms' processes. As an instructive example, look no further than the decades of litigation around appropriate notice of consumer rights in the EU.[325]

---

[319] *See* Cohen, *supra* note 15, at 262 (observing that "there is an intractable tension between the regulatory goal of specific, explicit consent to data collection and processing and the marketplace drift toward convenience"). On the burden consent-based frameworks create for individuals see IGNACIO N. COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY, 94–96 (2023).

[320] CNIL, Deliberation of the Restricted Committee SAN-2019-001, *supra* note 279, at ¶ 189.

[321] *Id.* at ¶¶ 148, 161.

[322] *Id.* at ¶¶ 97–103, 145.

[323] *Id.* ¶¶ 154–157.

[324] GDPR art. 83(5); DMA art. 30(1).

[325] *See* Nikolas Guggenberger, *Rechtsklarheit vs. Rechtswahrheit - Widerrufsbelehrung, Gesetzlichkeitsfiktion Und Die Lehre von Der Fehlerhaften Gesellschaft [Information Concerning the Exercise of Consumers' Right of Withdrawal, the Fiction of Legality, and the Doctrine of De Facto Corporation]*, 9 ZGS 397 (2011); Jonathon Watson, *Withdrawal Rights*, *in* RESEARCH HANDBOOK ON EU CONSUMER AND CONTRACT LAW 241, 249–55 (Christian Twigg-Flesner ed., 2016).

Compliance risks under the real choice paradigm are even more pronounced for firms with market power.[326] Although the ECJ dismissed the notion that a company's dominant market position inherently negates individuals' ability to choose freely, it acknowledged the possible coercive influence of such a position as a component in a holistic evaluation.[327] This puts the validity of consent on even shakier grounds for platforms with market shares like Meta's, currently standing at 89% for social media services in Europe and 60% in the U.S.[328] Effectively, real choice progressively inserts friction by setting higher bars for valid consent for platforms with market power—almost like a tax on market power.

Implementing the conditions for valid consent will require sophisticated consent management processes and increase operational costs. For users, more substantive and frequent choices may disrupt sign up processes and user experience, which may deter some customers entirely in the process. Although users already regularly click through simple consent boxes, behavioral science shows that even minimal additional doses of friction can determine outcomes—whether it is about opting for clean energy or overeating on candy.[329] The exact impact will depend on platforms' ability to smooth the process of obtaining consent. Smoothing itself, however, may create additional compliance risks. It is very plausible that data protection authorities would insist on some friction in the process to preserve the consent's warning function and enable deliberation.[330]

Moreover, relying on consent instead of contract inserts additional uncertainty into platforms' business model, because users can withdraw consent at any time. The practical impact of users' right to withdraw consent, however, is limited by the fact that platforms can infer analytical insights immediately when collecting users' data.[331] Irrespective of a later withdrawal of consent, the platforms keep the inferred knowledge. Yet, exiting from the data relation by withdrawing consent is easier than terminating a service contract

---

[326] *See* EDPB, *Opinion 08/2024 on Valid Consent*, *supra* note 21, ¶¶ 66–168, 90–110.

[327] Case C-252/21, *Meta Platforms Inc. v. Bundeskartellamt*, ECLI:EU:C:2023:537, ¶¶ 147–149 (July 4, 2023).

[328] *Social Media Stats Europe*, STATCOUNTER, https://gs.statcounter.com/social-media-stats/all/europe [https://perma.cc/F8GV-G7GM]; *Social Media Stats United States of America*, STATCOUNTER, https://gs.statcounter.com/social-media-stats/all/united-states-of-america.

[329] *See* STEPHAN J. GUYENET, THE HUNGRY BRAIN: OUTSMARTING THE INSTINCTS THAT MAKE US OVEREAT 98–99, 230–31 (2017) (recommending minor changes to our food environment to prevent overeating); THALER & SUNSTEIN, *supra* note 241, at 194–96 (discussing the impact of defaults on clean energy uptake); B. Wansink, JE Painter & Y-K Lee, *The Office Candy Dish: Proximity's Influence on Estimated and Actual Consumption*, 30 INT. J. OBES. 871, 874 (2006) (showing that "the proximity and visibility of a food can consistently increase an adult's consumption of it").

[330] Authorities may base that demand on the fairness principle, *see* GDPR art. 5(a), or privacy by design requirement, GDPR art. 25(1), for example.

[331] ZUBOFF, *supra* note 6, at 74–82.

entirely under surveillance by adhesion. This is because under real choice, individuals can continue to use the platforms' digital services.

Regardless of withdrawals, platforms will be required to obtain users' consent afresh whenever they modify the purpose or expand the scope of data processing. The GDPR mandates that the purpose of data processing be clearly defined in advance.[332] Consequently, individuals cannot consent to unknown future data usage and—in contrast to contractual assent—data consent cannot permit future unilateral changes by the platform. The transition from relying on contracts to requiring consent as a legal basis can thus significantly complicate pivoting business models or introducing new services; a challenge Meta has recently encountered. Outside the EU, Meta scaled up Threads, a micro-blogging platform akin to X (formerly Twitter), in record speed because it could leverage its enormous social graph and freely combine data from its various applications.[333] The GDPR, however, required Meta to obtain consent from its users to combine data across its platforms because the combination would amount to an additional purpose of processing users' personal data.[334] Due to regulatory concerns, Meta postponed the rollout of Threads within the EU.[335] Effectively, the limitation on future data uses inherent to the legal basis of consent significantly lowers the commercial value of data extracted from individual users in the first place.

Real choice may also exert friction by diminishing the commercial value of data to the platform at an aggregate level: If some users switch to data-sensitive alternatives, they reduce the social value of the data platforms extracted from other people. This can manifest in two ways. Platforms can no longer use their collected data to personalize advertising for as many users, even though the marginal costs of doing so would have been close to zero. At the same time, platforms will have less data to fine-tune their algorithms and personalize advertisements for those users who continue to 'pay' with their data. If the authorities limit the price for data-sensitive alternatives to levels that lead to actual switching,[336] the diminishing social value of users' data becomes all but automatic.

---

[332] GDPR rec. 39.

[333] Alex Heath, *Why Instagram is Taking on Twitter with Threads*, THE VERGE (Jul. 5, 2023), https://www.theverge.com/2023/7/5/23784870/instagram-threads-adam-mosseri-interview-twitter-competitor [https://perma.cc/L32D-SLTS**]**.

[334] Makena Kelly, *Here's Why Threads is Delayed in Europe*, THE VERGE, https://www.theverge.com/23789754/threads-meta-twitter-eu-dma-digital-markets [https://perma.cc/L64N-MJP9**]**.

