The GDPR: What It Really Does and How the U.S. Can Chart a Better Course

By Roslyn Layton & Julian Mclendon

Note from the Editor:

This article discusses the European Union's new General Data Protection Rule and argues that the regulation would not work well in the United States.

The Federalist Society takes no positions on particular legal and public policy matters. Any expressions of opinion are those of the authors. Whenever we publish an article that advocates for a particular position, as here, we offer links to other perspectives on the issue, including ones opposed to the position taken in the article. We also invite responses from our readers. To join the debate, please email us at info@fedsoc.org.

• Max Read, The E.U.'s New Privacy Laws Might Actually Create a Better Internet, N.Y. Mag. (May 15, 2018), http://nymag.com/intelligencer/2018/05/can-gdpr-create-a-better-internet.html.

• Trevor Butterworth, *Europe's tough new digital privacy law should be a model for US policymakers*, Vox (May 23, 2018), https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge.

• Press Conference by Jan Philipp Albrecht, European Parliament, https://multimedia.europarl.europa.eu/en/albrecht-general-data-protection-regulation_I155149-A_ra.

• Dennis Dayman, *Stop whining, GDPR is actually good for your business*, The Next Web (Mar. 18, 2018), https://thenextweb.com/contributors/2018/03/18/stop-whining-gdpr-actually-good-business/.

• Mike Gillespie, *Why Europe's GDPR privacy regulation is good for business*, Computer Weekly, https://www.computerweekly.com/opinion/Why-Europes-GDPR-privacy-regulation-is-good-for-business.

About the Authors:

Roslyn Layton is a visiting scholar at the American Enterprise Institute, where she focuses on evidence-based policy for information, communications, and digital technology industries. She is also a visiting researcher at Aalborg University Center for Communication, Media, and Information Technologies and a vice president at Strand Consult, both in Denmark. Julian Mclendon is a student at the University of Colorado Law School and a student member of the Federalist Society's Telecommunications & Electronic Media Practice Group.

Just seven hours after the European Union's General Data Protection Regulation (GDPR) came into effect on May 25, 2018, Austrian activist Max Schrems' non-profit None of Your Business (NOYB) lodged four complaints with European data protection authorities (DPAs) against Google and Facebook, claiming that the platforms force users' consent to terms of use and demanding damages of $8.8 billion.[1] Soon after, the French advocacy group La Quadrature du Net (LQDN) filed 19 complaints, gathering support from its "Let's attack GAFAM and their world" campaign with a declared objective to "methodically deconstruct" Google, Apple, Facebook, Amazon, and Microsoft (GAFAM) and their "allies in press and government."[2]

The purpose of the GDPR is to regulate the processing of personal data. The protection of persons in the processing of such data is deemed a fundamental EU right.[3] Specifically, the GDPR is legislation from the European Parliament composed of 173 recitals which cover 45 specific regulations on data processing, 43 conditions of applicability, 35 bureaucratic obligations for EU member states, 17 enumerated rights, eleven administrative clarifications, nine policy assertions, five enumerated penalties, and two technological allowances. The legislation applies to topics including Rights of Rectification and Erasure, Restriction of Processing, Objection to Direct Marketing, and requirements for businesses to perform risk assessments, hire data protection officers, and conduct international data transfers.

The European Commission's GDPR website claims that the goals of the regulation are to give users more control of their data and to make business "benefit from a level playing field."[4] But the statute itself suggests another set of stakeholders: litigants, non-profit organizations, data protection professionals, and data regulatory authorities. Non-profit organizations are empowered with new rights to organize class actions,[5] lodge complaints,[6] and receive compensation[7] from fines levied on firms' annual revenue, as high as four percent of annual revenue.[8] The 29 DPAs across the 28 member nations are charged with 35 new responsibilities to regulate data processing. While GDPR complaints against

1 *GDPR: Noyb.Eu Filed Four Complaints Over "Forced Consent" against Google, Instagram, Whatsapp and Facebook*, noyb (May 2018), https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.

2 *Attaquons les GAFAM et leur monde*, LQDN (April 17, 2018), https://www.laquadrature.net/fr/campagne_gafam.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance), Pub. L. No. 32016R0679, 119 OJ L, Recital 1, Article 1 (2016), http://data.europa.eu/eli/reg/2016/679/oj/eng (hereinafter GDPR).

