2022

The Hidden Harms of Privacy Penalties

Mary D. Fan

The Hidden Harms of Privacy Penalties

Mary D. Fan[*]

How to frame privacy penalties to protect our personal information is an important question as demands for legislation and proposals proliferate. The predominant assumption in calls for a comprehensive consumer privacy regime is that regulation and penalties arm the consumer David against Goliath businesses. Missing in the focus on powerful companies is attention to the potential harms of expanding privacy penalties for small-fry individuals and entities, especially from disfavored or marginalized groups. This Article is the first to illuminate the regressive risks of privacy penalties, showing how broad privacy penalties can become tools for harassment of small businesses and individuals with limited resources to defend.

Drawing on original research collecting and coding 571 privacy penalty decisions from 20 nations under the world's toughest privacy rights and penalties regime, the European Union's General Data Privacy Regulation ("GDPR"), this Article offers cautionary lessons. Illuminating a shadow jurisprudence of small targets, the Article shows how overly broad, amorphously worded privacy penalty provisions can be used to target disfavored groups and create weapons for the disgruntled, such as punishing people who record the police or in disputes between neighbors.

The Article offers three major principles to protect against targeting harms. First, the Article warns against vague broad language in framing penalty-backed obligations to curb discretion to harass and target

 Jack R. MacDonald Endowed Chair, University of Washington School of Law. Many thanks to Rabia Belt, Ann Cleaveland, Joe Grundfest, Deborah Hensler, Abraham Newman, Aileen Nielsen, Cindy Fester, Mark Lemley, Rob MacCoun, Julian Nyarko, Lisa Ouellette, Nate Persily, Elaine Sedenberg, Ido Sivan-Sevilla, David Alan Sklansky, Steven Weber, Richmond Wong, and participants at the Stanford Law School faculty workshop and U.C. Berkeley Center for Long-Term Cybersecurity for valuable insights. Special thanks to my outstanding coding team: Andrea Grande, Ashley Mixon, Gabriela Navarro-Santana, Joëlle Klein, Maria S. Gomes, Yina E. Finch. I am especially grateful to my superb editor Etelle Stephan and the excellent team of the *UC Davis Law Review*, led by Natalie Maas and Sue Jones — it is truly a pleasure to work with you.

disfavored groups. Second, the Article argues for a regulatory agency model with an explicit advisory role rather than a predominantly quasi-prosecutorial role. Third, the Article proposes safe harbors for individuals and small businesses and a complementary understanding that even seemingly minor penalties can carry major collateral consequences for the vulnerable.

TABLE OF CONTENTS

INTRODUCTION

In calls to expand privacy rights and penalties, the assumed target is usually behemoth businesses.[1] Proponents assume that privacy penalties arm and protect the small consumer David against Goliath companies.[2] Consumer and privacy advocates express dismay and alarm that despite decades of debates and attempts, the United States still lacks a baseline comprehensive privacy law.[3] Big Tech representatives also seek a national privacy law to clarify obligations and forestall a patchwork approach to rights and regulations.[4] The term Big Tech —

[1] *See, e.g.*, Mark Phillips & Bartha M. Knoppers, *Whose Commons? Data Protection as a Legal Limit of Open Science*, 47 J.L. MED. & ETHICS 106, 108 (2019) (noting the GDPR's "default lens tends to focus on relationships between private sector companies and their customers"); FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS, at iii to 3 (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [https://perma.cc/G5G9-9E9Y] (citing data and concerns regarding the privacy practices of major online web sites providing consumer services and arguing for privacy regulation).

[2] *See, e.g.*, Greg Bensinger, *Goliath vs. Goliath*, N.Y. TIMES (Dec. 19, 2020), https://www.nytimes.com/2020/12/19/opinion/facebook-apple-privacy.html [https://perma.cc/CWP8-V59N] ("Until the federal government more seriously takes up data privacy, consumers will be vulnerable to corporations that are motivated by profits to find new and creative ways to harvest personal information."); *Majority Statement* to *Hearings: Revisting the Need for Federal Data Privacy Legislation*, U.S. SENATE COMM. ON COM., SCI., & TRANSP. (Sept. 23, 2020, 10:00 AM), https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation [https://perma.cc/S2AJ-UMPK] (summarizing testimony before the Senate Committee indicating that "individuals needed rigorous privacy protections to ensure that businesses do not misuse their data").

[3] *See, e.g.*, *Hearing on Revisiting the Need for Federal Data Privacy Legislation Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. 3-4 (2020) (statement of Julie Brill, Former Comm'r, Federal Trade Commission and Corporate Vice President, Chief Privacy Officer, and Deputy General Counsel, Global Privacy & Regulatory Affairs, Microsoft Corporation), https://www.commerce.senate.gov/services/files/5404DCED-136B-4622-B922-49045EC7C03E [https://perma.cc/MSC8-8HGN] ("However, the U.S. remains one of the few developed countries not to have comprehensive privacy protections for its people. If this situation is not rectified soon, the United States will suffer as American businesses will be less able to effectively compete on the global economy."); Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass A Baseline Privacy Law*, BROOKINGS (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ [https://perma.cc/F3E2-JY2W] (summarizing calls for regulation and proposals over the decades).

[4] *See, e.g.*, Ryan Chiavetta, *Big Tech Privacy Pros Express Optimism for Federal U.S. Privacy Law*, IAPP (Jan. 14, 2021), https://iapp.org/news/a/big-tech-privacy-pros-express-optimism-over-federal-us-privacy-law-prospects/ [https://perma.cc/9VR2-WQWT] (discussing support by executives from major technology companies such as Twitter

the paradigmatic target in legislative debates over regulation — refers to some of the world's largest companies based on market capitalization, such as Apple, Microsoft, Amazon, Google/Alphabet, and Facebook.[5] The focus on big businesses misses an important issue in framing privacy regulations and penalties, however. This Article is about the overlooked potential hidden harms of expanding privacy penalties for small-fry individuals and entities, who may be marginalized, harassed, and under-resourced to defend against targeting.

The Article offers cautionary lessons derived from analyzing penalty decisions under the world's toughest privacy rights and penalties regime, the European Union's General Data Privacy Regulation ("GDPR").[6] The insights are important and timely as data privacy proposals and debates proliferate in the United States as well as abroad regarding how to frame and expand privacy penalties. The Article shows how experience under the GDPR reveals that amorphous and overly broad language and the ease of imposing privacy penalties can open avenues for potential harassment and retaliation.[7] The targets are not just Goliath giant businesses, but potentially much humbler persons with limited resources, such as migrants whose small businesses are symbols of backlash against immigration and multiculturalism.[8]

Consider the case of S.Z., the ethnically Turkish proprietor of a döner kebab snack stand in Austria, and S.Z.'s employee (not even given initials in the privacy penalty decision), whose attempt to stop alleged police harassment resulted instead in paying privacy penalties under the GDPR.[9] It is not the kind of GDPR case that makes the headlines and popular debates focused on Google, Facebook, and other highly

and Google for a federal privacy law and frequently expressed concerns over how to comply with a patchwork of murky obligations).

[5] Kean Birch, DT Cochrane & Callum Ward, *Data As Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech*, BIG DATA & SOC'Y, 1, 2, 5 (2021).

[6] Regulation 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 Privacy Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[7] *See* discussion *infra* notes 9–33 and Parts II–III.

[8] *See* discussion *infra* notes 9–33 and Parts II–III.

[9] Bundesverwaltungsgericht [BVwG] [Federal Administrative Court of Austria], Beschwerde des XXXX gegen das Straferkenntnis der Datenschutzbehörde [Complaint of [Name Redacted by the Court] against the Criminal Judgement of the Data Protection Authority] Nov. 25, 2019, Case W211 2210458-1/10, § I.1, https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20191125_W211_2210458_1_00/BVWGT_20191125_W211_2210458_1_00.html [https://perma.cc/PZ7R-J7BF].

capitalized businesses. Yet this humble criminal case exemplifies the hidden problem of privacy penalties.

Figure 1. A dönor kebab and pizza snack stand in Vienna, Austria.

Some sociopolitical context about the symbolism of döner kebab stands is valuable to understanding the import of the problem. Frequently served from immigrant-run snack stands, döner kebabs symbolize how immigration has shaped Western European multiculturalism.[10] Ubiquitous affordable spit-roasted meat conveniently wrapped in unleavened pita, döner represents cultural change in places such as Germany, Austria, France, and the United Kingdom.[11] Associated with working-class Turkish and Muslim immigrants, the food is both an ethnic signifier in Western Europe, and increasingly a marker of the region's fraught political and social conflicts over identity.[12] As Western Europe wrestles with recurring

[10] *See, e.g.*, Ayse S. Caglar, *McDöner: Döner Kebap and the Social Positioning Struggle of German Turks*, *in* MULTICULTURALISM: CRITICAL CONCEPTS IN SOCIOLOGY 413, 415 (Gerd Baumann & Steven Vertovec eds., 2011) (discussing the migration of Turkish migrant workers seeking work and how "*döner* became an integral part of Turkish migrants' relations with the Germans and of Turkish identities in Germany").

[11] *See, e.g.*, Ibrahim Sirkeci, *Transnational Döner Kebab Taking Over the UK*, 4 TRANSNAT'L MKTG. J. 143, 146 (2016) (describing the preparation of döner kebab in the UK and in continental Europe).

[12] Pierre Raffard, *The Doner Kebab, an Unlikely Symbol of European Identity*, THE WORLD (May 15, 2019, 1:30 PM EDT), https://www.pri.org/stories/2019-05-15/doner-kebab-unlikely-symbol-european-identity [https://perma.cc/68RT-VTHW]; *see also,*

anti-immigrant nationalist conflicts, döner kebabs snack stands are among the unlikely targets in the culture wars, decried by some as symbols of "rampant Islamification."[13]

The slogan "remove kebab" is used by extremists to express anti-migrant and anti-Muslim sentiment on social media.[14] In France, a far-right politician waged political battle to eliminate döner kebab stands, arguing the stands were not "in our culture" — specifically, "our Judeo-Christian culture."[15] In Italy, the Municipal Council in the Tuscan city of Lucca voted to prohibit granting licenses in the city center to dining "establishments whose activities can be tracked to different ethnicities."[16] The council said the ban was to preserve the city's traditional cultural identity.[17] The Tuscan regional government called out the ban for "introducing hidden forms of gastronomic or culinary racism."[18]

The penalties that befell the proprietor of S.Z., the ethnically Turkish döner kebab snack stand operator in Vienna, and S.Z.'s employee, should be evaluated in light of this context of multicultural backlash.[19]

e.g., Caglar, *supra* note 10, at 415 (discussing how food and food consumption "have symbolic and constitutive functions in intergroup relations" and can be signifiers for "ethnically and culturally differentiated groups," leading to manipulation of the meaning and symbolism of foods like döner as part of the evolution of intergroup relations).

13 Raffard, *supra* note 12.

14 SETA FOUND. FOR POL., ECON. & SOC. RSCH., EUROPEAN ISLAMOPHOBIA REPORT 157 (Enes Bayrakli & Farid Hafez eds., 2019), https://www.islamophobiaeurope.com/wp-content/uploads/2020/06/EIR_2019.pdf [https://perma.cc/JD8T-Q8CE].

15 Samuel Laurent, *Robert Ménard et le "Grand Remplacement Culinaire" à Béziers* [*Robert Ménard and the "Great Culinary Replacement" in Béziers*], LE MONDE (Oct. 30, 2015, 6:14 PM), https://www.lemonde.fr/les-decodeurs/article/2015/10/30/robert-menard-les-kebabs-et-la-culture_4800315_4355770.html [https://perma.cc/L9SS-NN3S] (quotations are translated from the original).

16 KRISHNENDU RAY & TULASI SRINIVAS, CURRIED CULTURES: GLOBALIZATION, FOOD, AND SOUTH ASIA 26 n.2 (Krishnendu Ray & Tulasi Srinivas eds., U.C. Press 2012).

17 Silvia Aloisi, *Tuscan City Criticized for Banning Foreign Eateries*, REUTERS (Jan. 27, 2009, 9:07 AM), https://www.reuters.com/article/us-italy-restaurants/tuscan-city-criticized-for-banning-foreign-eateries-idUKTRE50Q55320090127 [https://perma.cc/B28Q-B9YV].

18 *Id.*

19 Interestingly, though S.Z.'s name is pseudonymized, her ethnicity and gender are revealed by the Federal Administrative Court ("BVwG") in its decision on appeal of S.Z.'s conviction when the BVwG refers to S.Z.'s "Turkish compatriot" who helped S.Z. install the cameras and to the fact that S.Z. did not speak German well. Beschwerde des XXXX gegen das Straferkenntnis der Datenschutzbehörde [Complaint of [Name Redacted by the Court] against the Criminal Judgement of the Data Protection Authority], Bundesverwaltungsgericht [BVwG] [Federal Administrative Court of Austria] Nov. 25, 2019, No. W211 2210458-1, § I.6, https://www.ris.bka.gv.at/

S.Z. and the snack stand employee tried to seek redress for alleged harassment by a police inspector. In support of their police harassment claim, S.Z. and the employee submitted two videos of the police inspector's behavior at the döner stand.[20] S.Z. and the employee installed the surveillance camera to record the police inspector's alleged harassment.[21] Rather than being investigated for the alleged harassment, the police inspector reported S.Z. and the employee to the data protection authority.[22] S.Z. and the employee were hauled into the hassle and expense of hiring a lawyer to defend against criminal charges of violations of the GDPR for using security cameras at the snack stand to record the police.[23]

The prime witness against S.Z. and the employee in the privacy penalty proceedings was the police inspector whose alleged harassment prompted the snack stand operators to get the cameras.[24] The police inspector testified that S.Z. and the employee had installed three security cameras around the snack stand.[25] One security camera was on a storage container and two were in the interior of the snack stand.[26] The images recorded were displayed live on a computer and stored for up to 16 days, testified the police inspector.[27]

Trying to rebut the police inspector's case, S.Z., who spoke little German, had to defend and testify via an interpreter.[28] Based on the testimony, the Data Protection Authority convicted S.Z. and the unnamed employee of three GDPR violations.[29] The Data Protection Authority ruled that the recording violated the GDPR's requirements regarding data minimization, storage, and transparency by potentially capturing activities on the adjacent public road and gas station with insufficient notice and image storage for more than 72 hours.[30] For the offenses, the Data Protection Authority imposed penalties that totaled 1,800 euros (about $2,125).[31] The employee appealed the criminal

Dokumente/Bvwg/BVWGT_20191125_W211_2210458_1_00/BVWGT_20191125_W211_2210458_1_00.html [https://perma.cc/PZ7R-J7BF].

[20] *Id.* § I.1.

[21] *Id.*

[22] *Id.* § I.2.

[23] *See id.* § I.1.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *See id.* § II.2.

[29] *Id.* § II.3.

[30] *Id.* § I.2.