[335] Adam Mosseri, the head of Instagram, explained the unavailability of Threads in the EU as related to "the complexities with complying with some of the laws coming into effect next year," which was understood as a hint at the DMA, *see* Heath, *supra* note 329. *See also* Kelly, *supra* note 330.

[336] *See* II.C.1.

Finally, note that consent cannot overcome the GDPR's substantive limits on data processing.[337] And in line with the GDPR's vision of protected autonomy, the ECJ in October of 2024 clarified that GDPR's data protection principles, including fairness, data minimization, and proportionality apply to any data processing for the personalization of advertisements regardless of its legal basis.[338] Most notably the "principle of data minimization … precludes all of the personal data … from being aggregated, analysed and processed for the purposes of targeted advertising without restriction as to time and without distinction as to type of data."[339]

C. From 'Real Choice' to Contextual Advertising

If the real choice requirement renders consent sufficiently onerous to secure, precarious to sustain, restrictive to operationalize, and prone to litigation, it will undermine the commercial viability of personalized advertising.[340] Platforms will presumably switch to less intrusive contextual advertising. Essentially, the new paradigm may function as a soft data usage limitation. It is 'soft' because it does not explicitly ban certain data usages; instead, it incidentally discourages platforms from certain harmful practices by increasing the costs of the underlying data processing and diminishing expected profits. This conclusion holds true even if we assume that personalized advertising is effective.[341]

Contextual advertising, the norm for most of the twentieth century, may well return to its old prominence, mitigating some of the negative side- effects associated with granular personal targeting. As the name suggests, contextual advertising relies on context. An advertisement for sports gear might follow a post about soccer; the hashtag #knitting might invite coupons for wool. Contextual advertising does not tailor messages to the intended recipient and, therefore, neither requires behavioral tracking nor behavioral profiles

---

[337] On the mainly procedural nature of data protection provision *see* IGNACIO N. COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY, 97–103 (2023).

[338] *See* Case C-446/21, Maximilian Schrems v. Meta Platforms Ireland Ltd., anciennement Facebook Ireland Ltd. ECLI:EU:C:2024:834 ¶¶ 47-51.

[339] Case C-446/21, Maximilian Schrems v. Meta Platforms Ireland Ltd., anciennement Facebook Ireland Ltd. ECLI:EU:C:2024:834 ¶ 65.

[340] On deliberate friction as a regulatory tool see *supra* note 28. For ample evidence that friction in the privacy choice architecture for users has significant impact on commercial outcomes consider the decades of political fights over privacy defaults, namely opt-in versus opt-out rules. See Michael E. Staten & Fred H. Cate, The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA, 52 *Duke Law Journal* 745, 769–783 (2003); Jeff Sovern, *Opting in, Outing out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

[341] *See* ZUBOFF, *supra* note 6, at 63–92. *But see* HWANG, *supra* note 6, at 72–87 (doubting the effectiveness and the value of online advertising); Hoofnagle, *supra* note 70, at 42–48 (identifying no cognizable value in personalized advertising beyond brand awareness and political influence).

of individuals. In fact, personal data need not be processed at all. Rather, advertisements can be matched with specific signaling clues like words or pictures. Because the GDPR only applies to the processing of personal data,[342] it would not constrain contextual advertising. On the contrary, embracing contextual advertising may even be seen as an expression of privacy by design principles[343]—at least, compared to current practices.

No doubt, where context becomes very fine-grained, however, the lines between contextual and personalized advertising may start to blur.[344] Consider combinations of rare interests—maybe so rare that only one or a few people share them. In these cases, context may be sufficient to identify individuals. Anonymous location data may likewise reveal actual identities when put in context. Where that is the case, the delivery of advertisements would, in fact, involve the processing of personal data.[345] And whenever platforms crossed the line to using "information relating to an identified or identifiable natural person" for personalized advertising, they would need to revert to consent.[346]

Recent scholarship indicates that contextual advertising can be effective for many applications.[347] At the same time, some evidence suggests that platforms have oversold personalized advertising, which may not be sustainable.[348] Either way, the prospect of avoiding the newly-elevated operational costs and evading regulatory scrutiny while offering a marginally lower value proposition to advertisers may induce some platforms to switch. Platforms located near a potential point of sale—like Amazon or Google—may find it easier to adopt contextual advertising effectively than those that tend to be further removed—like Meta or YouTube. [349]

A shift from personalized to contextual advertising could yield several benefits. These benefits need no further explanation if one understands the exploitation of personal data as an inherent moral wrong. In more consequentialist terms, changes to the business model would mitigate some of the harms associated with personalized advertising. For example, less granular targeting holds less potential for discrimination. Although in some instances, contextual proxies might lead to similar outcomes. This is because many of our interests, for example, track our racial, ethnic, sexual, gender, and religious identities.

---

[342] GDPR art. 4(11).

[343] *See* GDPR art. 25(1).

[344] FTC, *Staff Report*, *supra* note 31, at iii.

[345] *See* Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779, ¶ 49 (Oct. 19, 2016) (holding that dynamic IP addresses can constitute personal data).

[346] GDPR art. 4(1).

[347] Hoofnagle, *supra* note 70, at 43–44.

[348] HWANG, *supra* note 6, at 75–91.

[349] *See* Hoofnagle, *supra* note 70, at 43–44.

Because contextual advertising does not build on personality profiles, it is also somewhat less prone to playing into our (worst) instincts. Granted, it might be overly tempting for some to see a burger during a football match and outright harmful for others to encounter advertisements for alcoholic beverages in rehabilitation forums, but contextual links remain less manipulative than personalized ads. That is because context is less sticky than personality. Context does not build up a history from which it generates subsequent recommendations and predictions. If users search for a different product or read the comments under a different post, they would be served different advertisements—ones that match the novel content, reducing the path dependence of prior behavior. A similar logic applies to polarization and partisanship, in which personalizing context supercharges the impact of misleading and aggravating content. As contextual advertising lacks behavioral memory, it is somewhat less prone to perpetuating political and cultural radicalization.

Moreover, contextual advertising leaves the decision to initiate the exposure to context to individuals; that is, within the constraints of the applications' choice architecture. Consider search engines. If we search for a term and are exposed to contextual advertisements, at least we have set the initial agenda, as opposed to Google or Bing, for example. Granted, searches often occur in context and one search might lead to another, which can guide subsequent searches and open the door for manipulation. Furthermore, contextual connections might be opaque, so much so that our setting a search agenda might lose its character as a deliberate expression of autonomy. Again, because contextual advertising lacks behavioral memory, however, the agenda setting would frequently occur anew, constantly affording individuals opportunities to reset the direction of their experiences.