4 2018 Reform of EU Data Protection Rules, European Commission, 2018, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

5 GDPR, Recital 142, Article 80.

6 GDPR, Recital 141, Article 77.

7 GDPR, Recital 143, Articles 78-79, 82.

8 GDPR, Recital 143, Article 83.

leading Silicon Valley firms are noted in the press, thousands of online entities, both in the EU and abroad, have proactively shuttered their European operations for fear of getting caught in the regulatory crosshairs. Some European DPAs report that complaints have at least doubled from last year.[9] Government entities find their previously unassailable social service projects now under scrutiny by users.[10] In the U.S., the popular press has lauded the GDPR,[11] and Senators Edward Markey, Dick Durbin, Richard Blumenthal, and Bernie Sanders have called on U.S. companies to voluntarily adopt its provisions;[12] some even want to require some of the provisions.[13] But a closer look at the GDPR suggests that many people misunderstand the policy, and that it creates serious and negative unintended consequences. This paper reviews those consequences considering U.S. laws and norms, urges caution about adopting GDPR-style measures, and highlights the need for careful attention in crafting any new data protection rules.

I. What Americans Need to Know About the GDPR

A. The GDPR Is About Data Protection, Not Privacy

A popular misconception about the GDPR is that it protects privacy; in fact, it is about data protection or, more correctly, data governance.[14] The word "privacy" does not even appear in the final text of the GDPR, except in a footnote.[15] Data privacy is about the use of data by people who are allowed to have it. Data protection, on the other hand, refers to technical systems that keep data out of the hands of people who should not have it. By its very name, the GDPR regulates the processing of personal data, not privacy.

Privacy is a complex notion having to do with being apart from others, being concealed or secluded, being free from intrusion, being let alone, and being free from publicity, scrutiny, surveillance, and unauthorized disclosure of one's personal information.[16] Data privacy is the application of these principles to information technology. The International Association of Privacy Professionals (IAPP) Glossary notes that data or information privacy is the "claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[17] Data protection, on the other hand, is the safeguarding of information from corruption, compromise, or loss. IPSwitch summarizes the difference: "data protection is essentially a technical issue, whereas data privacy is a legal one."[18] It is important to make this distinction because the terms are often used interchangeably in popular discourse but do not, in fact, mean the same thing.

Yet some assert that the GDPR is somehow a morally superior regime, conflating the high-minded value of privacy with a secular set of technical requirements on data protection.[19] The Data Protection Supervisor, the new EU super-regulator for data protection, bills itself as the "global gold standard," even though the components of the regulation that created it are relatively new and still being tested in both the marketplace and the courts.[20] The GDPR itself declares in Recital 4, "The processing of personal data should be designed to serve mankind."[21] Despite EU assertions to the contrary, there are many technical forms of data protection; each has its own features, but there is no one regime which is objectively and empirically "best."

Many Americans are persuaded by these lofty descriptions of the GDPR—contrasting them with what they see as a morally inferior laissez faire approach at home—both because they confuse data privacy and protection and because they are not familiar with America's own substantive personal informational privacy protections developed since the founding. Journalists and commentators glibly refer to the U.S. as the "wild west," as if there are no laws or regulation on data privacy and data protection.[22] In

9 John Choudhari, *Cataloging GDPR Complaints since May 25*, IAPP, June 25, 2018, https://iapp.org/news/a/cataloguing-gdpr-complaints-since-may-25/; Matthew Schwartz, *GDPR Effect: Data Protection Complaints Spike*, Bank Info Security, August 29, 2018, https://www.bankinfosecurity.com/gdpr-effect-data-protection-complaints-spike-a-11436.

10 Bronwyn Howell, *Data Privacy Debacle Down Under: Is Australia's My Health Record Doomed?*, AEI, August 6, 2018, http://www.aei.org/publication/data-privacy-debacle-down-under-is-australias-my-health-record-doomed/.

11 *See, e.g.*, Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. Times, June 9, 2018, https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html; Trevor Butterworth, *Europe's Tough New Digital Privacy Law Should Be a Model for US Policymakers*, Vox, May 23, 2018, https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge.

12 *Senator Markey Introduces Resolution to Apply European Privacy Protections to Americans*, Senator Ed Markey, May 24, 2018, https://www.markey.senate.gov/news/press-releases/senator-markey-introduces-resolution-to-apply-european-privacy-protections-to-americans.

13 *As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights*, Senator Ed Markey, April 10, 2018, https://www.markey.senate.gov/news/press-releases/as-facebook-ceo-zuckerberg-testifies-to-congress-senators-markey-and-blumenthal-introduce-privacy-bill-of-rights.

14 *What Is the GDPR?*, Evidon (last visited Aug. 25, 2017), https://www.evidon.com/education-portal/videos/what-is-the-gdpr/.