[31] *Id.* at § I.3.

convictions, which the Federal Administrative Court of Austria upheld, while slightly reducing the penalties to 1,500 euros (about $1,771) or a substitute custodial sentence of four days.[32]

What happened to S.Z. and the employee for recording the police is a cautionary tale against expanding privacy penalties, with timely lessons for the United States. Privacy penalty regimes are still in germination in the United States, as states and the federal government grapple with how to balance privacy protections with competing values, including First Amendment freedoms, regulatory burdens on businesses, and other important concerns.[33] The retaliation for recording alleged police harassment is a particularly stark example of how privacy penalties can transgress other deeply cherished freedoms against state control. For example, in the United States the right to record the police is constitutionally protected by the First Amendment[34] — though there are numerous controversial cases of retaliatory pretextual charges for recording the police.[35]

While privacy protections are often assumed to be a protection against the state, this Article illuminates how expanding privacy penalty regimes also can harm civil liberties and provide cover for harassment, potentially against disfavored groups. The Article seeks to rectify the neglect regarding how expanding privacy penalties can lead to potential targeting harms and harassment, particularly for marginalized communities and persons.

A note on the use of the terms "privacy penalties" and "privacy penalization" at the outset. Savvy legislatures sometimes use euphemisms for the straightforward term "penalties" because the word

---

[32] *Id.* § II.3.

[33] *See* discussion *infra* Part I.A.

[34] Fields v. City of Philadelphia, 862 F.3d 353, 356 (3d Cir. 2017); Turner v. Lieutenant Driver, 848 F.3d 678, 688 (5th Cir. 2017); Gericke v. Begin, 753 F.3d 1, 3 (1st Cir. 2014); ACLU of Ill. v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2012); Glik v. Cunniffe, 655 F.3d 78, 79 (1st Cir. 2011); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000); Fordyce v. City of Seattle, 55 F.3d 436, 439 (9th Cir. 1995); *see also, e.g.*, Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 184-99 (2017) (analyzing case law on the right to record generally); Jocelyn Simonson, *Beyond Body Cameras: Defending a Robust Right to Record the Police*, 104 GEO. L.J. 1559, 1569-74 (2016) (arguing that filming the police is a form of First Amendment-protected speech); Howard M. Wasserman, *Police Misconduct, Video Recording, and Procedural Barriers to Rights Enforcement*, 96 N.C. L. REV. 1313, 1336-47 (2018) (collecting and evaluating theories of the First Amendment foundations of the right to record).

[35] *See* MARY D. FAN, CAMERA POWER: PROOF, POLICING, PRIVACY, AND AUDIOVISUAL BIG DATA 70-77 (Cambridge Univ. Press 2019) (discussing the growing recognition of the right to record the police in the United States and retaliatory pretextual charges that persist despite this).

too openly and accurately captures the punitive experience of these sanctions.[36] For example, Proposition 24, amending the California Consumer Privacy Act ("CCPA"), strikes the previously used term "penalty" in the CCPA and substitutes the term "fine" — for the same sanction.[37] This Article uses the term "privacy penalties" to capture the experience of being on the receiving end of these sanctions for people like the Turkish döner kebab stand operator S.Z. and her unnamed employee.[38]

The Article proceeds in three parts. Part I offers background framing on the import and timeliness of the issue of privacy penalization. Beginning by contrasting the European Union's extensive privacy regime with the patchwork approach in the United States, this Section examines the push for the U.S. to converge in enacting strong privacy rules and penalties and proliferating legislative proposals. The drive for the United States to enact a privacy regime to "catch up" with the European Union's "gold standard" GDPR regime makes it all the more important to examine the lived experience on the ground of privacy penalties under the GDPR.[39] The approaches taken in the proliferating privacy proposals in the United States may also have some important lessons for the EU in terms of reducing the harm to individual persons and small businesses.[40]

Part II presents this investigation's methods and results, analyzing a dataset of 571 privacy penalty decisions from 20 national Data Protection Authorities under the GDPR. A multilingual team read and coded the majority of these cases in the original French, Spanish, German, or English. Additional privacy penalty decisions in languages

[36] As Herbert Packer decades ago wryly noted, the term "punishment" similarly goes by softer euphemisms such as treatment. *See* Herbert L. Packer, *Making the Punishment Fit the Crime*, 77 HARV. L. REV. 1071, 1080 (1964) (noting the "fashionable euphemism" of treatment for punishment).

[37] Proposition 24, California Privacy Acts of 2020, § 1798.155(b) (Text of Proposed Laws), https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf [https://perma.cc/9SKU-C7SW] [hereinafter Proposition 24].

[38] *See* discussion *supra* notes 9–32.

[39] *Cf., e.g.*, Mike Davis, *U.S. Must Catch Up with Rest of the World on Data Privacy*, ROLL CALL (Oct. 14, 2021, 6:00 AM), https://rollcall.com/2021/10/14/us-must-catch-up-with-rest-of-the-world-on-data-privacy/ [https://perma.cc/UVE8-ZCJN] (calling for the U.S. to "catch up" and enact "universal, comprehensive data privacy laws that protect consumers" like the GDPR and other laws modelled on the GDPR); Sabine Muscat, *How GDPR is Driving the U.S. Privacy Legislation Debate*, HEINRICH BÖLL STIFTUNG (May 24, 2019), https://us.boell.org/en/2019/05/24/how-gdpr-driving-us-privacy-legislation-debate [https://perma.cc/P2NE-GH4V] ("The EU has since promoted its law as the global gold standard–taunting the US to catch up in the race for digital governance.").

[40] For a discussion, see *infra* Part III.B.2.

besides the four within the linguistic skillset of the team also were coded with the aid of Google's machine translation system. This large dataset of privacy penalty decisions illuminates the humbler targets of penalties in the shadows, neglected in the headlines regarding Goliath companies. The results include prosecutions and penalties levied against individuals and small businesses like in S.Z.'s case.

The Article's analyses show that individual defendants are significantly more likely to be penalized under certain GDPR provisions compared to major corporations.[41] Small businesses are also significantly more likely to be penalized under certain provisions than major corporations.[42] Conversely, major corporations are significantly more likely to be penalized under certain provisions compared to small businesses.[43] The Article discusses which privacy provisions pose the heightened risk of petty privacy penalty proceedings that can be cover for harassment and expressing disgruntlement, potentially against persons or entities with limited resources to defend themselves.

Part III argues that expanding privacy penalties, like expanding seemingly minor criminal offenses, can have harassment and harm potential. This Part connects privacy law debates to the criminal justice literature on why seemingly minor penalties matter, exacerbating racial disparities and heaping harm on marginalized individuals and communities.[44] Part III proposes cautionary guard rails to prevent the use of privacy penalties as weapons to harass or retaliate against

[41] *See infra* Table 8.

[42] *See infra* Table 10.

[43] *Compare infra* Table 10 (penalties against small businesses) *with infra* Table 8 (penalties against major corporations).

[44] *See, e.g.*, ISSA KOHLER-HAUSMANN, MISDEMEANORLAND: CRIMINAL COURTS AND SOCIAL CONTROL IN AN AGE OF BROKEN WINDOWS 51-56, 66-73, 276 (2018) (illuminating how the processing of seemingly minor offenses exerts social control and widens surveillance, particularly against persons with limited resources); MALCOLM M. FEELEY, THE PROCESS IS THE PUNISHMENT: HANDLING CASES IN A LOWER CRIMINAL COURT 3-14, 181-85, 199-241 (1979) (shedding empirical light on the harms of processing seemingly lesser offenses); ALEXANDRA NATAPOFF, PUNISHMENT WITHOUT CRIME: HOW OUR MASSIVE MISDEMEANOR SYSTEM TRAPS THE INNOCENT AND MAKES AMERICA MORE UNEQUAL 3-12, 149-70 (2018) (discussing how the sprawling misdemeanor system traps impoverished persons and racial minorities and can be proxy social controls, such as enforcing gentrification boundaries); Eisha Jain, *Proportionality and Other Misdemeanor Myths*, 98 B.U. L. REV. 953, 956-64 (2018) (correcting common myths about misdemeanors that obscure the harms); Irene Oritseweyinmi Joe, *Rethinking Misdemeanor Neglect*, 64 UCLA L. REV. 738, 756-71 (2017) (discussing systemic harms to misdemeanor defendants); Jenny Roberts, *Why Misdemeanors Matter: Defining Effective Advocacy in the Lower Criminal Courts*, 45 UC DAVIS L. REV. 277, 297-306 (2011) (discussing the major collateral consequences posed by misdemeanor convictions such as loss of immigration status).

individuals and small businesses, particularly people bearing heavier burdens of marginalization and punishment.

I. PRIVACY AND PUNISHMENT: CALLS TO CONVERGE

While cultures are diverse among individuals, in a nation, and all the more varied among a collection of nations, identifying major axes of differences in cultural orientations can be analytically valuable.[45] An influential account of comparative privacy cultures depicts Europeans viewing privacy as a fundamental right while Americans view privacy as one interest to be balanced with competing concerns.[46] Times and privacy tastes in the United States are changing, however. A Pew Research Center survey found that 79% of respondents are concerned about how companies use the data they collect on people.[47] A 2020

[45] By analogy and as an example, the work of anthropologist Mary Douglas on worldviews that simplified the vast universe of differences among people along four major axes has been enormously fruitful in anthropology, the social sciences, and legal scholarship. MARY DOUGLAS, CULTURAL BIAS 6, 8-13 (1978) (framing group-grid theory with Durkheimian influences); MARY DOUGLAS, ESSAYS IN THE SOCIOLOGY OF PERCEPTION 3-6 (1982) (providing overview of theory); Karl Dake, *Orienting Dispositions in the Perception of Risk: An Analysis of Contemporary Worldviews and Cultural Biases*, 22 J. CROSS-CULTURAL PSYCH. 61, 63, 65 (1991) (framing theory in terms of psychology and political influences on perception); *see also, e.g.*, Dan M. Kahan, *The Cognitively Illiberal State*, 60 STAN. L. REV. 115, 122-24 (2007) (explaining usefulness of insights for understanding fiercely fought conflicts); Dan M. Kahan & Donald Braman, *More Statistics, Less Persuasion: A Cultural Theory of Gun-Risk Perceptions*, 151 U. PA. L. REV. 1291, 1310-14 (2003) (applying Douglas worldviews framework to analyzing partisan splits in perceptions on firearms); Dan M. Kahan, David A. Hoffman & Donald Braman, *Whose Eyes Are You Going To Believe?* Scott v. Harris *and the Perils of Cognitive Illiberalism*, 122 HARV. L. REV. 837, 859 (2009) (applying Douglas framework to explain how people viewing the same use of force recorded on video can reach sharply different conclusions); Dan M. Kahan, David A. Hoffman, Donald Braman, Danieli Evans & Jeffrey J. Rachlinski, *"They Saw a Protest": Cognitive Illiberalism and the Speech-Conduct Distinction*, 64 STAN. L. REV. 851, 884 (2012) (finding that perceptions of whether protesters were expressing dissent or physically intimidating others were shaped by cultural cognition); Mark E. Koltko-Rivera, *The Psychology of Worldviews*, 8 REV. GEN. PSYCH. 3, 3-4 (2004) (discussing prevalence and value of the worldviews theory).

[46] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 880 (2014).

[47] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/2LW5-5ULM]. For information on the American Trends Panel size, see Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *The American Trends Panel Survey Methodology*, PEW RSCH. CTR. (Nov. 15, 2019),

survey by the accounting firm KPMG found that 87% of U.S. respondents viewed privacy as a fundamental human right.[48]

There is an increasing call for the United States to "catch up" or converge with the European Union in enacting a strong privacy regime like the EU's GDPR.[49] The European Union was the earliest major mover in enacting a broad strong privacy regime, the General Data Privacy Regulation, which took effect on May 25, 2018.[50] The United States, in contrast, still lacks national baseline privacy legislation, despite numerous proposed bills, advocacy and efforts.[51] With a new Presidential regime, conditions seemed conducive to the framing and passage of federal privacy legislation, spurring new efforts in Congress.[52] As proposals for privacy regimes and potential sanctions are framed, it is timely and important to understand the lessons of the GDPR for potential privacy penalization regimes. This Section explains the GDPR regime and its influence abroad, including in the U.S., as a

https://www.pewresearch.org/internet/2019/11/15/data-privacy-methodology/ [https://perma.cc/2RG8-5VYJ] (reporting recruitment figures and response rates).

[48] KPMG LLP, THE NEW IMPERATIVE FOR CORPORATE DATA RESPONSIBILITY 4 (2020), https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf [https://perma.cc/67DE-ZLL5].

[49] *See, e.g.*, Brian Keogh, *50 Attorneys General Investigate Google: Surveillance Capitalism and Legal Privacy Frameworks*, 30 TRANSNAT'L L. & CONTEMP. PROBS. 267, 288 (2021) ("Citizens of the United States and users all over the world need protections like those put forth in the GDPR. As the United States enters the second decade of the 21st century, it is time for privacy law to catch up with the evolving economy."); Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 627 (2019) ("The United States should follow the EU's lead by recognizing a fundamental right to data privacy as essential to the 'well-being of individuals.'"); Caitlin Chin, *Highlights: The GDPR and CCPA as Benchmarks for Federal Privacy Legislation*, BROOKINGS (Dec. 19, 2019), https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/#cancel [https://perma.cc/SBY8-8PYQ] [hereinafter *Highlights*] (discussing the influence of the GDPR and California's Consumer Privacy Act (CCPA) on federal privacy bills).

[50] GDPR, *supra* note 6.

[51] *See, e.g.*, JONATHAN M. GAFFNEY, CONGR. RSCH. SERV. LSB10441, WATCHING THE WATCHERS: A COMPARISON OF PRIVACY BILLS IN THE 116TH CONGRESS1-4 (2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10441 [https://perma.cc/362L-65YT] (summarizing numerous legislative efforts at federal privacy legislation over the years).

[52] *See, e.g.*, Colin Rahill, *The State of Privacy Under a Biden Administration: Federal Cybersecurity Legislation, Strict Regulatory Enforcement, and a New Privacy Shield with the EU*, HARV. J.L. & TECH. (Feb. 20, 2021), https://jolt.law.harvard.edu/digest/the-state-of-privacy-under-a-biden-administration-federal-cybersecurity-legislation-strict-regulatory-enforcement-and-a-new-privacy-shield-with-the-eu [https://perma.cc/Q2SX-A86H] ("The beginning of the Biden administration coincides with a growing push for federal privacy legislation.").

foundation to frame the timely import of the Article's investigation of GDPR privacy penalties on the ground.

A. The Gold Standard of Privacy Protection — and Penalization

What happens when broadly worded privacy rights combine with strong penalties? As the first mover in framing the world's broadest and strongest privacy regime, the nations of the European Union became test subjects with its GDPR, which took effect on May 25, 2018.[53] The GDPR is oft-cited as the digital "gold standard" in privacy protection.[54] The EU's enactment of the GDPR spurred privacy legislation and proposals across the ocean in places such as Brazil, India, and California.[55] Influenced by the GDPR and oft-described as the U.S. response to the GDPR, the CCPA, as amended in 2020 by the California Privacy Rights Act, is inspiring other U.S. legislative proposals and state laws.[56]

---

[53] Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited July 13, 2022) [https://perma.cc/N9CJ-5Y4G].