All that said, switching to contextual advertising does not eliminate the conflicts of interest at the core of all advertising-funded services. As Google's founders Sergey Brin and Lawrence Page observed in 1998, selling users' attention to advertisers incentivizes prioritizing advertisers' interests over those of users, for example, by inserting bias in search algorithms.[350] It also rewards addictive features and can ultimately harm users' mental health, even inviting regulatory interventions that would discourage the practice entirely.[351] Despite that, returning to contextual advertising would mitigate

[350] Sergey Brin & Lawrence Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, 30 COMPUT. NETWORKS & ISDN SYSTS. 107 (1998) ("[W]e expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers.") (Appendix A available at http://infolab.stanford.edu/~backrub/google.html) [https://perma.cc/HZ9H-C6JH**]**.

[351] *See* Paul Romer, *Taxing Digital Advertising*, adtax.paulromer (May 17, 2021), https://adtax.paulromer.net/ (proposing a progressive Pigouvian tax on advertising revenues).

platforms' abilities to act upon their misaligned incentives: extreme gamification and dark patterns luring people into overconsumption would lose their personal tailoring and, thus, some of their deceptive power. To further mitigate conflicts of interest, platforms would need to ditch advertising as a funding model altogether—opting instead for a subscription-only model, for example—but this appears unlikely.[352]

IV. Friction from Consent as a Regulatory Tool for the U.S.

Like in the EU, individual control features prominently in the U.S. data privacy framework—yielding similarly insufficient privacy protections.[353] "[P]rivacy self-management," as envisioned by policymakers and regulators, has remained illusory.[354] Despite the FTC's laudable efforts to move beyond data control,[355] however, there is ample reason to believe that individual control will remain a staple of the regulatory toolkit.[356] Adopting a realpolitik approach to privacy,[357] I contend that policymakers and regulators in the US should leverage friction from fortified notions of consent into soft but powerful data usage limitations to end personalized advertising and similarly harmful business practices.[358] Part A discusses the limitations of privacy realpolitik and necessity of residual control. Part B proposes that policymakers and regulators reject contractual imperatives, and Part C calls for a leveraging of choice as welcome friction in the US.

---

[352] Advertising has cost, scaling, tax, and psychological advantages for platforms over subscription fees. *See* Alex Hern, *WhatsApp Drops Subscription Fee to Become Fully Free*, Guardian (Jan. 18, 2016), https://www.theguardian.com/technology/2016/jan/18/whatsapp-drops-subscription-fee-free [https://perma.cc/FP3R-4W9J]; Daniel Markovits, X (formerly Twitter) (Oct. 4, 2021), https://twitter.com/DSMarkovits/status/1445133991825248261 [https://perma.cc/9VUJ-VC2L].

[353] Richards & Hartzog, *supra* note 43, at 444.

[354] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1883 (2013); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 590–95 (2014).

[355] FTC, Remarks of Chair Lina M. Khan, As Prepared for Delivery IAPP Global Privacy Summit 2022, 6 (Apr. 11, 2022), https://www.ftc.gov/news-events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022 [https://perma.cc/96ZX-SZ5M]; McGeveran, *supra* note 42, at 198–207.

[356] Waldman, *supra* note 45, at 6 ("The dominant privacy discourse today…centers around notions of choice, consent, and control").

[357] For privacy protection within economic, constitutional, and factual constraints *see* A. Michael Froomkin, *The Death of Privacy*, 52 Stan. L. Rev. 1461, 1524–38 (2000).

[358] *See also* Brett M. Frischmann & Moshe Y. Vardi, *Better Digital Contracts* 1, 8 (Aug. 6, 2024), https://papers.ssrn.com/abstract=4918003 [https://perma.cc/9DCQ-DDLJ](proposing pro-social friction-in-design for digital contracting).

A. Privacy Realpolitik and Residual Control

At the federal level, the FTC polices a notice and choice framework to enable control over personal information.[359] Platforms inform the public about their intended usage of personal information (notice). Individuals can then decide to use the services offered and share their personal information (choice). The current self-regulatory framework for online data privacy has its roots in Fair Information Principles, developed in the 1970s[360] and was more recently shaped by a 1995 Clinton administration report to overcome individuals' reluctance to share information online and "encourage the vigorous consumer activity needed to unlock the full potential of the information infrastructure."[361] At the state level, nineteen different fundamentally control-based data privacy regimes have emerged.[362] No doubt, a radical reorientation of privacy protections is urgently needed.[363] For several reasons, however, the regulatory landscape will likely remain entrenched in the control paradigm for the foreseeable future.

First, fundamental realignment of the FTC's enforcement practices will take time,[364] is dependent on consistency within the FTC's leadership, and ultimately faces a "hostile judiciary."[365] In 2022, FTC Chair Lina Khan decisively broke with the agency's approach to safeguarding privacy online when she labeled notice and choice "outdated and insufficient" and called for substantive limitations instead.[366] The announced shift from primarily policing deceptive claims in privacy policies to more directly addressing the unfairness of business practices indeed holds promise for more effective privacy

---

[359] Solove, *supra* note 346, at 1883; Solove & Hartzog, *supra* note 346, at 592.

[360] IGNACIO N. COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY, 12–14 (2023).

[361] U.S. DEP'T OF COM., PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION, 2 (1995); Chander, *supra* note 188, at 665–66.

[362] C Kibby, *US State Privacy Legislation Tracker*, IAAP (Nov. 18, 2024), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/N95K-9RW6].

[363] *See* III.A.

[364] *See* Solove & Hartzog, *supra* note 346, at 606–27 (likening the FTC's enforcement actions to a common law framework that develops over time).

[365] Darren Bush & Spencer Weber Waller, *Using Consumer Protection Law to Achieve Competition Policy Goals* 4 (U. Hous. L. Ctr. Pub. L. & Legal Theory Rsch. Paper Ser., No. 2024-A-4, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4714225 [https://perma.cc/BF3W-BZT2](observing a "generally conservative and hostile judiciary").