15 GDPR, n.18 (referring to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector).

16 Privacy, dictionary.com, https://www.dictionary.com/browse/privacy (accessed September 27, 2018).

17 Information Privacy, Glossary, IAPP https://iapp.org/resources/glossary/#information-privacy (accessed September 27, 2018).

18 David Robinson, *Data Privacy vs. Data Protection*, IPSwitch (Jan. 29, 2018), https://blog.ipswitch.com/data-privacy-vs-data-protection.

19 *See, e.g.*, Ashwin Krishnan, *GDPR Is Not Just a Regulatory Framework. It's Also a Moral and Existential Blueprint*, CSO Online, February 23, 2018, https://www.csoonline.com/article/3257695/privacy/gdpr-is-not-just-a-regulatory-framework-it-s-also-a-moral-and-existential-blueprint.html.

20 *The History of the General Data Protection Regulation*, European Data Protection Supervisor, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (accessed September 27, 2018).

21 GDPR, Recital 4.

22 *See, e.g.*, Joe Nocera, *The Wild West of Privacy*, N.Y. Times, Feb. 24, 2014, https://www.nytimes.com/2014/02/25/opinion/nocera-the-wild-west-of-privacy.html.

fact there are literally hundreds of laws relating to privacy and data protection in the U.S.—including common law torts, criminal laws, evidentiary privileges, federal statues, and state laws.[23] The EU's laws are relatively new, officially dating from this century, and still lack the runway of judicial scrutiny and case law that characterizes U.S. law.

The main federal privacy law in the U.S. is 15 U.S.C. § 45, which charges the Federal Trade Commission (FTC) with preventing "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[24] In matters of privacy, the FTC's role is to enforce privacy promises made in the marketplace by suing companies that make such promises and then break them. Whereas the GDPR assumes that any data collection is suspect and therefore regulates it ex ante, the FTC focuses its enforcement efforts on sensitive information that should be protected against unwarranted disclosure. This helps avoid imposing costly and draconian compliance mandates on entities which are not a priori threats to personal privacy, such as personal blogs, small businesses, and informational websites. The FTC's approach seeks to allocate scarce regulatory resources to prevent the greatest threats to online privacy. To be sure, if a small entity behaves in an unfair or deceptive way, it can be prosecuted, but the FTC does not assume that every entity wants to harm online users. Several additional laws form the foundation on which the FTC carries out its charge: the Privacy Act of 1974,[25] the Gramm-Leach-Bliley Act,[26] the Fair Credit Reporting Act,[27] and the Children's Online Privacy Protection Act.[28]

The American notion of privacy is predicated in large part on freedom from government intrusion and as a counterweight to the growth of the administrative state.[29] The Bill of Rights' Third, Fourth, and Fifth Amendments responded to the egregious British abuses of personal privacy, including the quartering of soldiers in private homes, the search and seizure of colonists' property, and forcing colonists to divulge information. Some of the first laws in the new republic were enacted to protect privacy in the use of mail. These were followed by laws constraining the government's use of the census[30] and its ability to compel information in court.[31] The 1966 Freedom of Information Act (FOIA) ensured that people could access records held by the government. Given this history of pushing back against government intrusion, it is reasonable to be skeptical that increasing government power is now the key to privacy in the U.S.

23 *See* Daniel J. Solove, *A Brief History of Information Privacy Law* in Proskauer on Privacy (2006).

24 15 U.S.C. § 45 (2012).

25 5 U.S.C. § 552a.

26 15 U.S.C. §§ 6801-6809.

27 15 U.S.C. § 1681 et seq.

28 15 U.S.C. §§ 6501-6506.

29 *See* Solove, *supra* note 23, at 1-5, 1-6.

30 *See id.* at 7 (The Census and Government Records).

31 *See, e.g.*, Boyd v. United States, 116 U.S. 616 (1886).

B. The GDPR's Primary Goals Are Geopolitical

European leaders have expressed a positive view of the GDPR, often in terms that go beyond what it actually seeks to accomplish. But to analyze a policy like the GDPR, we must set aside the political pronouncements surrounding it and evaluate its real-world effects. Besides its effect on data processing, the GDPR can be investigated for its ability to achieve important European geopolitical goals, including (1) solidifying legitimacy for Brussels during a period of deep skepticism among voters, and (2) strengthening European political power against the real or perceived threat of American digital prowess.