[54] *See, e.g.*, Lydia de la Torre, *GDPR Matchup: The California Consumer Privacy Act 2018*, IAPP (July 31, 2018), https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/ [https://perma.cc/N243-BVU6] ("Most data protection professionals would agree that the GDPR sets the global 'gold-standard' for data protection and has forced companies across the globe to significantly update their data practices and ramp up their compliance programs.").

[55] *See, e.g.*, Chin, *Highlights*, *supra* note 49 (discussing the influence of the GDPR on data protection and privacy laws in California and around the world); Jonathan Keane, *From California to Brazil: Europe's Privacy Laws Have Created a Recipe for the World*, CNBC (Apr. 8, 2021, 1:32 AM EDT), https://www.cnbc.com/2021/04/08/from-california-to-brazil-gdpr-has-created-recipe-for-the-world.html [https://perma.cc/4QZU-PD4U] (discussing the influence of the GDPR on data protection and privacy laws in California and around the world).

[56] *See, e.g.*, *Hearing on Revisiting the Need for Federal Data Privacy Legislation Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. 2-6 (2020) (statement of Xavier Becerra, Attorney General of California), https://www.commerce.senate.gov/services/files/8AF136EE-DE50-4258-98C6-249F5BCECFA4 [https://perma.cc/XR9B-PN4K] (explaining California's exemplar to Senators framing federal privacy legislation); Greta Carlson, Jonathan McKinney, Elizabeth Slezak & Esther-Sarah Wilmot, *General Data Protection Regulation and California Consumer Privacy Act: Background*, 24 CURRENTS: J. INT'L ECON. L. 62, 67 (2020) (noting that the CCPA followed "on the heels of the GDPR . . . similarly sought to enact data privacy protections" and is "[w]idely perceived to be America's reply to the GDPR"); Jennifer Bryant, *2021 "Best Chance" for U.S. Privacy Legislation*, IAPP (Dec. 7, 2020), https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/ [https://perma.cc/2EA6-8682] (discussing how California's privacy legislation is spurring federal action).

The GDPR frames "fundamental rights and freedoms of natural persons" in their personal data.[57] The regime is an expansive successor to the EU's 1995 Data Protection regulation.[58] Under the GDPR, protected persons, termed "data subjects," have three main clusters of rights: (1) notice, transparency, and intelligible communication regarding how their personal data is gathered, used, and stored by controllers; (2) control over and access to personal data, including rectifying errors, supplementing information, porting data in usable format, and a right to be forgotten via data erasure; and (3) rights against "being subject to decision-making based solely on automated processing" and algorithmic profiling in matters such as credit, housing, job, or college applications.[59] This robust bill of rights in one's personal data under the GDPR has a progressive appeal.[60]

The GDPR is not just a statement of rights, however, but also imposes obligations on private individuals as well as entities backed by potentially steep sanctions.[61] The regime frames numerous sanctions-backed obligations on "data controllers" and "processors" using or holding data on natural persons.[62] A data controller is not just Facebook or Google. Targets for GDPR privacy penalties also may be humble individuals and small businesses, such as a driver or apartment dweller who uses a vehicle dash or window-mounted security camera.[63]

Persons and entities who acquire personal data of others, called data controllers, must adhere to principles of lawful, fair, and transparent

[57] *See* GDPR, *supra* note 6, arts. 1, 12-23, 77-79 (rights of the data subject).

[58] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[59] GDPR, *supra* note 6, arts. 12-22; *see also id.* art. 23 (setting forth limitations to the rights). For a discussion of the GDPR's right to contest automated decision-making, see Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI*, 121 COLUM. L. REV. 1957, 1975 (2021).

[60] *See, e.g.*, Federico Fabbrini & Edoardo Celeste, *The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders*, 21 GERMAN L.J. 55, 65 (2020) ("The EU is at the forefront of data protection worldwide. The GDPR represents the most comprehensive and advanced regulatory framework for data privacy to date.").

[61] *See* GDPR, *supra* note 6, arts. 83-84 (setting forth penalties and the power to levy administrative fines).

[62] *See id.* arts. 24-43 (obligations of the data controller and processor).

[63] *See, e.g.*, Penal Decision, Istvan O*** Sept. 27, 2018, (Austria), https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20180927_DSB_D550_084_0002_DSB_2018_00/DSBT_20180927_DSB_D550_084_0002_DSB_2018_00.pdf [https://perma.cc/T26L-PWT3] (imposing a fine of 300 euros on a driver for using two in-vehicle dash cameras without giving sufficient notice); Penal Decision, Rudolf D. Dec. 20, 2018, (Austria) (imposing a fine of 2,200 euros on an apartment dweller for putting a surveillance camera in his apartment doorway and window).

data processing, including giving notice, and data minimization.[64] Data minimization means collecting and retaining the minimum necessary data to serve a lawful purpose.[65] Lawful purposes are circumscribed to enumerated circumstances, such as when the subject consents; when necessary to perform on a contract, comply with legal obligations or protect vital interests; and carrying out tasks in the public interest.[66] To ensure security and "data protection by design and default," data controllers must deploy technical and organizational measures that protect against breaches.[67] Before deploying new technologies that are likely to result in high risk to data protection rights and freedoms, data controllers must conduct data protection impact assessments.[68]

Penalties vary by type of violation.[69] At the most severe end, penalties for infringing basic legal principles such as getting a subject's consent, can be up to 20,000,000 euros [approximately U.S. $23.5 million] for certain violations, or, in the case of businesses, "up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher."[70] EU member states may enact further penalties subject to the amorphous standard that the penalties be "effective, proportionate and dissuasive."[71] This broad grant of penalty power enabled, for example, the criminal penalties faced by the Turkish döner kebab stand workers in Austria for recording what they believed was police harassment.[72]

Several articles confer rights to lodge a complaint with a supervisory authority, which Member States must establish, and to effective remedies.[73] Complainants may pursue various avenues and remedies, including administrative fines before a supervisory body and — without prejudice to the administrative remedies — a judicial remedy by also lodging a complaint in the courts of the Member State.[74] The fines and penalties a person or entity faces varies by type of violation but can be

[64] GDPR, *supra* note 6, arts. 5(1)(a)-(c), 25(1).

[65] *Id.* art. 5(1)(c), (e).

[66] *Id.* art. 6.

[67] *Id.* arts. 5(1)(f), 25.

[68] *Id.* art. 35.

[69] *See, e.g.*, *id.* art. 83 (setting forth administrative fines by type of violation); Lukas Feiler, *Takeaways from the First GDPR Fines*, BAKER MCKENZIE (Dec. 19, 2018), (URL unavailable) [https://perma.cc/8Y6Q-Z7ZS] (reporting on early three cases of actual fines imposed for data privacy breaches ranging from 4,800 euros to 400,000 euros).

[70] GDPR, *supra* note 6, art. 83(5).

[71] *Id.*, art. 84(1).

[72] *See supra* notes 9–32 and accompanying text.

[73] GDPR, *supra* note 6, arts. 77-84.

[74] *Id.*

multimillion dollars as well as other penalties that a Member State may prescribe.[75] Numerous factors affect the amount of the fine including:

1. the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
2. the intentional or negligent character of the infringement;
3. any action taken by the controller or processor to mitigate the damage suffered by data subjects;
4. the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them . . .
5. any relevant previous infringements by the controller or processor;
6. the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
7. the categories of personal data affected by the infringement;
8. the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement . . . [and]
9. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.[76]

Much of the media coverage is on how potential GDPR fines are so severe that many U.S. companies would have difficulty paying, exceeding the scope of their insurance policies.[77] Another important aspect of the sanctions that escapes attention, however, is that the penalties can be levied against individuals and small businesses with

[75] *See* sources cited *supra* note 69.

[76] EUROPEAN DATA PROT. BD., GUIDELINES 04/2022 ON THE CALCULATION OF ADMINISTRATIVE FINES UNDER THE GDPR 16-18, 25-28 (2022), https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf [https://perma.cc/T2VT-F3AU].

[77] Henry Kenyon, *U.S. Firms May Be Lacking in Cyber Insurance Coverage Against GDPR Fines*, CONG. Q. ROLL CALL, Sept. 21, 2018, 2018 WL 4518889.

limited means of defending against the proceedings, even if fines are in the hundreds or thousands (or alternatively a few days of incarceration for those who cannot pay) rather than the multimillions.[78] Part II below will present findings on this neglected but important aspect of the privacy penalization regime that has valuable lessons for the United States.

B. The Drive to Get Tougher on Privacy in the United States

In contrast to the EU, the U.S. lacks a comprehensive coordinated federal privacy law despite having a major share of the world's consumers and data-intensive companies.[79] Depending on perspective, the U.S. laissez-faire approach to privacy is credited for openness to innovation or criticized as a "Wild West" mess of lawlessness reflecting a "weak tradition" of privacy.[80] Regardless of ideological perspective, what is clear is that U.S. data privacy law is a patchwork varying by jurisdiction and type of data. For example, health data is protected differently than educational data and both are far more protected than the personal data accumulated from the products we use and sites that we visit daily.[81]

---

[78] For examples of prosecutions against individuals and small businesses, see *supra* text accompanying notes 9–32; *infra* Part II.B.

[79] *See, e.g.*, Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, U.S. COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/9MNH-4M5U] ("[T]he United States — home to some of the most advanced, and largest, technology and data companies in the world — continues to lumber forward with a patchwork of sector-specific laws and regulations that fail to adequately protect data.").

[80] *Compare, e.g.*, Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 370, 411 (2019) (describing critiques of America's "weak tradition" and "weak or nonexistent privacy regime"), *with* Jennifer Huddleston, *Preserving Permissionless Innovation in Federal Data Policy*, 22 J. INTERNET L. 17, 18 (2019) (explaining the problems with European-type strict privacy regulations on innovation and preferring American openness toward innovation though noting "critics allege that the United States has been a "Wild West" when it comes to data privacy and protection").

[81] *Compare* Family Educational Rights and Privacy Act of 1974 (FERPA), Pub. L. No. 93-579, 88 Stat. 1896 (2000) (codified as amended at 5 U.S.C. § 552a (2018)) (educational data), *with* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996), https://www.govinfo.gov/content/pkg/STATUTE-110/pdf/STATUTE-110-Pg1936.pdf [https://perma.cc/7KS6-EUBY] (health data). For a further discussion, see Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1440-45 (2001); Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/SYZ6-8DPV].

Responding to mounting criticism and calls for clarity, Congress has considered and debated numerous proposed federal privacy legislation over the years.[82] Efforts have foundered over disagreements on issues such as preemption of state laws, freedom of commerce, regulatory burdens on businesses, remedial and penalty approaches, and root ideological differences.[83] Numerous state legislatures also have considered privacy bills.[84] This Subsection offers background on one of the most influential state privacy laws, the CCPA, as amended by Proposition 24, the California Privacy Rights Act of 2020.[85] The Subsection then summarizes the plethora of emulators and wannabe legislation — some of which aim to get tougher, borrowing ideas from the GDPR.

[82] *See* JENNIFER HUDDLESTON, MERCATUS CTR., POLICY BRIEF: AN ANALYSIS OF RECENT FEDERAL DATA PRIVACY LEGISLATION PROPOSALS 1-5 (2019), https://www.mercatus.org/system/files/huddleston_-_policy_brief_-_an_analysis_of_recent_federal_data_privacy_policy_proposals_-_v1.pdf [https://perma.cc/Q6VN-DGMJ] (offering an overview of federal consumer data privacy proposals in the 115th and 116th Congress).

[83] *See, e.g.,* Mabel Crescioni & Tara Sklar, *The Research Exemption Carve Out: Understanding Research Participants Rights Under GDPR and U.S. Data Privacy Laws*, 60 JURIMETRICS J. 125, 135-36 (2020) (discussing differences in approaches that render federal legislation difficult); *GDPR & CCPA: Opt-Ins, Consumer Control, and Impact on Competition and Innovation: Hearing Before the S. Comm. On the Judiciary*, 116th Cong. (2019), https://www.judiciary.senate.gov/meetings/gdpr-and-ccpa-opt-ins-consumer-control-and-the-impact-on-competition-and-innovation [https://perma.cc/UP2S-P2VW] (discussing bipartisan and industry interest in crafting federal data privacy legislation but splitting on approaches). For studies on ideology and differing worldviews on privacy, see, for example, Sophie Cockcroft & Saphira Rekker, *The Relationship Between Culture and Information Privacy Policy*, 26 ELECTRON MKTS. 55, 56, 59, 62-63 (2015) (analyzing cultural predictors of the level of privacy legislation in national jurisdictions, including factors such as "group collectivism" emphasizing relatedness within groups rather than individualism; "assertiveness," meaning the level of tolerance for aggressive confrontational assertive social relations; "power distance," meaning the extent to which authority, power, and status differences are accepted; the "humane orientation" of the culture, meaning the tendency to value altruistic caring conduct; and "uncertainty avoidance," the tendency toward desiring rules, procedures and social norms to alleviate unpredictability); Kevin Lewis, Jason Kaufman & Nicholas Christakis, *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, 14 J. COMPUT.-MEDIATED COMMC'N 79, 93-94 (2008) (discussing differing cultural preferences, of which a "taste for privacy" is only part of the influences, even among the relatively more homogenous group of U.S students at a private college).

[84] *See 2020 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx [https://perma.cc/7UP3-XFVS] (summarizing for each state consumer data privacy legislation that has been introduced and the outcome).

[85] California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.110 to .199 (2022), *amended by* California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Prop. 24.

1. European-Californian Fusion Privacy

Taking the lead with its large consumer base, California passed the farthest-reaching privacy law to be successfully enacted in the United States.[86] Enacted a month after the GDPR entered into effect in the EU, CCPA became operative in January 2020.[87] The CCPA's consumer privacy rights and remedies will further expand in 2023, when the voter-approved Proposition 24, takes effect as the California Consumer Privacy Act.[88]

Under the California privacy regime, consumers receive similar rights of information, access, and control over their personal data as under the GDPR.[89] The CCPA gives consumers the right to request and know what personal information businesses acquire about them; sources and uses of the information; and whether and which third parties have received their personal data.[90] Like the GDPR, the CCPA also reaches companies based outside the jurisdiction if business also is conducted in the jurisdiction.[91]

Entering into force in 2023, Proposition 24, also known as the California Privacy Rights Act ("CPRA"), further adds more GDPR-like

[86] *See* Grant Davis-Denny, Jordan Navarette & Nefi Acosta, The *California Consumer Privacy Act*: 3 Early Questions, LAW360 (July 2, 2018, 4:28 PM EDT), https://www.law360.com/articles/1059403/the-california-consumer-privacy-act-3-early-questions [https://perma.cc/SM93-S57M].