[366] FTC, Remarks of Chair Lina M. Khan, As Prepared for Delivery IAPP Global Privacy Summit 2022, 6 (Apr. 11, 2022), https://www.ftc.gov/news-events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022 [https://perma.cc/UXG4-5V92]; Herrine, *supra* note 36 (observing a shift away from consumer sovereignty). *See also* FTC Staff Report, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services i–iii (Sep. 2024), https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services [https://perma.cc/9BAS-X9M2] (Statement by Samuel Levine, Director, Bureau of Consumer Protection).

protection.[367] And precedent in cyber security law may give some hope that courts will uphold substantive restrictions on data usage under the unfairness prong in Section 5 of the FTC Act, even as Congress has failed to pass substantive legislation for decades.[368] Yet, assuming the FTC stays course and articulates substantive guardrails over time, a reorientation of the fundamental principles of privacy protection will face an uphill battle in the courts. Banning personalized advertising may well be seen as a "major question," requiring "clear congressional authorization."[369] Narrowing the FTC's room for maneuver in the absence of such clear authorization, in 2024 the Supreme Court in *Loper Bright Enterprises v. Raimondo* overruled the long-standing *Chevron* doctrine[370] and held that under the APA, "agency interpretations of statutes . . . are not entitled to deference."[371]This presumably leaves the FTC only with "*Chevron*'s doctrinal complement, *Skidmore*" deference,[372] referring to *Skidmore v. Swift*.[373] This doctrine "treat[s] an agency's views as evidence of statutory meaning," before finding ambiguity in a statute.[374] Effectively, these limitations put FTC rulemaking and major enforcement shifts in the area of privacy protection on shaky grounds.

Second, consider Congress' most recent and promising attempt to pass omnibus federal privacy legislation, the American Privacy Rights Act (APRA).[375] This can help to assess the Overton window.[376] If passed, the bill will grant individuals privacy rights, including access, correction, deletion, export, and opt-outs from certain practices.[377] To process sensitive data, covered entities would need to obtain express affirmative consent.[378] Data minimization—a concept that reaches beyond individual choice and is meant to

---

[367] MCGEVERAN, *supra* note 42, at 198–207.

[368] 15 U.S.C. § 45(a)(1); F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015).

[369] *See West Virginia v. EPA*, 142 S.Ct. 2587, 2609 (2022) (calling the major questions doctrine an "identifiable body of law that has developed over a series of significant cases all addressing a particular and recurring problem"); *Utility Air Regulatory Group v. EPA*, 573 U.S. 302, 324 (2014) (cited in *West Virginia v. EPA* as evidence of the existence of an "identifiable body of law" now labled major questions doctrine).

[370] *See Chevron*, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 843 (1984).

[371] Loper Bright Enters. v. Raimondo, 144 S.Ct. 2244 , 2261 (2024).

[372] Ryan D. Doerfler, *How Clear is "Clear"?*, 109 VA. L. REV. 651, 707 (2023). *See generally*, Cary Coglianese & Daniel E. Walters, The Great Unsettling: Administrative Governance After Loper Bright, ADMIN. L. REV. (forthcoming 2025) (arguing that it is unclear what the overruling of the *Chevron* doctrine practically means)

[373] *See generally* Skidmore v. Swift & Co., 323 U.S. 134 (1944).

[374] Doerfler, *supra* note 363, at 707.

[375] American Privacy Rights Act, H.R. Res. 8818, 118th Cong. (2024).

[376] *See* Solow-Niederman, *supra* note 42, at 1013–18.

[377] CHRIS D. LINEBAUGH ET AL., CONG. RSCH. SERV., LSB1116, THE AMERICAN PRIVACY RIGHTS ACT 2 (2024).

[378] H.R. 8818, at § 102(b); CHRIS D. LINEBAUGH ET AL. *supra* note 370, at 2.

limit data processing to the necessary extent—features more prominently than in existing legal frameworks.[379] Despite this, individual control still takes center stage. The new rights, paired with the definition of covered data that demands a direct connection to the individual aim to operationalize control, are all expressions of individual entitlements. The section containing the bulk of individuals' rights is even titled "Individual Control over Covered Data."[380] To be clear, there are bills, like the Banning Surveillance Advertising Act, aiming to ban personalized advertising directly.[381] These attempts have not garnered meaningful support thus far, however. All this is to say, the privacy reform proposals that double-down on individual control as the guiding regulatory paradigm have the best chances of passing.

Third and relatedly, the broader political economy remains favorable to notions of control over data.[382] Narrowly defined exceptions to control-based thinking prove the rule. Restrictions in niche areas like the "limitations on the sharing of account number information for marketing purposes" in the Gramm-Leach-Bliley Act fall into this category, as do the more ambitious but local efforts to ban facial recognition.[383] Although there is public support for bans on selected practices, such as facial recognition by social media platforms[384] and exploitation of children, and comprehensive federal privacy regulation,[385] polls dating back to the early 2000s consistently show support for individual control over personal data.[386] On the one hand, Americans largely perceive a lack of control over their data; on the other hand, they also overwhelmingly "trust themselves to make the right decisions about their personal information."[387] The alignment of natural instincts,[388] false hopes, and

---

[379] H.R. 8818, at § 102.

[380] *Id.* at § 105.

[381] Banning Surveillance Advertising Act of 2023, S.2833, 118th (2023).

[382] WALDMAN, *supra* note 45, at 6. *See also* Ohm & Frankle, *supra* note 34, at 835 (positively assessing the political economy of deliberate friction).

[383] 15 U.S.C § 6802(d), 12 C.F.R. 40.12(c)(1). *See* MCGEVERAN, *supra* note 42, at 923–24; Prentiss Cox, *The Invisible Hand of Preacquired Account Marketing*, 47 HARV. J. ON LEGIS. 425, 464–66 (2010); Rowe, *supra* note 40, at 43 (observing local governments' efforts to ban public use of facial recognition).

[384] Lee Rainie et al., *AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns*, PEW RESEARCH CENTER 41 (Mar. 2022), https://www.pewresearch.org/science/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns/ [https://perma.cc/SQ3B-DGNB].

[385] Colleen McClain et al., *How Americans View Data Privacy*, PEW RESEARCH CENTER 17 (Oct. 18, 2023), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2023/10/PI_2023.10.18_Data-Privacy_FINAL.pdf [https://perma.cc/UQ4T-Q86G].

[386] Electronic Privacy Information Center, *EPIC - Public Opinion on Privacy*, https://archive.epic.org/privacy/survey/ [https://perma.cc/VQ4R-3T4Y].

[387] McClain et al., *supra* note 376, at 7.

[388] Margot E. Kaminski, *The Case for Data Privacy Rights (Or Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 390 (2022) ("[I]ndividual rights reflect what most people think of when they think of privacy.").

industry interests in preventing meaningful, substantive limitations of their practices impedes transformative changes.[389] Against this background, it comes as little surprise that federal privacy bills and state-level regulation have continued to rely on control as a regulatory tool.