The GDPR can be examined in the context of a heightened pro v. anti-EU debate, fueled by a rise in Euroscepticism and nationalist parties which charge that European integration weakens national sovereignty.[32] Smarting from a disgruntled electorate and the Brexit bombshell,[33] pro-European coalitions support pan-European regulation such as the GDPR to legitimize the EU project. It should be noted that Eurosceptic political actors are not necessarily opposed to data protection regulation; they merely prefer the primacy of national institutions over European ones, largely because of concerns that EU institutions and policies are subverting democracy.

In the case of the GDPR, there was no groundswell of public support calling for the enactment of greater data protection regulation. The GDPR was enacted during a period of voter "disengagement."[34] Participation in European Parliament elections has dwindled from 62 percent in 1979 to just 42 percent in 2014.[35] This environment of voter disengagement is conducive for the collective action of organized special interests to defeat a diffuse, disgruntled, and unorganized majority.[36] Relatively few Europeans are even aware of the GDPR. For example, a United Kingdom survey found that only 34 percent of respondents recognized the law, and even fewer knew what it covered.[37] Essentially, a relatively small group of GDPR advocates successfully implemented massive pan-European regulation without significant voter buy-in. Public

32 Euroscepticism as a Transnational and Pan-European Phenomenon 133 (John FitzGibbon, Benjamin Leruth, Nick Startin eds., 2016).

33 *Id.* Euroscepticism is the notion that the European integration undermines the national sovereignty of its members states, that the EU lacks democratic legitimacy, is too bureaucratic, encourages high migration, and the perception that it is a neoliberal organization benefitting the elite at the expense of the working class—remains an obstacle to the goals some have for the European continent. *See also* Dalibor Rohac, *Europe's Pressure Points*, AEI, January 17, 2017, http://www.aei.org/feature/europes-pressure-points/.

34 John Curtice, *How Deeply Does Britain's Euroscepticism Run?*, NatCen (2016), http://www.bsa.natcen.ac.uk/media/39024/euroscepticism.pdf.

35 Turnout 2014 - European Parliament, European Parliament, http://www.europarl.europa.eu/elections2014-results/en/turnout.html (accessed July 27, 2018).

36 *See generally* Mancur Olson, The Logic of Collective Action (1971).

37 Kirsty Cooke, *Data Shows Awareness of GDPR Is Low amongst Consumers*, Kantar, March 27, 2018, https://uk.kantar.com/public-opinion/policy/2018/data-shows-awareness-of-gdpr-is-low-amongst-consumers/.

opinion as measured by the Eurobarometer poll[38] suggests that most people would prefer a more nuanced approach to data protection over the sledgehammer of the GDPR, and that most would rather strengthen regulation at the nation-state level than at the EU.[39] Nevertheless, the GDPR automatically supersedes national law, and only four of the 28 member states (Austria, Germany, Slovakia, and Sweden) have formally updated their local laws to align with the GDPR. If one country rules in a GDPR case in its own court, it can be overruled by a majority of EU nations.

A related geopolitical issue is the sense among Europeans that they have fallen behind U.S. and China in the internet economy.[40] The EU continues to watch the U.S., and increasingly China, capture the world market for internet innovation and revenue. A European company has not appeared on Mary Meeker's list of top internet companies since 2013.[41] So rather than compete in the global marketplace by making better internet products and services, the EU is seeking to compete geopolitically by creating tougher regulatory standards. The EU made a similar gambit for dominance in mobile standards by forcing the adoption of 3G/GSM, hoping to trounce America's competing code division multiple access (CDMA) platform. For a time, the strategy gave the European mobile industry a leg up.[42] But the U.S.—rather than following the Europeans down the regulatory road—jumped ahead to 4G and became the world leader in 4G/LTE mobile.[43]

C. Regulatory Approaches to Privacy Are Mediated by Cultural Norms and Vary Considerably Across Countries

The difference between U.S. and EU approaches to data protection and data privacy is underscored by demonstrated cultural differences and exigencies. For example, the Nordic countries, with their traditions of transparency and egalitarianism, have long maintained digital public databases of individual citizens' salary[44] and income tax records.[45] This disclosure of financial information contradicts America's traditions and strict laws on the protection of financial information. However, the U.S. makes criminal records available to the public at the federal, state, and county level,[46] whereas such information is not available in the same way across the EU. Both the U.S. and European countries have had telephone books and White and Yellow Pages for decades, but had they been invented in today's precautionary environment, it is doubtful that such valuable tools would be allowed. These differences and similarities demonstrate a key debate in the field of internet policy: the individual's right to privacy versus the public's right to know.[47]