[87] California Consumer Privacy Act of 2018, A.B. 375, 2017-2018 Reg. Sess. (Cal. 2018), *codified at* CIV. § 1798.100 to .199.

[88] *See* Sam Dean, *California Voters Approve Prop. 24, Ushering in New Rules for Online Privacy*, L.A. TIMES, https://www.latimes.com/business/story/2020-11-03/2020-california-election-tracking-prop-24 (last updated Nov. 4, 2020, 10:43 AM PT) [https://perma.cc/5RQP-TJLU] ("The new privacy law brings California more closely in line with the European Union's General Data Protection Regulation, and as the strongest law in the U.S. is likely to serve as the standard for companies across the nation.").

[89] *Compare* GDPR, *supra* note 6, arts. 12-23 (listing rights of the data subject), *with* CIV. § 1798.150 (enumerating consumer rights and protections).

[90] CIV. §§ 1798.100, 1798.115.

[91] Joanna Kessler, Note, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource,"* 93 S. CALIF. L. REV. 99, 112 (2019); Michael R. Overly, Is California's Consumer Privacy Act of 2018 Going to Be GDPR Version 2?, NAT'L L. REV. (Sept. 6, 2018), https://www.natlawreview.com/article/california-s-consumer-privacy-act-2018-going-to-be-gdpr-version-2 [https://perma.cc/ZPQ4-UR37]; *see* CIV. § 1798.140(c)(1) (defining a regulated business as one "that does business in California"); GDPR, *supra* note 6, art. 3 ("This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: 1. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or 2. the monitoring of their behaviour as far as their behaviour takes place within the Union.").

protections and principles.[92] For example, the legislation confers a similar right to the GDPR's principle of data minimization, requiring that the "collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed."[93] The voter-approved initiative also gives consumers the right to require that businesses correct incorrect information, or delete personal information altogether.[94] Consumers also have the right to know what information a business has on them, and the power to opt out of the sharing or sale of their personal information with third parties.[95]

While the robust bill of privacy rights bears European influences, the CCPA also is narrower than the GDPR in some major aspects. First, the CCPA, as amended by the CPRA, focuses obligations and penalties on businesses with substantial resources or access to data.[96] Regulated for-profit entities must meet at least one of the following criteria: (1) have more than $25 million dollars in gross annual revenues in the preceding year; (2) annually buys, sells or shares the personal information of 100,000 or more households; or (3) derives half or more of revenues from selling personal information.[97] In contrast, the GDPR is far broader in the potential reach of its regulations and penalties — regulating all "data controllers" — which can be natural as well as legal persons, from the humblest Uber driver or apartment dweller to multibillion-dollar corporations.[98]

Second, the CCPA is more limited in its conferral of a right of private action to supplement enforcement by governmental entities by seeking penalties than the GDPR.[99] The CCPA authorizes civil actions for data breaches, defined as "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate

[92] Dean, *supra* note 88.

[93] Proposition 24, § 1798.100(c).

[94] *Id.* §§ 1798.105 to .106.

[95] *Id.* §§ 1798.120, .135.

[96] *See* CIV. § 1798.140(d)(1).

[97] *Id.*

[98] GDPR, *supra* note 6, art. 4(7)-(8); *Data Controllers and Processors*, GDPR, https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/#What_Does_The_GDPR_Say_About_Controllers_And_Processors (last visited July 9, 2022) [https://perma.cc/38VM-THDE].

[99] *Compare* GDPR, *supra* note 6, arts. 77-84 (conferring rights to file complaints for violations of the GDPR with supervisory authorities and rights to a judicial remedy), *with* CIV. § 1798.150 (limiting the right to sue for data breaches).

to the nature of the information to protect the personal information."[100] As a further barrier, the CCPA as originally framed required consumers to provide a business with "30 days' written notice identifying the specific provisions . . . the consumer alleges have been or are being violated."[101] If the notified business cures the violation within 30 days and provides a written statement of the cure, then a civil suit for individual statutory damages or class-wide statutory damages is barred and the litigant is limited to suing for actual pecuniary damages.[102]

In contrast, under the GDPR, complainants have the right to lodge a complaint with a supervisory authority in their jurisdiction for an infringement of any of the GDPR's numerous protections and obligations — not just for data breaches.[103] Moreover, complainants also have an additional avenue through the right to a judicial remedy for any infringement of the GDPR, without prejudice to the administrative penalties sought.[104]

Third, the privacy penalties under the CCPA are far less severe than the privacy penalties under the GDPR. Statutory damages that may be recovered in civil actions for data breaches under the CCPA are limited to "seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater."[105] Administrative fines for CCPA violations are capped at $2,500 for each violation or $7,500 for each intentional violation under the CCPA as originally enacted.[106] Proposition 24, effective in 2023, will also extend the $7,500 penalty to violations involving the personal information of minors.[107]

In contrast, the GDPR's potential maximum administrative fines are far larger. For violations of certain obligations, such as data protection by design and security requirements, administrative fines can be "up to 10,000,000 EUR (approximately $11.8 million dollars), or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher."[108] The maximum fine amounts are doubled to "up to 20,000,000 EUR (approximately

[100] CIV. § 1798.150(a)(1).

[101] *Id.* § 1798.150(b).

[102] *Id.*

[103] GDPR, *supra* note 6, art. 77.

[104] *Id.* art. 79.

[105] CIV. § 1798.150(a)(1)(A).

[106] *Id.* § 1798.155(b). As amended by Proposition 24, entering into effect in 2023, the $7,500 heightened administrative fine applies to intentional violations involving the personal information of consumers that the business has actual knowledge are under 16 years old. Proposition 24, § 1798.155(a).

[107] Proposition 24, § 1798.199.90.

[108] GDPR, *supra* note 6, art. 83(4).

$23.6 million dollars), or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher" for violations of a range of other requirements, such as respecting data subjects' rights and obtaining consent.[109]

As originally framed in 2019, the CCPA delegated enforcement of the panoply of CCPA rights and obligations and the power to seek administrative penalties to the Attorney General's Office.[110] Businesses also could seek guidance on compliance from the Attorney General's Office.[111] Proposition 24, effective in 2023, strikes the provision explicitly providing that businesses may seek guidance on compliance from the Attorney General's Office.[112] The new provisions also delegate enforcement to a newly established California Privacy Protection Agency, governed by a five-member board.[113] The removal of an advisory role and creation of a dedicated enforcement agency brings California's privacy regime closer to the GDPR in regulatory design as well. The principal enforcers of the GDPR are dedicated Data Protection Authorities appointed in each member state, frequently a single body within each member state.[114]

Thus, California's consumer bill of rights bears strong European-style GDPR influences, such as the right to compel data deletion, reminiscent of the GDPR's right to be forgotten via data erasure.[115] The revisions in 2020 make California's enforcement mechanism more similar to the GDPR regime too. The most important distinction is in the range of potential targets and sanctions. In its current iteration, California's take on privacy rights goes after bigger-game highly capitalized companies with smaller-caliber penalties than the GDPR — at least for now. More proposals are multiplying, including legislation that would levy obligations and penalties on natural persons like the GDPR, not just focus on multimillion-dollar companies like the CCPA.[116] U.S. privacy

[109] *Id.* art. 83(5).

[110] CIV. § 1798.155(b).

[111] *Id.* § 1798.155(a).

[112] *See* Proposition 24, § 179.155.

[113] *Id.* § 1798.199.10.

[114] For a discussion of Data Protection Authorities, see, for example, Brian Daigle & Mahnaz Khan, *The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities*, J. INT'L COM. & ECON. 1, 5-8 (2020), https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf [https://perma.cc/7W7E-NDEP] (explaining GDPR enforcement structure).

[115] *See* CIV. § 1798.105 (right to seek deletion). *Cf.* GDPR, *supra* note 6, arts. 16-20 (right to seek erasure).

[116] *See, e.g.*, An Act Concerning Consumer Privacy, S.B. 893, 2021 Gen. Assemb., Jan. Sess. (Conn. 2021) (defining regulated controllers to mean "a natural or legal

law is in a fertile state of fluidity and flux as the U.S. searches for a more unified and protective regime, making insights about the impact of enforcement timely and important to attain to inform the debate.[117]

2. Proliferating Proposed Privacy Legislation

Since the passage of the CCPA, the states and U.S. Congress have debated an expanding volume of data privacy proposals.[118] Many of the bills deploy similar language, rights, and approaches as the GDPR, showing its enormous influence across the ocean. Some bills resemble the CCPA in focusing on large business entities.[119] But several of the proposed and recently passed comprehensive privacy regimes would sweep more broadly in causes of action and potential targets than the CCPA and — like the GDPR — penalize natural persons as well as major companies.

The nation's second major state data privacy regime to become law after the CCPA, Virginia's Consumer Data Privacy Act ("VCDPA"), uses the GDPR terms of "controller" and "processor" to refer to regulated persons and entities.[120] Virginia's law reaches more potential targets than the CCPA. Whereas the CCPA focuses on multi-million dollar businesses and enterprises that control or derive substantial portions of profits from selling personal data,[121] Virginia's law reaches natural as well as legal persons similar to the GDPR.[122] There is an American-style narrowing, however, to focus on persons conducting business or targeting consumers in Virginia that (i) "control or process personal data of at least 100,000 consumers or (ii) control or process personal

person that, alone or jointly with others, determines the purpose and means of processing personal data"); An Act Relating to the Management, Oversight, and Use of Data, S.B. 5062, 67th Leg., Reg. Sess. (Wash. 2021) (defining "controller" to mean "the natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data").

117 See discussion *supra* Part I.B.

118 *See* MÜGE FAZLIOGLU, IAPP, U.S. FEDERAL PRIVACY LEGISLATION TRACKER (2022), https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf [https://perma.cc/BYY4-HVM6]; *2021 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Dec. 27, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx [https://perma.cc/UH43-GW6K] (tracking state proposals).

119 *See, e.g.*, H.B. 1126, 2021 Gen. Assemb., Reg. Sess. (Pa. 2021) (focusing on large business entities, much like the CCPA).

120 Virginia Consumer Data Protection Act [VCDPA], 2021, ch. 52, 2021 Va. Acts § 59.1-571.

121 *See* CAL. CIV. CODE § 1798.140(c)(1) (2022).

122 VCDPA § 59.1-572(A).

data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data."[123]

Like the GDPR, the Virginia law requires data controllers and processors to practice data minimization, specifically, to "[l]imit the collection of personal data to what is adequate, relevant, and reasonably necessary."[124] Among other obligations, data processors and controllers also must establish reasonable data security practices and give consumers accessible privacy notices.[125] Virginia's law gives consumers the right to know what personal data regulated entities hold and the power to require correction of inaccuracies or deletion of their data.[126] Virginia consumers also may opt out of the use of their data for targeted advertising or sales of their data, among other rights.[127] The Attorney General holds the exclusive authority to pursue civil penalties, which can be up to $7,500 per violation plus payment of reasonable expenses incurred by the Attorney General in investigating and preparing the case, including attorney fees.[128]

Recent proposed legislation in diverse states such as Connecticut, Minnesota, Utah, and Washington, among others, would similar to the GDPR impose obligations on data "controllers" and "processers," including natural persons, not just companies.[129] The proposed state legislation would focus obligations and sanctions on persons or entities who control or process the data of 100,000 or more consumers per calendar year or 25,000 or more consumers while also deriving more than 25% (or 50% in some proposals) of gross revenue from personal data sales.[130]

Among other obligations, data controllers would, similar to the GDPR, be required to minimize personal data collection to what is reasonably necessary, relevant, and proportionate to the lawful purpose

[123] *Id.*

[124] *Id.* § 59.1-574(A)(1).

[125] *Id.* § 59.1-574(A)(3), (C).

[126] *Id.* § 59.1-573(A)(1)-(3).

[127] *Id.* § 59.1-573(A)(5).

[128] *Id.* § 59.1-580(A), (C)-(D).

[129] S.B. 893, 2021 Gen. Assemb., Jan. Sess. (Conn. 2021) (joint favorable substitution) (defining regulated controllers to mean "a natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data"); Minnesota Consumer Data Privacy Act, H.F. 1492, 2021 Leg., 92d Sess. (Minn. 2021); Utah Consumer Privacy Act, S.B. 200, 2021 Leg., Gen. Sess. (Utah 2021); Washington Privacy Act, S.B. 5062, 67th Leg., Reg. Sess. (Wash. 2021).

[130] Conn. S.B. 893 § 2; Minn. H.F. 1492 § 3250.03; Utah S.B. 200 § 13.58-201; Wash. S.B. 5062 § 102.

of collection disclosed to the consumer.[131] Civil penalties for a violation vary; for example in Connecticut, Minnesota, and Washington it would be up to $7,500 per violation.[132] States such as Connecticut and Washington also provide for the payment of reasonable expenses incurred by the Attorney General in investigating and preparing the case.[133]

These are just snapshots of some of the major legislation proliferating in the states, many drawing from the successfully enacted regimes of the GDPR, the CCPA, and the VCDPA. Even when terms are taken from the GDPR such as data "controllers" and "processors" to define regulated entities, whether the terms are defined to include natural persons as well as business entities differ. For example, recently introduced legislation in Florida borrows the term controller and processor from the GDPR and the VCDPA but defines it more narrowly, to focus on business entities, similar to the CCPA.[134]

Thus, U.S. privacy law is in fertile flux as proposals are amended and proposals hybridized into an evolving European-American fusion of privacy rights. An emerging theme across some U.S. proposals from New York to Washington is a European-style explicit recognition of privacy as a fundamental right.[135]

II. THE IMPACT OF PRIVACY PENALIZATION BEYOND THE HEADLINES

While strong information privacy rights in the lawbooks are a major advance, the details of how privacy penalties actually impact people is important.[136] To understand the impact of privacy punishment, it is important to look beyond the formal law on the books to operation on the ground.[137]

---

131 Conn. S.B. 893 § 5; Minn. H.F. 1492 § 3250.09; Utah S.B. 200 §§ 13.58-201, 13.58-302(2); Wash. S.B. 5062 § 107(2)-(3).

132 Conn. S.B. 893; Minn. H.F. 1492; Wash. S.B. 5062.

133 Conn. S.B. 893; Wash. S.B. 5062.

134 Florida Privacy Protection Act, S.B. 1864, 2022 Leg., Reg. Sess. (Fla. 2022).

135 *See, e.g.*, New York Privacy Act, S.B. 6701, 2021-2022 Leg., Reg. Sess. (N.Y. 2021) ("Privacy is a fundamental right and an essential element of freedom."); Wash. S.B. 5062 ("The legislature finds that the people of Washington regard their privacy as a fundamental right and an essential element of their individual freedom.").

136 *See, e.g.*, John C. Reitz, *How to Do Comparative Law*, 46 AM. J. COMPAR. L. 617, 630 (1998) (explaining from a comparativist's perspective, the need to be attentive to potential gaps between formal laws and "the actual impact of the law in the world").

137 *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN L. REV. 247, 259 (2011) (explaining the importance of going beyond the privacy laws on the books to examine privacy practices in the field and on the ground).