Fourth, as mentioned above, nineteen states' new omnibus privacy laws fundamentally build on various notions of individual control, facilitated through individual entitlements and transparency requirements.[390] Some contain rights of action, while others rely entirely on public enforcement.[391] Leaving aside all variance in detail, these control-based frameworks are established; their enforcement will define privacy protections for millions of Americans. No doubt, reforms and adjustments are always on the table. But it is hard to imagine that the frameworks' fundamental logic will be turned upside down any time soon. Take for example the California Consumer Privacy Act (CCPA), as recently amended by the Privacy Rights Act (CPRA).[392] The pioneering state privacy law involves elaborate protection mechanisms, complex compliance guidelines developed by a new agency, the California Privacy Protection Agency, and complicated amendment processes.[393] Businesses, in turn, have implemented the new regime and adjusted their business practices accordingly. All this creates vested interests in the status quo, mobilizes lobbyists, and enforces path dependencies for the regulatory trajectory.[394]

Finally, even if we universally adopted democratic visions of data governance, a free society must preserve space for individual control over personal data.[395] This is because control can be essential for self-expression, both as speech and identity. People may want to share intimate information with trusted circles, but not the public at large.[396] They may deliberately want to nurture different images: a private and a professional character or an intimate

---

[389] *See* WALDMAN, *supra* note 37, at 81–83 (observing industry agenda setting that foregrounds control).

[390] Kibby, *supra* note 353.

[391] *Id.*

[392]

[393] Proposition 24 § 24 (Cal. 2020); ERIC GOLDMAN, INTERNET LAW: CASES & MATERIALS 369, (2022) (observing that "[t]his makes it virtually impossible for California to sync with other states' laws" and predicting that "the one-way-ratchet almost certainly will be a no-way-ratchet"); MCGEVERAN, *supra* note 42, at 319–21.

[394] Caitriona Fitzgerald, Kara Williams & R.J. Cross, *The State of Privacy: How State Privacy Laws Fail to Protect Privacy and What They Can Do Better*, ELEC. PRIVACY INFO. CENTER & U.S. PIRG EDUC. FUND 15 (Feb. 2024), https://epic.org/release-report-state-laws-are-failing-to-protect-privacy/ [https://perma.cc/5SL3-9W3H**]**.

[395] Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 734 (1999) (emphasizing the delicate balance between forced privacy and control); Kaminski, *supra* note 379, at 393. *See also* WESTIN, *supra* note 211, at 42 ("A free society leaves this choice [about reserve and disclosure] to the individual, for this is the core of the 'right of individual privacy.'").

[396] NEIL RICHARDS, WHY PRIVACY MATTERS 29–32 (2022).

and public persona, for example.[397] As an illustration, consider the tragic story of Oliver (Billy) Sipple.[398] After thwarting an assassination attempt on President Gerald Ford in 1975, the San Francisco Chronicle nationally outed him as homosexual.[399] Although Sipple had already been public about his sexual orientation in San Francisco, he didn't want his family in Michigan to know.[400] By rejecting Sipple's claim for invasion of privacy based on considerations of speech and press freedoms,[401] courts ultimately refused him the ability to define his identity within the respective contexts.[402] Whether or not one shares the California Court of Appeals' conclusions in the 1984 case of *Sipple v. Chronicle Publishing*, the very idea of sexual informational privacy is hard to imagine without reverting to some notions of individual control over information.[403] Therefore, as a new privacy consensus gains traction, it would have to accommodate some level of individual control over personal information or risk undermining both human identity and, consequently, the collective self-determination it sought to better protect in the first place.

Thus, within the constraints of privacy realpolitik and the inevitability of residual elements of control, a primary concern is the extent to which regulators can leverage control-based frameworks to curb the excesses of informational capitalism. Where democratic data governance is unattainable or impractical, friction from granular articulations of consent offers a powerful second-best regulatory option.

B. Rebuking Contractual Imperatives

As a first step toward embracing friction, policymakers and regulators should reject contractual imperatives that prioritize efficiency and obedience for data relations.[404] Conceptually, this demands recognizing data relations as independent from service contracts.[405] More specifically, policymakers and

---

[397] *See* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF 129–31 (2012); RICHARDS, *supra* note 310, at 29–32.

[398] Dan Morain, *Sorrow Trailed a Veteran Who Saved a President and Then Was Cast in an Unwanted Spotlight*, L.A. TIMES (Feb. 13, 1989), https://www.latimes.com/archives/la-xpm-1989-02-13-vw-1568-story.html [https://perma.cc/L24Z-KL4A].

[399] *Id.*

[400] *Id.*

[401] Sipple v. Chronicle Publishing Co., 154 Cal. App. 3d 1040, 1049 (1984).

[402] RICHARDS, *supra* note 310, at 31–32.

[403] Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1882–88, 1909–24 (2019) ("Being able to reveal one's naked body, gender identity, or sexual orientation at the pace and in the way of one's choosing is crucial to identity formation.").

[404] On contractual ordering of data relations *see* Janger & Schwartz, *supra* note 71, at 1248.

[405] *See* Balkin, *supra* note 35, at 1205–07 (suggesting fiduciary relationships governed by tort separate from contractual agreements). For a conceptually related proposal to detangle business to consumer contractual relationships by distinguishing between consent to the transaction and assent

regulators should construct disclosures of and consent to data practices insulated from the overly permissive norms in contract law—approximating the GDPR's approach.[406] Although U.S. privacy frameworks generally do not require justifications for data usage, let alone consent,[407] individuals' consent may be required to diffuse otherwise successful intrusion claims,[408] or to satisfy sector-specific requirements. Take the Fair Credit Reporting Act (FCRA)[409] or the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule,[410] for example.[411] Both frameworks feature consent requirements,[412] and courts have already moved beyond contract law's low thresholds for assent. In this spirit, platforms' "disclosures must have only one plausible interpretation" to provide a valid basis for consent.[413] And platforms bear the burden of proof.[414] 45 CFR § 164.508(b)(4) restricts the conditioning of health services on patient's authorization to use medical information, a heightened form of consent for especially sensitive information. All this goes to show that some parts of the American privacy framework already require justifications for data usage and even reach beyond contractual norms.[415] Policymakers and regulators can extend their logic.

State privacy frameworks provide an even clearer basis for a conceptual separation of data relations and circumstantial contracts. In parallel to the GDPR, the CCPA, for instance, rejects contractual imperatives and fortifies choice. First, it offers the basis to second-guess the subject matter of contractual agreements where these agreements otherwise define data subjects' individual rights. The Right to Limit Use and Disclosure of Sensitive Personal Information, for example, enables "the consumer to limit [a business'] use of the consumer's sensitive personal information to that use which is necessary to perform the services . . . expected by an average consumer."[416] Put differently, the expectations of average consumers about the kind of service—as

---

to boilerplate see Andrea J. Boyack, The Shape of Consumer Contracts, 101 Denver Law Review 1, 43-50 (2023).

[406] *See* II.B., C.

[407] MCGEVERAN, *supra* note 42, at 339–40, 875.