Many academic studies have documented cultural differences in opinions about privacy and their implications for policy.[48] The existence of these cultural differences suggests that exporting the GDPR's one-size-fits-all approach to other nations with digital platforms may not be optimal for realizing what those other countries want in terms of data protection.[49] Consider Professor Geert Hofstede's study of cultural dimensions of citizens of the U.S. and Germany and the potential implications for data protection.[50] Americans score highly on individualism, geographical mobility, interacting with people they don't know, and seeking information from others. This could explain why Americans are more comfortable with sharing information, as they anticipate benefits from doing so. Germans, in contrast, score highly on uncertainty avoidance and may be more cautious with information sharing. That the leading architects of the GDPR are German and Austrian could reflect a cultural desire to lessen or avoid what they see as uncertainty in the data-driven economy, whereas Americans may believe the benefits of sharing information in society today outweigh the risks of imperfect information about the future. These conclusions regarding the different preferences for caution when disclosing data have been noted by

38 European Commission, Public Opinion, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm.

39 Roslyn Layton, *How the GDPR Compares to Best Practices for Privacy, Accountability and Trust*, SSRN Scholarly Paper, March 31, 2017, https://papers.ssrn.com/abstract=2944358.

40 Craig Willy, *Europe's tech race - trying to keep pace with US and China*, EU Observer, June 22, 2018, https://euobserver.com/opinion/142056.

41 *Internet Trends Report 2018*, Kleiner Perkins, May 30, 2018, https://www.kleinerperkins.com/perspectives/internet-trends-report-2018.

42 Jacques Pelkmans, *The GSM standard: explaining a success story*, 8 J. of European Pub. Pol. 432 (2001).

43 *North America Region a World Leader in 4G and Smartphone Adoption, According to New GSMA Report*, GSMA, September 12, 2017, https://www.gsma.com/newsroom/press-release/north-america-region-world-leader-4g-smartphone/.

44 *Privacy, What Privacy? Many Nordic Tax Records Are a Phone Call Away*, Reuters, April 12, 2016, https://www.reuters.com/article/us-panama-tax-nordics-idUSKCN0X91QE.

45 *Tax Statistics for Personal Tax Payers*, ssb.no, April 18, 2018, https://www.ssb.no/en/inntekt-og-forbruk/statistikker/selvangivelse/aar-forelopige/2018-04-18; Patrick Collinson, *Norway, the Country Where You Can See Everyone's Tax Returns*, The Guardian, April 11, 2016, https://www.theguardian.com/money/blog/2016/apr/11/when-it-comes-to-tax-transparency-norway-leads-the-field; *Income and Tax Statistics in Sweden*, Statistiska Centralbyrån, October 1, 2018, http://www.scb.se/en/finding-statistics/statistics-by-subject-area/household-finances/income-and-income-distribution/income-and-tax-statistics/.

46 James Jacobs and Tamara Crepet, *The Expanding Scope, Use, and Availability of Criminal Records*, 11 N.Y.U. J. L. & Pub. Pol'y 177 (2012), http://www.nyujlpp.org/wp-content/uploads/2012/10/Jacobs-Crepet-The-Expanding-Scope-Use-and-Availability-of-Criminal-Records.pdf.

47 Fred Cate, D. Fields, and James McBain, *The Right to Privacy and the Public's Right to Know: The 'Central Purpose' of the Freedom of Information Act*, 46 Admin. L. Rev. 41 (1994), https://www.repository.law.indiana.edu/facpub/737.

48 Jeremy Hainsworth, *Global Privacy Ethics Subject to Cultural Differences*, BNA, April 13, 2016, https://www.bna.com/global-privacy-ethics-n579820698O7/.

49 Bhaskar Chakravorti, *Why the rest of the world can't free ride on the GDPR*, Harv. Bus. Rev., Apr. 30, 2018, https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules.

50 *Country Comparison*, Hofstede Insights, https://www.hofstede-insights.com/country-comparison/ (accessed September 27, 2018).

Professors Robert Thomson[51] and Steven Bellman.[52] Furthermore, studies of privacy behavior find that it is not monolithic even within cultures. Privacy concerns can diminish with education and experience.[53] A nation's policy choices on data privacy and protection are imbued at least to some extent with the local and culturally relevant preferences.[54]

The conflicting theoretical views regarding data privacy and protection are well summarized in Adam Thierer's *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*.[55] He describes the precautionary principle as the belief that "innovations should be curtailed or disallowed until their developers can prove they will not cause any harm to individuals, groups, specific entities, cultural norms, or various existing laws, norms or traditions," and contrasts it with permissionless innovation, in which "experimentation with new technologies and business models should be generally permitted by default" unless a "compelling" case can be made that an innovation will bring serious harm.[56] The EU is following the precautionary principle by enacting and enforcing the GDPR, while the U.S. subscribes to permissionless innovation by allowing innovation unless and until it has proved harmful. While the EU has deemed certain data practices presumptively harmful, it has not proved the alleged harm.