Critics of GDPR enforcement, such as the International Bar Association, have raised concerns that few corporate giants have been penalized under the GDPR despite repeated data breaches.[138] This Article investigates a different important question that is oft-overlooked in the focus on the highly capitalized and powerful. What is the impact of the GDPR's privacy and punishment regime on people and entities with less power and resources? The goal is to bring the privacy penalty jurisprudence of the powerless out from the shadows. This Part presents the methods deployed to investigate the question and findings.

To summarize: while the GDPR has been the basis for some headline-garnering penalties against major companies, there is also what this Article terms a shadow jurisprudence of the disgruntled sheltered by obscurity, away from public attention. Police officers angry about being recorded by members of the public,[139] neighbors disgruntled by another neighbor's security system,[140] false Tinder profiles,[141] even the use of simulated security video surveillance that did not actually record on a building façade,[142] and similar such irritations have led to GDPR penalty proceedings and this overlooked jurisprudence of small targets. This hidden-in-plain-sight category of GDPR litigation is not a mere benign

[138] Margaret Taylor, *Data Protection: Threat to GDPR's Status as "Gold Standard,"* INT'L BAR ASS'N (Aug. 25, 2020), https://www.ibanet.org/article/A2AA6532-B5C0-4CCE-86F7-1EAA679ED532 [https://perma.cc/67SD-4VL4].

[139] *See, e.g.*, Datenschutzbehörde [DSB] [federal Data Protection Authority for Austria], Istvan O*** Straferkenntnis [Penalty Judgment] Sept. 27, 2018, Case DSB-D550.084/0002, at II.II.2, https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20180927_DSB_D550_084_0002_DSB_2018_00/DSBT_20180927_DSB_D550_084_0002_DSB_2018_00.pdf [https://perma.cc/L3MK-94SQ] (prosecution of a motorist for having dash cameras noted by police officers during a stop).

[140] *See, e.g.*, [Autoritié de Protection des Données] [APD] [Belgian Data Protection Authority] Nov. 24, 2020, Case 74/2020, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-74-2020.pdf [https://perma.cc/PV68-EMYW] (adjudicating and imposing penalties in a dispute brought by neighbors against the defendant's installation of security cameras on the defendant's property that could also capture in the field of view the public record and parts of neighbors' property).

[141] *See, e.g.*, Agencia Espa ola Protección Datos [AEPD] [national Data Protection Authority for Spain] Oct. 19, 2020, Procedimiento Nº: PS/00278/2020, Resolución R/00565/2020 de Terminación del Procedimiento por Pago Voluntario, https://www.aepd.es/es/documento/ps-00278-2020.pdf [https://perma.cc/Z553-Z2KV] (adjudicating and imposing penalties based on complaint brought by pseudonymized plaintiff who discovered that a person on Tinder was using the plaintiff's photos in profile and on Whatsapp account used for setting up encounters).

[142] Agencia Espa ola Protección Datos [AEPD] [national Data Protection Authority for Spain] Oct. 16, 2020, Procedimiento Nº: PS/00215/2020, Resolución R/00589/2020 de Terminación del Procedimiento por Pago Voluntario, https://www.aepd.es/es/documento/ps-00215-2020.pdf [https://perma.cc/AA6N-DT67] (imposing penalties for installing non-recording cameras on a business to deter robberies).

oddity because it shows the risk that expansive privacy penalty regimes and broad amorphous rights can provide cover to vent hostilities and harass.

A. Methods

More than three years of experience under the GDPR has yielded a body of privacy penalty decisions that offer potentially valuable data regarding the experience of privacy penalization on the ground.[143] The challenge of collecting and analyzing these cases is that the documents are in various national Data Protection Agency databases and come in a linguistic rainbow: Czech, Dutch, Estonian, French, German, Italian, Polish, Spanish, Swedish, and much more.[144]

For this study, a multilingual team focused on collecting privacy penalty decisions from 20 European Union Member states. The team had the linguistic capacity to read decisions in the original English, French, German, and Spanish. For decisions in other languages, the team first sought official English translations and, where unavailable, used Google's machine translation system. Table 1 below shows the EU members states represented in the dataset.

Table 1. Privacy Penalty Decisions from 20 European Member States

Austria	Estonia	Ireland	Portugal
Belgium	Finland	Isle of Man	Romania
Croatia	France	Italy	Slovakia
Czech Republic	Germany	Luxembourg	Spain
Denmark	Iceland	Poland	United Kingdom

The study covers decisions rendered between 2018, when the GDPR first entered into full effect, through January 3, 2022. The search for privacy penalty decisions began with the GDPR Enforcement Tracker created by CMS International and radiated to searches of the databases of national Data Protection Authorities and governmental entities,

[143] *See* discussion *infra* Parts II.B.1, II.B.2.

[144] For example, see the GDPR penalty decisions discussed *supra* notes 9, 20–32, 139–42 and *infra* notes 171–93; *cf. Languages*, EUROPEAN UNION, https://european-union.europa.eu/principles-countries-history/languages_en#:~:text=The%20EU%20has%2024%20officialial,%2C%20Slovenian%2C%20Spanish%20and%20Swedish (last visited Feb. 7, 2022) [https://perma.cc/B2VY-M9PH] (noting that the "EU is characterized by its cultural and linguistic diversity" and the EU has 24 official languages).

supplemented where necessary with media searches.[145] The GDPR Enforcement tracker by CMS, a data protection and information security specialist firm, lists dates of decisions and the name of the data controller or processor receiving the penalty, where the name is available.[146] Drawing on these leads, the team searched for the actual decision on the sites of the national Data Protection Authority to code whenever available. The team began with a set of 617 potential penalties to analyze and ultimately were able to locate the details of cases to successfully code 571 penalty decisions.

A codebook for analyzing the decisions became refined via an iterative process useful in law and policy analyses where discoveries of further variations can inform and update constructs at the outset.[147] Examples of key variables included the identity category of the complainant (for example, neighbor, customer, police, or government inspector) and the identity category of the defendant (for example, individual, small business, or large business). The team also coded and analyzed the complaint pattern based on identity categories (for example, customer against major corporation, neighbor against neighbor). The team examined the penalty amount assessed, whether the proceeding was characterized as criminal or civil, the main types of allegations, and the GDPR articles that formed the basis of the complaint and penalty.

To check inter-rater reliability, a second coder coded a random sample of another coder's batch of decisions. Inter-rater reliability calculations using Cohen's kappa, summary statistics, and two-sample proportion tests for significance of differences were conducted using Stata 14 SE statistical software.[148] There was substantial agreement in the coding. The team resolved any conflicts by consensus involving a third review.

As discussed further below, the study found significant differences in the probability of individual defendants compared to major corporations being prosecuted under certain GDPR provisions.[149] The study also found significant differences in the proportion of small businesses compared to major corporations being targeted under

[145] *GDPR Enforcement Tracker*, CMS, https://www.enforcementtracker.com/ (last visited Feb. 8, 2022) [https://perma.cc/PH3U-YM3X].

[146] *Id.*

[147] For a discussion of iterative process in law and policy evaluation, see Charles Tremper, Sue Thomas & Alexander C. Wagenaar, *Measuring Law for Evaluation Research*, 34 EVALUATION REV. 242, 244 (2010).

[148] StataCorp., Stata Statistical Software: Release 14 (2015).

[149] *See infra* Tables 6, 8.

certain GDPR provisions.[150] Whether the differences in proportions were statistically significant was evaluated using a two-sample test for the equality of proportions.[151]

B. Target Thy Neighbor or Local Small Business: Findings

One of the aims of this Article is to illuminate the targets of privacy penalties who are neglected in breathless press coverage focused on multimillion dollar penalties against major companies.[152] Accordingly, this Section discusses findings on the proportion of penalty decisions issued against private individuals and small businesses, patterns in how such cases were initiated, fine amounts, and which GDPR articles are most likely to be the basis of penalties.[153] This Section also reports findings regarding which GDPR articles are significantly more likely to be the basis of penalties against individuals and small businesses, compared to major corporations.[154] Conversely, the findings also include which GDPR articles are significantly more likely to be the basis of penalties against major corporations compared to individuals or small businesses.[155]

In addition to the quantitative figures, this Section also offers qualitative stories from what the Article dubs the shadow privacy penalty jurisprudence of the powerless. Beyond the numbers, the case studies delve into how privacy penalties can be used and abused in vendettas against people and small businesses with far less resources to defend than the usual megacompanies that capture attention.

---

150 *See infra* Tables 7-8.

151 In Stata 14 SE, this is the command prtest. *Prtest — Tests of Proportions*, STATA.COM, https://www.stata.com/manuals/rprtest.pdf (last visited July 31, 2022) [https://perma.cc/5R8K-2DAV].

152 *See, e.g.*, Natasha Lomas, *France Spanks Google $170M, Facebook $68M over Cookie Consent Dark Patterns*, TECHCRUNCH (Jan. 6, 2022, 3:03 AM PST), https://techcrunch.com/2022/01/06/cnil-facebook-google-cookie-consent-eprivacy-breaches/ [https://perma.cc/4PTU-BSWR] (noting recent fines against Google and Facebook); *Three Years of GDPR: The Biggest Fines so Far*, BBC NEWS (May 24, 2021), https://www.bbc.com/news/technology-57011639 [https://perma.cc/9C2N-AKMX] (reporting on 50 million euro fine against Google, 35.3 million euro fine against H&M, and other multimillion euro fines against massive corporations).

153 *See infra* Tables 2-10.

154 *See infra* Tables 6-7.

155 *See infra* Table 8.

1. Private Person and Small Business Targets for Privacy Penalties

In the more than three years since the GDPR has taken full effect, small businesses such as snack stands, convenience shops and laundromats, comprise 15.5% of the targets for penalties in this large sample.[156] Individual targets comprise nearly 6% of the targets — and nearly half of the individual-target cases involved disputes against a neighbor.[157]

Even more concerning, at least 20.6% of the privacy penalty cases against individual persons were designated criminal.[158] At least 25.56% of the privacy penalty cases against small businesses were designated criminal.[159] In addition to the formal fine, a criminal designation carries a panoply of potential collateral consequences affecting employment, housing eligibility, licensing, immigration status and more — potentially inducing what Gabriel Chin termed "civil death."[160]

[156] *See infra* Table 2.

[157] *See infra* Table 2.

[158] Specifically, 7 out of 34 cases against individuals, including neighbors, were designated criminal. This is a baseline figure because the civil or criminal designation could not be determined from the decision text in four cases.

[159] Specifically, 23 out of 90 small business cases were designated criminal. This is a baseline figure that could be higher because the civil or criminal designation could not be determined from the decision text in three cases.

[160] For discussions of collateral consequences of criminal convictions see Gabriel J. Chin, *The New Civil Death: Rethinking Punishment in the Era of Mass Conviction*, 160 U. PA. L. REV. 1789, 1790-92, 1799-802 (2012) [hereinafter *The New Death*]; Michael Pinard, *Collateral Consequences of Criminal Convictions: Confronting Issues of Race and Dignity*, 85 N.Y.U. L. REV. 457, 489-90 (2010).

Table 2. Who Are the Defendants in Privacy Penalty Decisions?

Defendant Type	Number of Cases[161]	Proportion of Sample
Neighbor of Complainant	16	2.76%
Individual (not neighbor)	18	3.1%
Government	51	8.78%
Small Business	90	15.52%
Medium-Large Business	127	21.89%
Major High Cap Business	172	29.66%
Nongovernmental Organizations	5	0.86%
Health Sector (e.g., physician, clinic, pharmacy med. ass'n)	35	6.03%
Housing Association	9	1.55%
Law Enforcement Officer	4	0.69%
Politician/Political Candidate/Political Party	11	1.90%
Schools/Education	16	2.76%
Website/Media	10	1.72
Union	1	0.17

The shadow privacy penalty jurisprudence against small-fry individuals is a tapestry of tales of the disgruntled — particularly disgruntled neighbors. The most prevalent complaining party who launched a privacy penalty proceeding against an individual was a neighbor (35.29%). More than half of all privacy penalty cases against individuals were launched by another individual or neighbor (55.88%). In distant third place as the catalyzing category of complainants in cases against individuals are police officers or government inspectors (8.82%), who were coded separately from private individuals though it is worth acknowledging potential conceptual slippage in the categories because an officer is an individual; albeit an official one.

[161] The number of cases for which we were able to code the defendant type was 580 in total rather than 571 because more data was available on the defendant than other variable categories, such as complainant.

Table 3. Complaining Parties in Cases Against Individuals

Complainant against Individual	Number of Cases	Proportion of Cases[162]
Neighbor	12	35.29%
Individual	7	20.59%
Police or Inspector	3	8.82%
Group of Businesses	2	5.88%
Customer	1	2.94%
Municipality	1	2.94%
Residential/Homeowner's Ass'n	1	2.94%
Residents of Property	1	2.94%
Unknown	2	5.88%

Apparently disgruntled individuals also comprise the largest category of complainants against small businesses at 37.67% of the sample of penalty decisions against small businesses. Customers comes in second as a category of catalyzing complainant at 17.78% of the small business penalty decisions in the sample. Again, police officers or inspectors comes in as the third most prevalent catalyzing complainant in cases against small businesses.

Table 4. Complaining Parties in Cases Against Small Businesses

Complainant against Individual	Number of Cases	Proportion of Cases[163]
Individual	34	37.67%
Customer	16	17.78%
Police or Inspector	13	14.44%
Municipality or Gov't Agency	7	7.77%
Employee	5	5.56%
Neighbor	4	4.44%
Unknown	3	3.33%
Self-Reported Violation	2	2.22%
Residential/Homeowner's Ass'n	2	2.22%
NGO	1	1.11%
Other Business(es)	2	2.22%
Pedestrians	1	1.11%

[162] The denominator is the number of cases against individuals, including neighbors, which equals 34.

[163] The denominator is the number of cases against small businesses, which equals 90.

The most prevalent bases for penalties against individuals are violations of GDPR Articles 5 and 6. To compare whether Articles 5 and 6 are more likely to be the basis of penalties against individuals than major corporations in the sample, the data analysis included a two-sample test on the equality of proportions. This significance testing found that Articles 5 and 6 accounted for a significantly larger proportion of penalties against individuals in the sample, than against major corporations in the sample (art. 5: p=0.0043; Art 6: 0.046). During coding, major corporations were defined as highly capitalized businesses with a market capitalization in the multimillions or multibillions such as Google, Vodafone, and Twitter.

Article 5 is a broad statement of general principles related to data processing.[164] Article 5 provides, in relevant part that is most frequently invoked against individuals:

> Personal data shall be:
>
> > (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
> >
> > (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes . . . ;
> >
> > (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').[165]

Article 6, the second most prevalent basis of penalties against individuals, requires consent by the data subject for processing, unless an exception applies, such as the "vital interests of the data subject or another person" or necessity to perform a contract.[166]

[164] GDPR, *supra* note 6, art. 5(1)(a)-(c).

[165] *Id.*

[166] *Id.* art. 6.