[408] *See* Hammerling v. Google LLC, 615 F. Supp. 3d 1069, 1087–91 (N.D. Cal. 2022); In re Google Assistant Priv. Litig., 546 F. Supp. 3d 945, 957–59 (N.D. Cal. 2021); McCoy v. Alphabet, Inc., 2021 WL 405816, at *6–8 (N.D. Cal. Feb. 2, 2021).

[409] 15 U.S.C. § 1681 et seq.

[410] 42 U.S.C. § 264; 45 CFR § 164.

[411] *See* MCGEVERAN, *supra* note 42, at 395–96, 875 (identifying FCRA and HIPPA Privacy Rule as data protection frameworks).

[412] 15 U.S.C. § 1681b; 45 C.F.R. § 164.506(a), (b) (for non-routine uses).

[413] *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021). *See also In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793–94 (N.D. Cal. 2022).

[414] In re Meta Pixel Healthcare Litig., 647 F. Supp. 3d at 793; *Calhoun*, 526 F. Supp. 3d, at 620.

[415] Balkin, *supra* note 35, at 1200–1202.

[416] Cal. Civ. Code § 1798.121(a).

determined by regulators and courts—define the extent of consumers' rights to limit data usage, not platforms' terms of service.

Second, like the GDPR, California recognizes that meaningful choice requires plausible options to choose from. The GDPR incorporates this recognition directly into the standards for valid consent, requiring real choice.[417] The CCPA achieves a similar outcome by prohibiting platforms from penalizing consumers for exercising their rights.[418] This anti-retaliation provision implicitly recognizes a data relation separate and independent from the service contract. Practically, the provision amounts to a price cap on data-sensitive alternatives, which platforms must offer to their users. To comply with the CCPA, any difference in price between the default and the data-sensitive option must be "reasonably related to the value provided to the business by the consumer's data."[419] Other than the EU's paradigm of real choice, however, the CCPA only selectively ends some aspects of surveillance by adhesion. This is because the CCPA only grants rights to "Opt Out of Sale or Sharing of Personal Information" and to "Limit Use and Disclosure of Sensitive Personal Information."[420] In a glaring loophole to more effective privacy protection, it does not rein in the first-hand use of non-sensitive personal information in the same manner. Policymakers and regulators should expand the category of sensitive data to rebuke contractual imperatives governing personalized advertising more effectively and lay the groundwork for more friction.

C. Leveraging Choice as Friction

Privacy reform so far has concentrated on actualizing control by minimizing friction within the choice architecture.[421] The logic was that if it were easier to make choices about personal information, people would do it. Automated opt-out tools, such as the failed 'Ad Choices' (industry self-regulation) and 'Do Not Track' (civil society governance) programs, fall into that category—as do Colorado Privacy Act's mandatory recognition of consumers' opt-outs and California's new requirement for browsers to offer universal opt-out preference signals.[422] To be clear, easing opt-outs from surveillance would certainly improve the *status quo*. Even if universal opt-outs were implemented nationally, however, they would face the same systemic shortcomings as all control-based regimes; most notably they would not protect

[417] *See* II.C.1.

[418] Cal. Civ. Code § 1798.125(a)(1).

[419] *Id*. at § 1798.125(a)(2).

[420] *Id*. at §§ 1798.120(a), 1798.121(a).

[421] MCGEVERAN, *supra* note 42, at 475–76. *See also* Frischmann & Vardi, *supra* note 350, at 4–5 (criticizing the push for an optimization of efficiency in digital contracting).

[422] A.B. 3048, Reg. Sess. (Cal.2024); Col. Priv. Act Rules, 4 CCR 904-3, Rule 5.03 (2023).

collective privacy interests.[423] It may, therefore, be worth considering the opposite—embracing the effects of friction from more meaningful choice.[424]

To start, consider the options at the federal level, under the FTC Act. Even absent a consent requirement, under Section 5, the agency can scrutinize the substantive fairness of the choice architecture[425] without the litigation risk of a fundamental realignment of enforcement practices.[426] Specifically, the FTC could challenge surveillance by adhesion as unfair and, in parallel to the ECJ, demand data-sensitive alternatives, "if necessary for an appropriate fee."[427] Although the GDPR's requirement of a justification for data processing and conditions for valid consent provide a more straightforward path, this demand necessitates neither. Instead, it directly questions the fairness of the platforms' terms of service.

Demand for data-sensitive alternatives would likely meet the elevated standard of proof for the FTC Act's unfairness prong.[428] The absence of data-sensitive alternatives, whether for a fee or not, "is likely to cause substantial injury to consumers." It further reduces their ability to self-manage their privacy.[429] As consumers often lack alternatives to platforms' digital services, they cannot reasonably avoid injury. Finally, "benefits to consumers or

---

[423] *See* III.A.1.

[424] *See* Frischmann & Vardi, *supra* note 350, at 4–5, 38–46 (proposing prosocial friction-in-design for digital contracting). On constitutional challenges to deliberately inserting friction into the process of obtaining consent *see* Balkin, *supra* note 35, at 1204 (observing that too much friction associated with shifting entitlements may raise First Amendment concerns); Frischmann & Benesch, *supra* note 28, at 420–34 (defending deliberate friction against First Amendment challenges); Goodman, *supra* note 28, at 648 ("[T]he introduction of content-neutral frictions may be one of the very few regulatory interventions that are consistent with American free speech traditions."); Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1169 (2005) (opining "that most privacy regulation that interrupts information flows in the context of an express or implied commercial relationship is [not] 'speech'"); Zachary Schapiro, Note, *Data Protection in the Digital Economy: Legislating in Light of* Sorrell v. IMS Health Inc., 63 B.C. L. Rev. 2007 (2022) (discussing the free speech implications of imposing personal data protection) . *But see* Ryan Calo, *Code, Nudge, or Notice?*, 99 IOWA L. REV. 773, 796–801 (2014) (calling for facilitation over friction).

[425] *See* THALER & SUNSTEIN, *supra* note 241, at 81–100 (explaining the concept of "choice architecture").

[426] *See* IV.A.

[427] Case C-252/21, *Meta Platforms Inc. v. Bundeskartellamt*, ECLI:EU:C:2023:537, ¶ 150 (July 4, 2023).

[428] *See* 15 U.S. Code § 45(n). *See* Bush & Waller, *supra* note 280, at 4–5 (observing that the thresholds are surmountable). On weighing individuals' privacy interests *see* In re Google Assistant Priv. Litig., 546 F. Supp. 3d 945, 974–75 (N.D. Cal. 2021) (applying the Cal. UCL); In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1072–73 (2012) (applying Cal. UCL); McCoy v. Alphabet, Inc., 2021 WL 405816, at *10 (N.D. Cal. Feb. 2, 2021) (applying Cal. UCL). *See also* Davis v. HSBC Bank Nevada, *N.A.*, 691 F.3d 1152, 1169–70 (9th Cir. 2012) (applying Cal. UCL); South Bay Chevrolet v. General Motors Acceptance Corp., 72 Cal. App. 4th 861, 887 (1999) (applying Cal. UCL).