D. A Decade of GDPR-type Policy Has Not Created Greater Online Trust in the EU

The GDPR could be justified if there were evidence that the many European internet-regulation laws to date have created greater trust in the digital ecosystem, but there is no such evidence. After a decade of GDPR-type regulations—in which Europeans have endured intrusive pop-ups and disclosures on every digital property they visit—Europeans report no greater sense of trust online.[57] As of 2017, only 22 percent of Europeans shop outside their own country (a paltry increase of 10% in a decade), demonstrating that the European Commission's Digital Single Market goals are still elusive.[58] Moreover, only 20 percent of EU companies are highly digitized.[59] These are primarily large firms. Small to medium sized companies invest little to modernize and market to other EU countries.[60] The EU has not yet offered to provide any measure that the GDPR is working to create greater trust.

A poll conducted by the U.S. Census Bureau for the National Telecommunications and Information Administration (NTIA) in 2015 and 2017 gives insight into Americans' sense of online trust.[61] Three-quarters of Americans report concerns about risks associated with online privacy and security, but the proportion of online households reporting privacy or security concerns "fell from 84 percent to 73 percent during this period. Similarly, the proportion of online households that said privacy concerns stopped them from doing certain online activities dropped from 45 percent to 33 percent."[62] The survey also notes that recent events such as the Office of Personnel Management cybersecurity breach had an impact on responders' perception. The survey is somewhat confusing because it conflates security concerns—such as identify theft, bank fraud, and the loss of personal information—with privacy concerns. A closer look at the data reveals that Americans overall are more concerned about data security than data privacy.[63]

The Pew Research Center surveyed expectations of online trust going forward by canvassing some 1,200 technologists, scholars, practitioners, strategic thinkers, and other leaders. They found that "48% chose the option that trust will be strengthened; 28% of these particular respondents believe that trust will stay

51 Robert Thomson, Masaki Yuki, and Naoya Ito *A socio-ecological approach to national differences in online privacy concern: The role of relational mobility and trust*, 51 Computers in Human Behavior 285 (2015).

52 Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, 20:5 The Info. Soc'y 313 (2004).

53 Michael M. Harris, Greet Van Hoye, and Filip Lievens *Privacy and Attitudes Towards Internet-Based Selection Systems: A Cross-Cultural Comparison*, 11 Int'l J. Selection & Assessment 230 (2003); Donna L. Hoffman, Thomas P. Novak, and Marcos A. Peralta, *Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web*, 15 The Info. Soc'y 129 (1999); Philip J. Reed, Emma S. Spiro, and Carter T. Butts, *Thumbs up for privacy?: Differences in online self-disclosure behavior across national cultures*, 59 Social Sci. Research 155 (2016).

54 Sophie Cockcroft, *Culture, Law and Information Privacy*, Proceedings of European and Mediterranean Conference on Information Systems, Polytechnic University of Valencia, Spain, June 24-26, 2007, http://emcis.eu/Emcis_archive/EMCIS/EMCIS2007/emcis07cd/EMCIS07-PDFs/642.pdf.

55 Adam Theirer, Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom, *available at* https://www.mercatus.org/publication/permissionless-innovation-continuing-case-comprehensive-technological-freedom.

56 *Id.*

57 Daniel Castro and Alan McQuinn, *The Economic Cost of the European Union's Cookie Notification Policy*, ITIF, Nov. 6, 2014, https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy.

58 European Commission, *Use of Internet Services*, 2018, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/3_desi_report_use_of_internet_services_18E82700-A071-AF2B-16420BCE813AF9F0_52241.pdf. *See id*. at 4 ("Growth in the use of online services is generally slow.").

59 European Commission, *Integration of Digital Technology*, 2018, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/4_desi_report_integration_of_digital_technology_B61BEB6B-F21D-9DD7-72F1FAA836E36515_52243.pdf.

60 European Commission, *Better Access for Consumers and Business to Online Goods*, 2015, https://ec.europa.eu/digital-single-market/en/better-access-consumers-and-business-online-goods.

61 Rafi Goldberg, *Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds*, National Telecommunications and Information Administration, August 20, 2018, https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds.