Table 5. Most Common GDPR Articles Underlying Penalties by Defendant Type[167]

Order of Impact	Individual	Small Business	Major Corporation
1st Prevalent Basis	Art. 5 (70.6%)	Art. 5 (52.2%)	Art. 6 (47.1%)
2d Prevalent Basis	Art. 6 (61.8%)	Art. 13 (38.9%)	Art. 5 (45.9%)
3d Prevalent Basis	Art. 13 (17.6%)	Art. 6 (35.6%)	Art. 32 (26.7%)
4th Prevalent Basis	Art. 14 (8.8%)	Art. 12 (13.3%)	Art. 13 (10.5%)
5th Prevalent Basis	Art. 7 (5.9%)	Art. 32 (11.1%)	Art. 12 (9.9%)

Table 6. Heightened Risk of an Individual Defendant, Compared to a Major Corporation, Incurring Penalties, by GDPR Article, P-Values (Significance Test for Difference in Proportions)

GDPR Article	Individ. % (tot. N=34)	Major Corp % (tot. N =172)	P-Value
Art. 5	70.6%	45.9%	0.0043*
Art. 6	61.8%	47.1%	0.046*
Art. 13	17.6%	10.5%	0.12

For small businesses, GDPR Article 13 was another prevalent basis of privacy penalties in addition to Article 5. To compare whether certain GDPR articles are more likely to be the basis of penalties against small businesses compared to major corporations in the sample, the data analysis included a two-sample test on the equality of proportions. The analysis found that GDPR Articles 13 and 14 accounted for a significantly larger proportion of privacy penalties against small businesses in the sample than major corporations (Art. 13: $p < 0.001$; Art. 14: $p=0.03$;). Article 13 governs notice by prescribing the kinds of information a data controller must give to the subject when personal data is collected.[168] Article 14, an infrequent basis of penalties in the sample, governs the kinds of information a data controller must give a data subject even where personal data has not been collected.[169]

[167] Because multiple GDPR articles can be the basis of imposing a penalty, the proportions exceed 100%.

[168] GDPR, *supra* note 6, art. 13.

[169] *Id.* art. 14.

Table 7. Heightened Risk of a Small Business Defendant, Compared to a Major Corporation, Incurring Penalties, by GDPR Article, P-Values (Significance Test for Difference in Proportions)

GDPR Article	Sm. Bus. % (tot. N=90)	Major Corp % (tot. N=172)	P-Value
Art. 5	52.2%	45.9%	0.17
Art. 12	13.3%	9.9%	0.20
Art 13	38.9%	10.5%	0.00*
Art. 14	8.9%	3.5%	0.03*

Table 8. Heightened Risk of a Major Corporation Defendant, Compared to Individual Defendant and Small Business Incurring Penalties, by GDPR Article, P-Values (Significance Test for Difference in Proportions)

GDPR Article	Major Corp % > Small Bus. % P-Value	Major Corp % > Individual % P-Value
Art. 6	0.053*	0.95
Art. 7	0.052*	0.41
Art. 12	0.095	0.80
Art. 15	0.15	0.065
Art. 25	0.026*	0.22
Art. 32	0.0017*	0.0013*

Which articles were more likely to be the basis of penalties against major corporations rather than small businesses and individuals is valuable to know because it shows which provisions are more likely to be used against large game rather than small fry individuals. To compare whether certain GDPR articles are more likely to be the basis of penalties against major corporations compared to individuals and small businesses, the data analysis included a two-sample test on the equality of proportions.

In general Articles 7 and 32 far more frequently formed the basis of penalties against major corporations than for individuals and small businesses. Article 7 governs the conditions for obtaining and demonstrating consent to processing and prescribes the right to withdraw consent. Article 7 was significantly more likely to be the basis of penalties against major corporations than small businesses ($p=0.052$).

Article 32 requires controllers and processors to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk," including, among other measures,

"pseudonymisation and encryption of personal data" and "resilient" processing systems and services.[170] Article 32 was significantly more likely to be the basis of penalties against major corporations than either individuals (p=0.0013) or small businesses (p=0.0017). Major corporations also were more likely to be punished for violations of Article 25 on data protection by design and default, and Article 6 on lawfulness of processing than small businesses (Art 25: p=0.026; Art. 6: p=0.053).

2. Stories from the Shadow Privacy Penalty Jurisprudence of Small Targets

Beyond the numbers, consider these cautionary tales from the shadow privacy penalty jurisprudence of small targets. Take the case of Mr. Istvan O*** ("Istvan"), a low-income Hungarian national who, was driving a vehicle with a Hungarian license plate in Austria.[171] During a roadside stop by police on May 9, 2018, officers noticed Istvan had a dashcam on his front windshield and rear window that was triggered by motion.[172] When asked why he had the cameras, which were recording the officers, Istvan explained that he needed the footage in case of an accident.[173] The officers testified that Istvan admitted at the scene that images from the dash cams were stored on a memory card though in subsequent police interrogation he denied the images were stored.[174]

For the temerity of having dash cameras — technology frequently used by U.S. motorists for the same reasons as Istvan and for protection in police encounters[175] — the police put Istvan in criminal proceedings.[176] The charges against Istvan were violations of GDPR Article 5 and 6. Recall that GDPR Article 5 is a broad statement of principles, including fair and transparent data processing, and data

[170] *Id.* art. 32.

[171] Istvan O Straferkenntnis [Penalty Judgment], Case DSB-D550.084/0002-DSB, *supra* note 139, at I.I.1.

[172] *Id.* at I.I.3.

[173] *Id.* at II.II.2.

[174] *Id.* at II.II.3.

[175] *See, e.g.*, Benjamin Preston, *Dash Cams Can Be Silent Witnesses During Police Traffic Stops and Other Incidents*, CONSUMER REP., https://www.consumerreports.org/law-enforcement/dash-cams-can-be-silent-witnesses-during-police-traffic-stops-and-other-incidents/ (last updated July 29, 2020) [https://perma.cc/8445-VS7M] (explaining how motorists protect against racial profiling and pretextual stops).

[176] Istvan O Straferkenntnis [Penalty Judgment], Case DSB-D550.084/0002-DSB, *supra* note 139, at II.II.2.

minimization to what is necessary and relevant.[177] GDPR Article 6 concerns the conditions for lawful data processing, requiring the data subject's consent or another basis.[178]

The Austrian Data Protection ruled that Istvan's dashcams constituted "a high level of wrongdoing" and "systematic violation" of the GDPR provisions because they were activated by motion on roadways, potentially recording motorists (and apparently police officers) without their consent.[179] The Austrian Data Protection Authority refused to recognize "any legitimate interest" in the operation of the dash cameras, especially in the motion sensor feature.[180]

Istvan asked for mercy on the penalty from the Austrian Data Protection Authority, explaining he was the father of three children, one of whom was physically disabled.[181] He had "marginal employment," as the Data Protection Authority put it, and earned a net monthly income of 900 euros.[182] He also had no assets and was behind in tax payments, owing 1,300 euros.[183] The Austrian Data Protection Authority imposed a fine of 300 euros — or 36 hours of substitute imprisonment if he could not afford to pay.[184]

Police officers are hardly the only disgruntled entities with the power to haul people into privacy penalty proceedings under the GDPR. More frequently, it's the neighbors.[185] Consider, for example, how privacy penalties became the latest salvo in "longstanding neighborly disputes" between the accused Martin N*** ("Martin", the complainant Ms. Susanne F*** ("Susanne"), and their spouses.[186]

Susanne took sick leave from her work, claiming that neighbor Martin had induced a mental illness in her.[187] Based on Susanne's claim that her leave was due to mental illness induced by Martin, her municipal

---

177 GDPR, *supra* note 6, art. 5.

178 *Id.* art. 6.

179 Istvan O Straferkenntnis [Penalty Judgment], Case DSB-D550.084/0002-DSB, *supra* note 139, at IV.IV.4.

180 *Id.* at III.III.7.

181 *Id.* at I.I.5.

182 *Id.*

183 *Id.*

184 *Id.* at 2.

185 *See supra* Table 3.

186 Datenschutzbehörde [DSB] [federal Data Protection Authority for Austria], Beschuldigter: Martin N*** [Accused: Martin N***] Aug. 5, 2021, Case 2021-0.518.795, at 1.4, https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20210805_2021_0_518_795_00/DSBT_20210805_2021_0_518_795_00.html [https://perma.cc/68Y5-ED97].

187 *Id.* at 1.6, 3.6.

employer sent a demand for payment from Martin for lost services from Susanne.[188] In an email, Martin contested the demand for payment by saying he was not the cause of Susanne's alleged disability.[189] In his defense email, he attached a doctor's statement about the bases of Susanne's condition that he obtained from prior litigation between the disputatious neighbors.[190]

Martin's attempt to defend against the demand for payment by appending his evidence to the email became the basis for the criminal privacy penalty proceeding. The Data Protection Authority and the Federal Administrative Court of Austria found Martin in violation of Article 9 of the GDPR, pertaining to special categories of personal data, including health data.[191] Martin informed the Federal Administrative Court that he was unemployed and subsisted off social assistance benefits.[192] Nonetheless, the Court imposed a fine of 600 euros or 36 hours of substitute incarceration if he was unable to pay the fine.[193]

III. HOW TO PROTECT THE VULNERABLE FROM PRIVACY PENALIZATION HARMS

In framing privacy penalties justified on the basis of harms that major players can wreak, people and small businesses with far less resources to defend should not also be swept into the net as collateral damage. The point is that broad privacy penalties can become tools to harm and harass — and this finding is important regardless of what proportion of GDPR penalty decisions such cases constitute. The fact that many privacy penalty cases do indeed involve other entities with more power and resources does not address the lived experience of potential harm for people and small businesses with far less power.[194] To take a more familiar analogy in our popular discourse on police reform: the fact that traffic stops do indeed net many speeders, intoxicated persons, and other motorists who pose a danger does not make minor stops based on invidious racial profiling any less destructive for the people impacted — and ultimately for inequality and mistrust in the nation.[195] Moreover,

[188] *Id.*

[189] *Id.*

[190] *Id.* at 1.2, 1.6, 3.6.

[191] GDPR, *supra* note 6, art. 9.

[192] Beschuldigter: Martin N***, Case 2021-0.518.795, *supra* note 186, at 1.7.

[193] *Id.*

[194] *See supra* Parts II.B.1–II.B.2, Tables 2, 3-4, 6-7.

[195] *See, e.g.*, Richard R.W. Brooks, *Fear and Fairness in the City: Criminal Enforcement and Perceptions of Fairness in Minority Communities*, 73 S. CAL. L. REV. 1219, 1228 (2000) (discussing the harmful impact on minority-police relations and community

it would be cruel to demand that impacted people parse an opaque corpus of decisions where invidious intent is often veiled to meet some threshold of prevalence to get protection.[196]

This Part crosses the disciplinary silos between critical criminal justice movements and information privacy to explain why seemingly minor penalties can exacerbate inequality and offer proposals on how to better prevent harms. The Article proposes three guidelines for framers of privacy regimes. First while broad language makes for grand statements of rights, such amorphous language increases the risk of misuse if allowed to constitute the basis of penalties. Penalty language must be more precise as to what constitutes punishable wrongdoing and who can be punished. Second, privacy penalty regimes should have safe harbors for individual persons and small businesses with less resources. Here the EU can learn from U.S. privacy proposals, which often contain better focused targeting of penalties on entities and persons with more power to perpetrate privacy harms — and to meet regulatory standards and defend in penalty proceedings. Third, the Part proposes an advisory capacity for regulators, not just a primary quasi-prosecutorial role. After all, the goal is to prevent privacy harms in the first place and induce better practices — not just impose penalties after harms are done.

experiences and perceptions); Devon W. Carbado, *Stop-and-Strip Violence: The Doctrinal Migrations of Reasonable Suspicion*, 55 HARV. C.R.-C.L. L. REV. 467, 481-89 (2020) (discussing the experience of violence, fear and intimidation underlying police stops based on racial profiling); David A. Harris, *"Driving While Black" and All Other Traffic Offenses: The Supreme Court and Pretextual Traffic Stops*, 87 J. CRIM. L. & CRIMINOLOGY 544, 570-71 (1997) (discussing how targeted people feel "helpless" and despair at such practices); Tracey Maclin, Terry v. Ohio*'s Fourth Amendment Legacy: Black Men and Police Discretion*, 72 ST. JOHN'S L. REV. 1271, 1282-83 (1998) (discussing the "resentment and hostility" generated by such practices); David A. Sklansky, *Traffic Stops, Minority Motorists, and the Future of the Fourth Amendment*, 1997 SUP. CT. REV. 271, 272 ("For many motorists, particularly those who are not white, traffic stops can be not just inconvenient, but frightening, humiliating, and dangerous.").

[196] *Cf.* Alan David Freeman, *Legitimizing Racial Discrimination Through Antidiscrimination Law: A Critical Review of Supreme Court Doctrine*, 62 MINN. L. REV. 1049, 1056 (1978) (critiquing the "nearly impossible burden of isolating the particular condition of discrimination, produced by and mechanically linked to the behavior of an identified blameworthy perpetrator"); Aziz Z. Huq, *What Is Discriminatory Intent?*, 103 CORNELL L. REV. 1211, 1286 (2018) (discussing the regressive effect of evidentiary burdens to prove discriminatory intent and the opacity of discerning intent); Sandra L. Simpson, *Everyone Else Is Doing It, Why Can't We? A New Look at the Use of Statistical Data in Death Penalty Cases*, 12 J. GENDER RACE & JUST. 509, 519 (2009) (discussing how heavy evidentiary burdens "hamstring criminal defendants and saddle them with the heavy burden of providing nearly unattainable evidence").

A. Why Seemingly Minor Penalties Matter

A new wave of recent criminal justice scholarship and activism has argued for attention to how seemingly minor offenses and penalties can produce major harms.[197] Misdemeanors, civil offenses, and other ostensibly minor legal sanctions evade attention, yet carry collateral consequences and put substantial burdens on people least well-situated to bear them.[198] Even penalties for formally civil offenses can be the entryway into amplifying harms for people unable to pay fines, fees, and assessments that if unpaid can become criminal matters.[199]

A seemingly minor offense can disqualify people for jobs, licenses, and the ability to earn a living and find housing.[200] Immigration consequences can ensue for people perilously placed because of immigration status and the intersection of immigration status, economic uncertainty, and racial and ethnic disparities.[201] The growing literature on the yolk of legal financial obligations ("LFOs") illuminates how an initial fine amount can balloon for people who cannot afford to pay, with interest, additional penalties, and potentially even criminal sanctions for nonpayment.[202]

Worse, because minor offenses capture a lot of commonplace conduct, the risk of arbitrary and discriminatory enforcement is higher.[203] The more everyday behavior falls within a minor offense's

---

197 *E.g.*, KOHLER-HAUSMANN, *supra* note 44, at 51-56, 66-73, 276 (discussing how minor offenses can produce major harms); NATAPOFF, *supra* note 44, at 3-12, 149-70; Joe, *supra* note 44, at 756-71 (arguing that even convictions of minor offenses significantly harm defendants); Roberts, *supra* note 44, at 297-306 (arguing that even minor offenses can produce major harms).