[429] For the concept of privacy self-management *see* Solove, *supra* note 271, at 1882–1993; Solove & Hartzog, *supra* note 271, at 590–95.

competition" do not outweigh consumers' injury: consumers receive additional options, and product differentiation remains possible. Friction resulting from consumers' meaningful exercise of choice is not detrimental to either consumers or competition. In fact, such genuine choice is essential for competition to function effectively. To the extent that the friction was to amount to soft data usage limitations, it would only show that the practice's benefits had been marginal from the get-go.

The FTC may also be able to draw parallels to limitations on tying and bundling, which can provide the basis for unfairness claims assuming a "tendency to ripen into violations of the antitrust laws."[430] As the ECJ has pointed out and state laws presume, the delivering personalized advertisements is not necessary to provide social media services.[431] To support the additional requirement that the arrangements tend to ripen into antitrust law violations"[432] the FTC could point at the potentially concentrating effects of personalized advertising.

Leaning into the prohibition on deception, the FTC could argue that omitting specific information about any data usage, beyond what users should reasonably expect, amounts to deception.[433] If successful, this would diffuse the effects of overly broad privacy policies[434] and tie platforms to specifically articulated data uses. More specifically articulated uses, in turn, would become more susceptible to deception claims. Additionally, the FTC could further expand its basis for deception claims. As William McGeveran explains, "recent cases [already] include a broader range of representations, such as implications reasonably drawn from statements of the suggestions made by the design of a user interface."[435] The agency settled a complaint against Snapchat on this basis, for example.[436] Although it is admittedly challenging to insert decisive friction into a framework that, so far, bases individuals' choice on mere usage of services and applications, these examples show that plenty of levers for additional friction remain. And where federal privacy

---

[430] FTC, Policy Statement Regarding the Scope of Unfair Methods of Competition, FTC Rep. No. P221202, at 13 (Nov. 10, 2022), https://www.ftc.gov/legal-library/browse/policy-statement-regarding-scope-unfair-methods-competition-under-section-5-federal-trade-commission [https://perma.cc/V9B7-3T9C].

[431] *See Meta*, ECLI:EU:C:2023:537, at ¶¶ 97–104.

[432] *See* FTC, Policy Statement, *supra* note 421, at 13.

[433] Case law rejecting claims for breach of contract for lack consideration do not contradict a finding of deception. *See In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 610–11 (9th Cir. 2020); Hammerling v. Google LLC, 615 F. Supp. 3d 1069, 1094–95 (N.D. Cal. 2022).

[434] *See* A. Michael Froomkin, *Big Data: Destroyer of Informed Consent*, 21 YALE J.L. & TECH. 27, 42–45 (2019) (observing the consequences of "broad consent").

[435] MCGEVERAN, *supra* note 42, at 232.

[436] Complaint, In re. *Snapchat*, FTC, Docket No. C-4501 (2014); MCGEVERAN, *supra* note 42, at 232.

regulation follows the data protection model and requires justifications for certain data usage,[437] choice can be more easily leveraged into friction.

State-level privacy protections are yet more amenable to creating friction that leverages choice into soft data usage limitations. In fact, Illinois' BIPA and Texas' CUBI provide instructive domestic examples, illustrating how consent can factually manifest as a usage limitation.[438] BIPA Section 15 stipulates that before a private entity obtains "biometric identifier or biometric information" it must inform the subject in writing of the collection, its purpose and duration and receive "a written release."[439] Biometric identifier is defined as "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[440] Biometric information further expands the scope of the consent requirement to include "any information . . . based on an individual's biometric identifier used to identify an individual."[441]

Under BIPA, claims could add up quickly and BIPA litigation has skyrocketed over the past ten years.[442] In 2023, the Illinois Supreme Court found in *Cothron v. White Castle* that "every scan or transmission of biometric identifiers or biometric information" could give rise to a separate claim based on Section 15's consent requirement.[443] Whether White Castle, the plaintiff's employer, gained new information when it scanned its employees' fingerprints remained irrelevant.[444] Consequently, plaintiffs were not limited to actual damages for an initial loss of secrecy; they could invoke statutory damages of $1,000 and $5,000, respectively, for every instance of unauthorized data use.[445]

In the same year, in *Tims v. Black Horse Carriers*, the same court applied a five-year limitations period to claims based on Section 15's consent requirement.[446] When applied in *Cothron* this five-year cut-off provided the basis for

---

[437] *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1747–49 (2021) (distinguishing European data protection from U.S. consumer protection). *See also* MCGEVERAN, *supra* note 42, at 395–96.

[438] 740 ILL. COMP. STAT. 14 (2008); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017). Other states passed similar laws, *see e.g.* WASH. REV. CODE ANN. § 19.375.010 (West 2017). *See* Elvy, *supra* note 128, at 488–96 (detailing the different frameworks).

[439] 740 ILL. COMP. STAT. 14/15(b) (2008) (partially paraphrased and edited).

[440] 740 ILL. COMP. STAT. 14/10 (2024).

[441] *Id*.

[442] MCGEVERAN, *supra* note 42, at 458–59; Charles N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, 43 S. ILL. U. L.J. 819, 821–22 (2019).

[443] *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918, 929 (Ill. 2023).

[444] *Id.* at 931.

[445] *Id* at 934.; *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1203 (Ill. 2019). Limitations on Article III standing articulated in *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190, 2198 (2021) (requiring that "the asserted harm has a 'close relationship' to a harm traditionally recognized… in American courts") do not constrain state courts. *See* MCGEVERAN, *supra* note 42, at 455.