62 *Id.*

63 Gus Hurwitz, *For Americans, Cybersecurity Outweighs Privacy*, AEI, August 10, 2016, http://www.aei.org/publication/americans-cybersecurity-outweighs-privacy/.

the same; and 24% predicted that trust will be diminished."[64] Trust among Americans can also be inferred from user response to Facebook in the wake of the Cambridge Analytica revelation.[65] Daily active users (DAU) on Facebook in the U.S. and Canada have held steady for the past year despite negative press coverage.[66] It appears that millions of U.S. Facebook users either do not know or are not concerned about the Cambridge Analytica scandal. Overall, the platform has gained 5 million DAU since the 2016 election. This is not to say that there are not concerns about the platform. Indeed, a recent poll reports that two-thirds of Americans aged 53–72 want tech companies to be regulated like big banks, even though respondents overall have some doubts about whether governments can successfully regulate such firms.[67] But it does suggest that policymakers need to be careful about generalizing about all Facebook users and adopting policies predicated on an incorrect understanding of its diverse users.

Regulatory advocates would likely describe most Facebook users as suffering from a "privacy paradox" (understanding the value of privacy but failing to practice privacy enhancing behaviors),[68] but the reality may be more complex. Users interpret privacy within a context, and they don't object to sharing information per se, only to sharing that is inappropriate based on the context.[69] Many users get value from Facebook; they like having their family and friends, photo albums, and messaging all in one place. They likely understand that advertising and data collection underpin the platform and make the valuable services possible, just as advertising supported analog television, radio, and print in the past. Naturally, users expect to be treated well, but they do not necessarily expect that platform providers will never make mistakes. Indeed, users could be upset about Cambridge Analytica, but rather than quitting Facebook, they would like to see how Facebook responds to the situation by making improvements to the platform. This may be related to Facebook having a resilient "brand personality" such that users understand that it is an imperfect and evolving platform.[70] Indeed, Facebook experienced an increase in engagement from U.S. users following the Cambridge Analytica revelation, as users went online to change their privacy settings.[71]

However, many U.S. users do quit Facebook. Hill Holliday's survey of Generation Z (those born since 1994) shows that so-called digital natives, who are estimated to comprise 40 percent of U.S. consumers by 2020 and of whom more than 90 percent use social media platforms, found that more than one-half had switched off social media for extended periods and one-third had canceled their social media accounts.[72] Users cited time wasting as the reason for quitting twice as often as a concern about privacy. While service providers don't like the high rates of churn on their platforms,[73] they are indicative of a competitive market in which consumers find it easy to leave and try other platforms with different features.

Additionally, reports suggest that some forms of user engagement are declining.[74] This could be related to Facebook changing its model to emphasize posts from family and friends over news. The most significant market response was the company losing $119 billion following its second quarter financial results, the biggest market value drop for a company on a single day in U.S. history.[75] This amount is roughly 10 times the maximum fine that authorities could levy on the company under the GDPR. Moreover, Facebook's shareholders have demanded leadership changes[76] and have lodged lawsuits against the company.[77] The response demonstrates that users and the marketplace can be effective regulators and is consistent with the literature about

64 Lee Rainie and Janna Anderson, *The Fate of Online Trust in the Next Decade*, Pew Research Center, August 10, 2017, http://www.pewinternet.org/2017/08/10/the-fate-of-online-trust-in-the-next-decade/.

65 Deepa Seetharaman and Katherine Bindley, *Facebook Controversy: What to Know About Cambridge Analytica and Your Data*, Wall St. J., March 23, 2018, https://www.wsj.com/articles/facebook-scandal-what-to-know-about-cambridge-analytica-and-your-data-1521806400.

66 Facebook, *Facebook Q2 2018 Results*, https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Q2-2018-Earnings-Presentation.pdf.

67 HarrisX, *Inaugural Tech Media Telecom Pulse Survey 2018*, April 2018, http://harrisx.com/wp-content/uploads/2018/04/Inaugural-TMT-Pulse-Survey_-20-Apr-Final.pdf.

68 Benjamin Wittes and Jodie Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, Brookings, November 30, 2001, https://www.brookings.edu/research/the-privacy-paradox-the-privacy-benefits-of-privacy-threats/.

69 Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (2009), https://www.sup.org/books/title/?id=8862.

70 Jennifer L Aaker, *Dimensions of brand personality*, 34 J. Marketing Res. 347 (Aug. 1997), http://www.haas.berkeley.edu/groups/finance/Papers/Dimensions%20of%20BP%20JMR%201997.pdf

71 Daniel Turdiman, *Facebook Engagement Surge Post-Cambridge Analytica*, Fast Company, April 24, 2018, https://www.fastcompany.com/40563518/why-facebooks-engagement-surged-after-cambridge-analytica.