198 Joe, *supra* note 44, at 758-69.

199 ALEXES HARRIS, A POUND OF FLESH: MONETARY SANCTIONS AS PUNISHMENT FOR THE POOR 18 (2016).

200 Chin, *The New Death*, *supra* note 160, at 1790-92, 1799-802; Pinard, *supra* note 160, at 489-90.

201 Roberts, *supra* note 44, at 297-99.

202 HARRIS, *supra* note 199, at 52-70, 151-55; KATHERINE A. BECKETT, ALEXES M. HARRIS & HEATHER EVANS, WASH. STATE MINORITY & JUST. COMM'N, THE ASSESSMENT AND CONSEQUENCES OF LEGAL FINANCIAL OBLIGATIONS IN WASHINGTON STATE 36-61 (2008), https://media.digitalarchives.wa.gov/do/0913F10B8D16D1EEC8A99FEC93E4772E.pdf [https://perma.cc/6P75-XJP9]; Karin D. Martin, Bryan L. Sykes, Sarah Shannon, Frank Edwards & Alexes Harris, *Monetary Sanctions: Legal Financial Obligations in U.S. Systems of Justice*, 1 ANN. REV. CRIMINOLOGY 471, 471-89 (2018).

203 *See, e.g.*, Debra Livingston, *Police Discretion and the Quality of Life in Public Places: Courts, Communities, and the New Policing*, 97 COLUM. L. REV. 551, 610-11 (1997) (discussing the risks of laws penalizing "trivial misconduct" for "increased danger of abusive enforcement"); Robert Weisberg, *Foreword: A New Agenda for Criminal Procedure*, 2 BUFF. CRIM. L. REV. 367, 375 (1999) ("For years, critics of police discretion

definition, the more law enforcers can choose who to target for fines, penalties, and assessments.[204] Targeting the powerless continues the cycle of silence and evasion of attention. Indeed, after the protests and outcry in Ferguson, Missouri, a U.S. Department of Justice investigation found the Ferguson police force targeted BIPOC persons for revenue-generating fines, penalties, and forfeitures to raise revenues.[205] There is a perverse incentive to focus potentially predatory practices on people with the least power and voice to halt such practices and bring them to light.[206]

The import of privacy penalties against small fry individuals and entities that do not make the headlines must be viewed from this critical lens of the impact of seemingly minor offenses and fines. Penalties against individuals and small businesses are not the multimillion-dollar major fines against giants like Twitter or Google that garner headlines and scrutiny. As summarized in Tables 9–10 below, the fines against individuals and small businesses tend to be in the hundreds or thousands. Yet such fines in the hundreds or thousands matter more for exacerbating inequality and imposing unbearable burdens than the millions against a major corporate giant because they pose the greatest harm for people least situated to bear it.

Table 9. Fine Amounts in Cases against Individuals

Fine Range	Number of Cases	Proportion of Cases[207]
150-300 Euros	6	17.65%
500-600 Euros	4	11.76%
900-1,000 Euros	2	5.88%
1,500-2,500 Euros	12	35.29%
3,000-5,000 Euros	7	20.59%
9,000-10,000 Euros	3	8.82%

have complained that the combination of vague and minimal substantive definitions of traffic violations and the broad power to *Terry*-stop drivers and frisk — or even fully search occupants — has enabled police to engage in egregious racial discrimination without a trace of any official documentation of prejudicial intent.").

[204] Livingston, *supra* note 203, at 610-11.

[205] U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT 9, 62-63 (2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf [https://perma.cc/9SAV-8DR7].

[206] *See* Martin et al., *supra* note 202, at 271-76.

[207] The denominator is the number of cases against individuals, including neighbors, which equals 34.

Table 10. Fine Amounts in Cases against Small Businesses

Fine Range	Number of Cases	Proportion of Cases[208]
0 Euros	2	2.22%
200-600 Euros	5	5.56%
900-1,000 Euros	12	13.33%
1,200-2,500 Euros	26	28.89%
3,000-4,000 Euros	23	25.56%
5,00-6,000 Euros	9	10.00%
7,000-8,000 Euros	3	3.33%
10,000-12,000 Euros	7	7.78%
20,000 Euros	2	2.22%
30,000 Euros	1	1.11%

B. Guidelines to Reduce the Risk of Harm, Improve the Aim of Privacy Penalties

Framing privacy rights with teeth is an important project and a timely issue as the United States and other nations debate how to frame a comprehensive data privacy regime like the EU's GDPR.[209] An important statutory framing and regulatory design issue is how to better frame privacy regimes to capture entities that pose the great potential privacy harms without sweeping up the powerless in the nether regions of the net too. Drawing insights from this study's findings regarding the impact of privacy penalty decisions under the GDPR, this Section proposes three guidelines to reduce the risk of harm to people and improve the aim of privacy regimes.

The first principle draws insights from criminal justice scholarship about the dangers of arbitrary and discriminatory enforcement that arise from amorphous broad penalty language. The second principle concerns safe harbors for small fry individuals and small businesses with the least power to defend. And the third principle is about how regulatory design should prevent privacy harms with guidance and advice — not just have a predominantly quasi-prosecutorial role after harm has happened.

1. The Perils of Amorphous Penalty Language

A fundamental insight in criminal law that needs wider recognition in privacy circles is that the power to punish — and potentially target

[208] The denominator is the number of cases against small businesses, which equals 90.

[209] *See* discussion *supra* notes 49–55 and accompanying text.

disfavored groups or persons for punishment — is amplified by vague amorphous wording of legal obligations.[210] In the criminal enforcement context, courts and scholars have long recognized the perils of broad amorphous language for arbitrary and discriminatory enforcement.[211] Indeed the U.S. Supreme Court has interpreted the Due Process Clause of the U.S. Constitution to prohibit penalty language that is so broad as to give law enforcers potentially arbitrary and discriminatory enforcement power.[212] Due Process void-for-vagueness doctrine recognizes how overly vague language can violate civil rights and civil liberties by effectively granting unconstrained discretion to select targets.[213]

Even if penalty language does not amount to a constitutional violation, amorphous standards that reach broad swathes of commonplace conduct is problematic. Criminal law and procedure cases and critical race theorists have discussed how broad amorphous language can give cover to discrimination and harassment of disfavored groups.[214] The difficulty in discerning smoking-gun evidence of intent and societal reluctance to credit circumstantial proof of discrimination makes adducing proof of harmful targeting for invidious reasons difficult.[215] Rather than demanding quantitative or direct proof, we

---

[210] *See, e.g.*, Chicago v. Morales, 571 U.S. 41, 56-64 (1999) (discussing how vague, overly broad prohibitions backed by punishment encourage arbitrary and discriminatory enforcement and may violate Due Process rights of the accused); Shon Hopwood, *Clarity in Criminal Law*, 54 AM. CRIM. L. REV. 695, 696 (2017) ("The lack of clarity in criminal law has historically been used as a tool of oppression. States have employed vague and ambiguous criminal laws to target disfavored groups: vagrancy laws were used against the poor and homeless; loitering laws targeted African-Americans and Latinos; and masquerading laws were aimed at the gay community."); Livingston, *supra* note 203, at 611-18 (discussing the history of concern over vague and amorphous laws that confer power on law enforcement to engage in arbitrary or discriminatory enforcement and targeting of unpopular persons).

[211] *E.g.*, Kolender v. Lawson, 461 U.S. 352, 357 (1983) (discussing the dangers of broad language in enforcement); John Calvin Jeffries, Jr., *Legality, Vagueness, and the Construction of Penal Statutes*, 71 VA. L. REV. 189, 196-97 (1985) (recognizing the perils of broad language for discriminatory enforcement).

[212] *Morales*, 571 U.S. at 56-64.

[213] *E.g.*, Papachristou v. City of Jacksonville, 405 U.S. 156, 162 (1972) (invalidating vague statute for failing to give fair notice and creating the risk of "arbitrary and erratic arrests and convictions").

[214] *E.g.*, Devon W. Carbado, *From Stopping Black People to Killing Black People: The Fourth Amendment Pathways to Police Violence*, 105 CALIF. L. REV. 125, 151-63 (2017) (explaining the lived experience of harm arising from broad delegation to law enforcers to enforce seemingly minor commonplace conduct).

[215] Michael Selmi, *Was the Disparate Impact Theory A Mistake?*, 53 UCLA L. REV. 701, 768 (2006).

must be attentive to how the structure of law creates the conditions for targeting the vulnerable and under-resourced.[216]

Theory is borne out by one of the noteworthy findings in this study of GDPR penalty decisions. As discussed in Part II.B.1., a statistically significantly larger proportion of penalties against individuals were assessed for violations of GDPR Article 5 (p=0.0043).[217] Article 5 is a sweeping and stirring declaration of rights of data subjects, providing:

> Article 5: Personal data shall be:
>
> > (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
> >
> > (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; . . .
> >
> > (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') . . . ;
>
> . . . .
>
> > (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed . . . [218]

What counts as "adequate, relevant and limited" and "no longer than necessary"? What counts as "fairly" and "a transparent manner"? The words sound grand and compelling, as suited for a declaration of principles.

But this GDPR provision also is backed by a severe penalty, up to a maximum of 20,000,000 euros [approximately U.S. $23.5 million] or

---

[216] *See, e.g.*, Samuel R. Bagenstos, *The Structural Turn and the Limits of Antidiscrimination Law*, 94 CALIF. L. REV. 1, 41-44 (2006) (discussing the need to address structural inequalities and the shortfalls of antidiscrimination law in doing so); Reva B. Siegel, *Foreword: Equality Divided*, 127 HARV. L. REV. 1, 14 (2013) (noting how legal standards might "probe for covert bad purpose and remedy structural discrimination"); Reva B. Siegel, *Race-Conscious but Race-Neutral: The Constitutionality of Disparate Impact in the Roberts Court*, 66 ALA. L. REV. 653, 657-59 (2015) (discussing approaches to addressing structural discrimination); William M. Wiecek, *Structural Racism and the Law in America Today: An Introduction*, 100 KY. L.J. 1, 4, 7 (2011) (discussing the problems with requiring proof of "deliberate malevolence" and the law's neglect of "structural racism").

[217] *See supra* Part II.B.1, Table 6.

[218] GDPR, *supra* note 6, art. 5.

4% of revenues of the prior year, whichever is higher.[219] These were among the provisions the Turkish döner kebab stand workers in Austria were charged with after their attempt to record the police.[220] These malleable standards do not give much notice as to how to comply in advance — but certainly permit post hoc punishment if the ire of authorities is roused.

Framers of penalty provisions can and should do better in specifying the basis for criminal and civil offenses beyond broad statements of principles better suited for a declaration of principles or preamble. Interestingly, other GDPR provisions that are statistically significantly more likely to be the basis of fines against major corporations are more specific. GDPR Article 32 is an excellent example. Recall from Part II.B.1 that Article 32 accounted for a statistically significantly larger proportion of penalties against major corporations compared to either individuals (p=0.0013) or small businesses (p=0.0017).[221]

Article 32 is a more specific penalty provision that fleshes in the details of the more broadly worded duty to implement data security by default and design.[222] Article 32 provides in relevant part:

> 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> 1) the pseudonymisation and encryption of personal data;
>
> 2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> 3) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

[219] *Id.* art. 83(5).

[220] *See* discussion *supra* notes 9–32 and accompanying text.

[221] *See supra* Part II.B.1, Table 8.

[222] *See* GDPR, *supra* note 6, art. 32.

> 4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[223]

In contrast to the amorphous principles in Article 5, Article 32 offers specific examples of measures people and entities can take to avoid running afoul of the provision. Offering specific guidance and examples is a good design mechanism seen in model penal codes by expert organizations such as the American Law Institute.

The use of more specific penalty provisions to flesh in how to comply with — or transgress — grand statements of principles and declarations of rights is a better practice. More specific penalty provisions help prevent privacy harms in the first place by giving clearer guidance on how to comply. More specific penalty provisions also reduce the risk of potentially arbitrary and discriminatory enforcement or entrapping the unwitting.

2. Safe Harbors for Small Fry

Though oft-portrayed as the laggard in comprehensive data privacy protections compared to the EU,[224] U.S. privacy proposals also offer some important best practices for the EU to consider incorporating. Specifically, proposed U.S. legislation and the few enacted state regimes tend to focus on entities and persons who pose greater harm and have more resources to address problems and defend.[225] Exemptions or safe harbors for those least well-situated to defend against privacy penalty proceedings is an emerging better practice that has important lessons for the EU's GDPR and its international emulators.

Recall from Part I.B. how CCPA limited targets to large powerful businesses.[226] To be a business regulated by the CCPA, as amended by Proposition 24, the entity must have (1) have more than $25 million dollars in gross annual revenues in the preceding year; (2) annually buys, sells or shares the personal information of 100,000 or more households; or (3) derives half or more of revenues from selling personal information.[227] The second major state data privacy regime to follow the CCPA, Virginia's Consumer Data Privacy Act ("VCDP"), is

[223] *Id.* art. 32.

[224] *See* discussion *supra* notes 39, 79–80 and accompanying text.

[225] *E.g.*, CAL. CIV. CODE § 1798.140(d)(1) (2022) (focusing on entities and persons who pose greater harm); Virginia Consumer Data Protection Act [VCDPA], 2021, ch. 52, 2021 Va. Acts § 59.1-572(A).

[226] *See supra* Part I.B.1.

[227] CIV. § 1798.140(d)(1).

potentially broader, reaching natural persons as well as legal persons such as corporations.[228] The more expansive Virginia approach still includes a better-aimed focus on persons conducting business or targeting consumers in Virginia that (i) "control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data."[229]

Other potentially tough proposed federal legislation also offers examples of a salutary focus on businesses big enough to bear the regulatory and defense burdens. For examples, the Mind Your Own Business Act of 2019, proposed by Senator Ron Wyden, a Democrat from Oregon, is tough yet focused on targets able to bear the toughness.[230] Spurred by data breach controversies and targeting large companies such as Facebook, the legislation has similarly severe financial penalties like the GDPR, but unlike the GDPR is limited to large companies as defined by gross revenues.[231]

U.S. proposals and legislation borrow some GDPR concepts, such as declarations of rights and the use of the terms data "controller" and "processor" as regulated entities.[232] The proposals take what is useful but add a salutary attention to the impact on small businesses and ordinary folks by imposing additional thresholds that focus on persons or entities controlling the data of large numbers of persons or with major revenues. These thresholds operate as a de facto exemption for humbler small businesses and ordinary individuals. In contrast, the GDPR's reach extends from the humblest motorist with no assets, or the

[228] VCDPA § 59.1-577(C).

[229] *Id.* § 59.1-572(A).

[230] Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019).