[446] *Tims v. Black Horse Carriers, Inc.*, 216 N.E.3d 845, 850–54 (Ill. 2023).

claims potentially amounting to millions of dollars per employee and exceeding $17 billion class-wide.[447] A recently enacted amendment to BIPA, however, defines repeated identical scans or transmissions without consent concerning the same individual as one violation.[448] This amendment limits statutory damages for identical repeat violations to $1,000 and $5,000 per plaintiff, respectively. The reform also eased the form requirement for consent by expanding the definition of "written release" to include electronic signatures.[449]

Over the past few years, various platforms have already paid hefty sums to settle BIPA lawsuits. In 2022, Google, for example, disbursed $100 million to settle alleged violations of BIPA by Google Photos' face grouping tool.[450] Snap Inc. settled a similar class action lawsuit over Snapchat's lenses and filters for $35 million in the same year.[451] And Meta, too, paid an enormous $650 million to compensate users in Illinois for its Tag Suggestions tool's incompliance with BIPA's consent requirement.[452] In light of the recent reforms, future settlements should be expected to yield significantly lower dollar values, however. That said, the settlement with Meta, for example, included significant changes to Facebook's practices: users will have to affirmatively opt-in to "Face Recognition," and the company promised to delete existing face templates unless it obtains individuals informed written consent.[453] Notably, Facebook emphasized that it would implement these changes globally rather than solely in Illinois.[454]

Texas' Capture or Use of Biometric Identifier (CUBI) statute also demands informed consent for any commercial capture of biometric identifiers.[455] Going beyond BIPA, it further restricts any subsequent disclosure to four predefined purposes: identification in case of disappearance or death;

---

[447] *Cothron*, 216 N.E.3d at 934. *See* Emma Graham, *Burdened by BIPA: Balancing Consumer Protection and the Economic Concerns of Businesses*, 2022 U. ILL. L. REV. 929, 956, 959 (2022) (recommending legislative reform to limit claims to disclosure and shorten the limitations period to three years).

[448] 740 ILL. COMP. STAT. 14/20(b), (c) (2024) (introduced by Public Act 103-0769).

[449] 740 ILL. COMP. STAT. 14/10 (2024) (introduced by Public Act 103-0769).

[450] Emma Roth, *Google to Pay $100 Million to Illinois Residents for Photos' Face Grouping Feature*, THE VERGE, https://www.theverge.com/2022/6/6/23156198/google-class-action-face-grouping-biometric-information-illinois-privacy-act [https://perma.cc/XK8A-QVJG](Jun. 6, 2022).

[451] Talia Soglin, *Snapchat Parent Reaches $35 Million Biometric Privacy Class-Action Settlement in Illinois*, CHI. TRIB. (Aug. 23, 2022), https://www.chicagotribune.com/2022/08/22/snapchat-parent-reaches-35-million-biometric-privacy-class-action-settlement-in-illinois/ [https://perma.cc/CD5T-VY7N**]**.

[452] In re. *Facebook Biometric Information Privacy Litigation*, 522 F. Supp. 3d 617, 622 (N.D. Cal. 2021).

[453] *Id.*

[454] *Id.*

[455] TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017).

completion of financial transactions; federal statutory requirements; and compliance with a warrant.[456] The law allows for civil penalties of up to $25,000 per violation[457] and has shown teeth already. In the biggest state privacy settlement ever, Meta agreed in July 2024 to pay $1.4 billion to resolve a lawsuit brought by the Texas Attorney General over Meta's Tag Suggestions without users' consent.[458] Texas' lawsuit against Google over the company's unauthorized use of biometric data by its Photo App, Nest camera, and Voice Assistant is still pending, and could result in a penalty of several billion dollars.[459]

Illinois' and Texas' consent requirements do not ban the collection of biometric identifiers[460] but insert so much friction that certain applications can become virtually impossible.[461] Commentators have called BIPA a "potential business killer"[462] and some platforms went beyond attempts to comply with state biometric privacy laws stringent standards. Without admitting a direct connection to BIPA, Google, for example, has withheld its Arts & Culture app's selfie feature, allowing users to match their photos with artwork, from Illinois and Texas.[463] Google also restricted its Nest camera features in Illinois, disabling facial recognition.[464] Obtaining informed consent for facial recognition from passing strangers is prohibitively onerous; its costs would outweigh the commercial benefit. All of this demonstrates that BIPA has a tangible impact and can even entirely halt specific business practices—namely those where the operational friction of obtaining informed written consent outweighs the expected benefits to the platform.

Finally, recall the CCPA's prohibition on retaliation against consumers who exercise their rights. In practice, this introduces significant operational hurdles and compliance risks, categorically similar to those created by the EU's real choice paradigm.[465] Depending on the emerging enforcement practices, this friction could amount to soft data usage restrictions on personalized

---

[456] *Id.* § 503.001(c)(1).

[457] *Id.* § 503.001(d).

[458] Agreed Final Judgement, Texas v. Meta Platforms, Inc., No. 22-0121 (Tex. Dist. Ct. 2024).

[459] Complaint, Texas v. Google LLC, No. CV58999 (Tex. Dist. Ct. 2022); Kashmir Hill & David McCabe, *Texas Sues Google for Collecting Biometric Data Without Consent*, N.Y. TIMES (Oct. 20, 2022), https://www.nytimes.com/2022/10/20/technology/texas-google-privacy-lawsuit.html [https://perma.cc/6TYZ-DYH2**]**.

[460] In contrast, 740 ILL. COMP. STAT. 14/15(c) (2008) contains direct usage limitations, stipulating that "[n]o private entity… may sell, lease, trade, or otherwise profit from a … biometric identifier or biometric information."

[461] Rowe, *supra* note 40, at 41–42.

[462] Bellamy & Fernandez, *supra* note 38.

[463] Rowe, *supra* note 40, at 41; Marotti, *supra* note 40.

[464] Rowe, *supra* note 40, at 41–42.

[465] *See* LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW 99 (5th ed. 2023) (describing difficulties with the implementation of the CCPA's anti-discrimination requirements). For the operational hurdles and compliance risks associated with the EU's real choice paradigm see above […].

advertising—albeit limited to sensitive personal information due to the CCPA's narrow definition of rights. Where unknown future uses of data represent a significant part of the data's value, purpose limitations and the need to re-obtain consent diminish that value. This applies to genetic information, for example, and reduces the incentive to collect the information in the first place. Generally, friction from choice can play the biggest role where privacy harms largely depend on scale and business practices are cost sensitive.

Conclusion

Instead of facilitating control, consent can serve as a vehicle for friction. In *Meta* v. *Bundeskartellamt*, the ECJ found surveillance by adhesion—the authorization to exploit personal data via boilerplate—incompatible with the GDPR. Valid consent, according to the court, requires real choice, which demands a data-sensitive option for an appropriate fee. Ending surveillance by adhesion fundamentally alters the relationship between platforms and users from promise to permission, pushing back against contractual imperatives.

Practically, real choice over personal data and similar fortified notions of consent can introduce sufficient friction to gum up the works of personalized advertising. This may induce shifts to less harmful, contextual advertising. Appreciating friction from fortified notions of choice should be an integral part of privacy realpolitik in the U.S., where data usage limitations are not available or desirable. Regulators and enforcers can build on laws against unfair, deceptive, and abusive practices to end surveillance by adhesion and frameworks like Illinois' BIPA and Texas' CUBI to leverage consent as friction and establish soft but potent data usage limitations.