[231] *Id.*

[232] *See, e.g.*, S.B. 893, 2021 Gen. Assemb., Jan. Sess. (Conn. 2021) (joint favorable substitution) (defining regulated controllers to mean "a natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data"); Minnesota Consumer Data Privacy Act, H.F. 1492, 2021 Leg., 92d Sess. (Minn. 2021) (defining controller as a "natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data"); Utah Consumer Privacy Act, S.B. 200, 2021 Leg., Gen. Sess. (Utah 2021) (defining controller to mean a "person doing business in the state who determines the purposes for which and the means by which personal data is processed"); Washington Privacy Act, S.B. 5062, 67th Leg., Reg. Sess. (Wash. 2021) (defining a controller as a "natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data").

snack stand operator to multi-billion-dollar corporations.[233] The exemptions for small businesses and ordinary persons is the better practice for privacy regime framing and reforms.

3. Regulator as Advisor and Negotiator, Not Just Prosecutor

A third better practice is to give data privacy regulatory bodies an advisory role to assist in compliance rather than a predominantly quasi-prosecutorial role. As originally framed, the first major data privacy regime in the U.S., the CCPA, envisioned an advisory role for the California Attorney General, not just an enforcement role.[234] The idea was to give regulated entities the opportunity to seek to comply with obligations before unleashing sanctions.[235]

In the CCPA's early days in operation in 2020 and 2021, the California Attorney General's Office sent out 30-day notice-to-comply letters rather than launching splashy penalty actions under the CCPA.[236] While the Attorney General's Office has pursued and settled privacy law enforcement actions under other laws, such as the state Confidentiality of Medical Information Act, the Business and Professions Code, and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[237] the Attorney General's starting strategy with CCPA enforcement was confidential warning letters to secure compliance rather than bringing formal penalty proceedings.[238]

Before much of a track record could be established for the CCPA enforcement approach, regulatory design soon shifted. Proposition 24, the California Privacy Rights Act ("CPRA"), removed the advisory role

[233] GDPR, *supra* note 6, art. 4(7)-(8); *see Data Controllers and Processors*, *supra* note 98. See also tales from the shadow privacy penalty jurisprudence of small targets, *supra* Part II.B.2 and text accompanying notes 9–32.

[234] CAL. CIV. CODE § 1798.155(b) (2022).

[235] *Id.* § 1798.155(a).

[236] Press Release, Xavier Becerra, Att'y Gen. of Cal. (Mar. 15, 2021), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data [https://perma.cc/3R42-VFH2].

[237] For a list of privacy enforcement actions brought by the California Attorney General's Office, see *Privacy Enforcement Actions*, CAL. DEP'T OF JUST.: OFF. OF THE ATT'Y GEN., https://oag.ca.gov/privacy/privacy-enforcement-actions (last visited July 20, 2022) [https://perma.cc/7AUF-TMSC].

[238] Allison Schiff, *It May Seem All Quiet on the CCPA Front, but Don't Get Complacent: CCPA Enforcement Has Begun*, ADEXCHANGER (Sept. 28, 2020, 12:35 AM.), https://www.adexchanger.com/privacy/it-may-seem-all-quiet-on-the-ccpa-front-but-dont-get-complacent-ccpa-enforcement-has-begun/ [https://perma.cc/KW46-8RG3].

and enforcement role from the Attorney General altogether.[239] Instead, the CPRA establishes a California Privacy Protection Agency, governed by a five-member board.[240] This choice of an independent enforcement agency without an explicit advisory role brings the California privacy regime closer to the GDPR approach, which deploys dedicated Data Protection Authorities in each member State.[241]

Amid outrage and controversies over data breaches and other harms by major companies holding vast volumes of consumer data, it may seem alluring to have a strong independent agency to bring enforcement actions. However, an agency model too slanted toward a primary quasi-prosecutorial role poses problems too. Privacy law can learn from the painful experiences of the criminal law enforcement sector, which is rife with concerns over a predominant focus on prosecution and punishment rather than preventing harms in the first place.[242] Important scholarship in the immigration context also has illuminated how "government lawyers engaged in prosecutorial functions have been largely freed of limits that might be imposed by ethical norms, as they have pursued the agency imperatives of a carceral state."[243]

An independent enforcement agency should also advise on how to comply with privacy obligations and prevent privacy harms before injuries arise, resulting in the need for enforcement actions. Administrative law has well-developed principles for separating personnel offering advice from assuming investigative, prosecuting, or advocating roles.[244] Some of the major administrative agencies today

---

239 Proposition 24, § 1798.155.

240 *Id.* § 24.1.

241 For a discussion of Data Protection Authorities, see, for example, Daigle & Khan, *supra* note 114 (explaining GDPR enforcement structure).

242 *E.g.*, Hadar Aviram, *Legally Blind: Hyperadversarialism,* Brady *Violations, and the Prosecutorial Organizational Culture*, 87 ST. JOHN'S L. REV. 1, 34-35 (2013) (explaining how prosecutors have a culture of only focusing on winning); Susan Bandes, *Loyalty to One's Convictions: The Prosecutor and Tunnel Vision*, 49 HOW. L.J. 475 (2006) (explaining that prosecutors have tunnel vision to achieve convictions rather than prevent harms); Alafair Burke, *Neutralizing Cognitive Bias: An Invitation to Prosecutors*, 2 N.Y.U. J.L. & LIBERTY 512 (2007) (explaining how prosecutor's main focus is punishing); Keith A. Findley & Michael S. Scott, *The Multiple Dimensions of Tunnel Vision in Criminal Cases*, 2006 WIS. L. REV. 291, 333 (explaining how prosecutors have tunnel vision to achieve convictions).

243 Stephen Lee & Sameer M. Ashar, *DACA, Government Lawyers, and the Public Interest*, 87 FORDHAM L. REV. 1879, 1909 (2019).

244 *See, e.g.*, 5 U.S.C. § 554(d)(2) (2018) ("An employee or agent engaged in the performance of investigative or prosecuting functions for an agency in a case may not, in that or a factually related case, participate or advise in the decision, recommended decision, or agency review . . . except as witness or counsel in public proceedings.");

such as the Internal Revenue Service ("IRS"), the U.S. Department of Labor, and the U.S. Equal Employment Opportunity Commission ("EEOC") offer opinion letters to prevent misconduct.[245] Placing government lawyers in an advisory role can expand an agency from prosecution tunnel vision that neglects other important principles of harm prevention and equity.[246]

CONCLUSION

Aggressive privacy penalty regimes are oft-depicted as a way to check powerful highly capitalized business targets such as Twitter, Google, and Facebook.[247] Missing and important in the debate over framing comprehensive privacy laws is the impact of expanding penalties on humbler targets who may lack the resources to defend against harassment or dislike of disfavored groups. This Article fills the gap, drawing on the experience of the world's most aggressive comprehensive privacy penalty regime and insights from criminal justice literature on discretion and the risk of discrimination and harassment in the enforcement of punitive regimes.

Penalty proceedings launched under the European Union's GDPR offers important cautionary tales for the United States. Beyond the headlines breathlessly highlighting multimillion dollar fines against big businesses, there is a shadow GDPR jurisprudence of the disgruntled and petty, pursuing penalty proceedings against small-fry targets. This ostensible jurisprudence of the minor and easily overlooked offers

REVISED MODEL STATE ADMIN. PROC. ACT, art. 6, § 601 cmt. (NAT'L CONF. OF COMM'RS ON UNIF. STATE L. 2010), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=3ab796d4-9636-d856-48e5-b638021eb54d [https://perma.cc/2AAR-JHQC] (explaining that providing for "a separate hearing agency" ensures "impartiality and fairness in contested cases by separating the adjudication function from the prosecution and investigative functions").

[245] *Cf.* David B. Spence, *The Shadow of the Rational Polluter: Rethinking the Role of Rational Actor Models in Environmental Law*, 89 CALIF. L. REV. 917, 990 (2001) (arguing for more frequent use of opinion letters in other agency contexts, such as the Environmental Protection Agency ("EPA")).

[246] *Cf.* Lee & Ashar, *supra* note 243, at 1909 (discussing how government lawyers acting in advisory roles incorporated notions of public interest and equity-based rationales into their work and in advising their principals).

[247] *See, e.g.*, Chris O'Brien, *EU Report Finds GDPR Enforcement Inadequate in Its First 2 Years*, VENTUREBEAT (June 24, 2020, 7:45 AM), https://venturebeat.com/2020/06/24/eu-report-finds-gdpr-enforcement-inadequate-in-its-first-2-years/ [https://perma.cc/H76Z-EGZ6] (depicting the General Data Protection Regulation as a "big step toward limiting the power of major digital platforms such as Google, Facebook, and Twitter").

valuable insights about the risk of harassment and targeting harms despite the relatively small monetary sanctions incurred.

The Article bridges the disconnect between privacy scholarship and insights from the vast literature on criminalization and punishment about why seemingly minor penalties against small-time targets matter the most for aggravating inequalities and the burdens of penalty regimes. To protect the vulnerable from the harms of expanding privacy penalties, the Article proposes three principles. First, privacy laws should avoid the temptation to frame broad amorphously defined rights backed by sanctions, which can be cover for vast discretion to selectively target — or harass. Second, privacy penalty regimes should offer exemptions or safe harbors for small fry lacking the resources to defend in penalty proceedings. Third, privacy laws should frame an enforcement agency with explicit duties to advise and educate, rather than primarily serve in a quasi-prosecutorial capacity.

APPENDIX A: TABLES

For ease of reference, tables used in the text are set forth in this Appendix.

Table 1. Privacy Penalty Decisions from 20 European Member States

Austria	Estonia	Ireland	Portugal
Belgium	Finland	Isle of Man	Romania
Croatia	France	Italy	Slovakia
Czech Republic	Germany	Luxembourg	Spain
Denmark	Iceland	Poland	United Kingdom

Table 2. Who Are the Defendants in Privacy Penalty Decisions?

Defendant Type	Number of Cases[248]	Proportion of Sample
Neighbor of Complainant	16	2.76%
Individual (not neighbor)	18	3.1%
Government	51	8.78%
Small Business	90	15.52%
Medium-Large Business	127	21.89%

[248] The number of cases for which we were able to code the defendant type was 580 in total, rather than 571, because more data was available on the defendant than other variable categories, such as complainant.

Major High Cap Business	172	29.66%
Nongovernmental Organizations	5	0.86%
Health Sector (e.g., physician, clinic, pharmacy med. ass'n)	35	6.03%
Housing Association	9	1.55%
Law Enforcement Officer	4	0.69%
Politician/Political Candidate/Political Party	11	1.90%
Schools/Education	16	2.76%
Website/Media	10	1.72
Union	1	0.17

Table 3. Complaining Parties in Cases Against Individuals

Complainant against Individual	Number of Cases	Proportion of Cases[249]
Neighbor	12	35.29%
Individual	7	20.59%
Police or Inspector	3	8.82%
Group of Businesses	2	5.88%
Customer	1	2.94%
Municipality	1	2.94%
Residential/Homeowner's Ass'n	1	2.94%
Residents of Property	1	2.94%
Unknown	2	5.88%

Table 4. Complaining Parties in Cases Against Small Businesses

Complainant against Individual	Number of Cases	Proportion of Cases[250]
Individual	34	37.67%
Customer	16	17.78%
Police or Inspector	13	14.44%
Municipality or Gov't Agency	7	7.77%
Employee	5	5.56%
Neighbor	4	4.44%
Unknown	3	3.33%
Self-Reported Violation	2	2.22%

[249] The denominator is the number of cases against individuals, including neighbors, which equals 34.

[250] The denominator is the number of cases against small businesses, which equals 90.

Residential/Homeowner's Ass'n	2	2.22%
NGO	1	1.11%
Other Business(es)	2	2.22%
Pedestrians	1	1.11%

Table 5. Most Common GDPR Articles Underlying Penalties by Defendant Type[251]

Order of Impact	Individual	Small Business	Major Corporation
1st Prevalent Basis	Art. 5 (70.6%)	Art. 5 (52.2%)	Art. 6 (47.1%)
2d Prevalent Basis	Art. 6 (61.8%)	Art. 13 (38.9%)	Art. 5 (45.9%)
3d Prevalent Basis	Art. 13 (17.6%)	Art. 6 (35.6%)	Art. 32 (26.7%)
4th Prevalent Basis	Art. 14 (8.8%)	Art. 12 (13.3%)	Art. 13 (10.5%)
5th Prevalent Basis	Art. 7 (5.9%)	Art. 32 (11.1%)	Art. 12 (9.9%)

Table 6. Heightened Risk of an Individual Defendant, Compared to a Major Corporation, Incurring Penalties, by GDPR Article, P-Values (Significance Test for Difference in Proportions)

GDPR Article	Individ. % (tot. N=34)	Major Corp % (tot. N =172)	P-Value
Art. 5	70.6%	45.9%	0.0043*
Art. 6	61.8%	47.1%	0.046*
Art. 13	17.6%	10.5%	0.12

[251] Because multiple GDPR articles can be the basis of imposing a penalty, the proportions exceed 100%.

Table 7. Heightened Risk of a Small Business Defendant, Compared to a Major Corporation, Incurring Penalties, by GDPR Article, P-Values (Significance Test for Difference in Proportions)

GDPR Article	Sm. Bus. % (tot. N=90)	Major Corp % (tot. N=172)	P-Value
Art. 5	52.2%	45.9%	0.17
Art. 12	13.3%	9.9%	0.20
Art 13	38.9%	10.5%	0.00*
Art. 14	8.9%	3.5%	0.03*

Table 8. Heightened Risk of a Major Corporation Defendant, Compared to Individual Defendant and Small Business Incurring Penalties, by GDPR Article, P-Values (Significance Test for Difference in Proportions)

GDPR Article	Major Corp % > Small Bus. % P-Value	Major Corp % > Individual % P-Value
Art. 6	0.053*	0.95
Art. 7	0.052*	0.41
Art. 12	0.095	0.80
Art. 15	0.15	0.065
Art. 25	0.026*	0.22
Art. 32	0.0017*	0.0013*

Table 9. Fine Amounts in Cases against Individuals

Fine Range	Number of Cases	Proportion of Cases[252]
150-300 Euros	6	17.65%
500-600 Euros	4	11.76%
900-1,000 Euros	2	5.88%
1,500-2,500 Euros	12	35.29%
3,000-5,000 Euros	7	20.59%
9,000-10,000 Euros	3	8.82%

[252] The denominator is the number of cases against individuals, including neighbors, which equals 34.

Table 10. Fine Amounts in Cases against Small Businesses

Fine Range	Number of Cases	Proportion of Cases[253]
0 Euros	2	2.22%
200-600 Euros	5	5.56%
900-1,000 Euros	12	13.33%
1,200-2,500 Euros	26	28.89%
3,000-4,000 Euros	23	25.56%
5,00-6,000 Euros	9	10.00%
7,000-8,000 Euros	3	3.33%
10,000-12,000 Euros	7	7.78%
20,000 Euros	2	2.22%
30,000 Euros	1	1.11%

[253] The denominator is the number of cases against small businesses, which equals 90.