72 Hill Holliday, *Meet Gen Z: The Social Generation*, http://thinking.hhcc.com/?utm_campaign=Thought%20Leadership%20%E2%80%94%20Gen%20Z&utm_source=Press%20Release (last visited June 25, 2018).

73 Connie Hwong, *Why Churn Rate Matters: Which Social Media Platforms Are Losing Users?*, Verto Analytics, May 4, 2017, https://www.vertoanalytics.com/chart-week-social-media-networks-churn/.

74 Ryan Erskine, *Facebook Engagement Plunging Over Last 18 Months*, Forbes, August 13, 2018, https://www.forbes.com/sites/ryanerskine/2018/08/13/study-facebook-engagement-sharply-drops-50-over-last-18-months/#69c1de5794e8.

75 Fred Imbert, Gina Francolla, *Facebook's $100 Billion-plus Rout Is the Biggest Loss in Stock Market History*, CNBC, July 26, 2018, https://www.cnbc.com/2018/07/26/facebook-on-pace-for-biggest-one-day-loss-in-value-for-any-company-sin.html.

76 Trillium Asset Management, *Facebook, Inc. — Independent Board Chairman (2019)*, http://www.trilliuminvest.com/shareholder-proposal/facebook-inc-independent-board-chairman-2019/ (accessed August 20, 2018).

77 Owen Bowcott and Alex Hern, *Facebook and Cambridge Analytica Face Class Action Lawsuit*, The Guardian, April 10, 2018, https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit.

corporate response to public relations disasters such as the Tylenol scare and plane crashes: firms take steps to improve safety, frequently without being compelled by government to do so.[78]

II. Legal and Policy Risks of the GDPR

Under the GDPR, data regulators and supervisors become de facto intermediaries between consumers and firms, disrupting and distorting free exchange between the parties.[79] There are significant legal and policy risks that have emerged with the GDPR, including the potential for selective enforcement, the undue empowering of litigants, and the strengthening of the European data protection bureaucracy, which is largely unaccountable to voters.[80]

A. Enforcement Discretion

Selective enforcement or enforcement discretion occurs when authorities choose whether and how to punish an actor which has violated the law. While selective enforcement may sometimes be more efficient, it can also produce bias, corruption, and prejudice. For example, there is evidence of bias in the selective enforcement of human rights laws,[81] as well as in the selective enforcement of industrial regulation in the UK.[82] A recent doctoral thesis in the European University Institute's Department of Law documents the European Commission's policy of selective law enforcement and argues that it is based upon the pillars of confidentiality, bilateralism, flexibility, and autonomy.[83] While it has been pressured to increase its legitimacy by improving enforcement with standards such as transparency, trilateralism, objectivity, and accountability, the Commission has resisted, and its position has been upheld in the European Court of Justice. The thesis explains that selective enforcement is prevalent because the Commission's ability to enforce the law is limited. Indeed, the Commission is reluctant to improve standards and formalize enforcement because doing so would create administrative burdens, which would in turn decrease its efficiency.[84] In an editorial blog post titled *GDPR and the Abusive Potential of Selective Enforcement*, the authors note that "EU bureaucrats wanted to flex their muscles against Facebook—but kicked every single European enterprise in the face with the same regulatory maneuver (the GDPR) . . . . Autocrats love rules that make everyone punishable, but don't worry, they will practice discretion—if they like you."[85] The article notes a number of concerns about the GDPR, including that its creates a heavier compliance burden on small enterprises, which ironically strengthens large companies like Facebook; that it deters innovation by European startups; that enforcement, driven by local authorities, will create a market for "regulation avoidance"; that it requires additional corporate and government bureaucracy; that it gives rise to "data commissars"; that it reduces the free flow of information; and that it commercializes compliance as an industry.

But GDPR architects have touted selective enforcement to reassure stakeholders, as literal interpretation of the GDPR could bring commerce to a halt. Green Party Parliamentarian Jan Philipp Albrecht,[86] the "father of the GDPR," has assured critics that GDPR investigations will not focus on small to medium enterprises, but instead "will concentrate on the bigger ones that pose a threat to many consumers."[87] He noted the firms that "already for quite a time now are under suspicion of not complying with European data protection rules" and "that have been on their screen for years will be the first to be looked at."[88] He indicated that it could be two years before cases are resolved given the process for investigation, adjudication, and appeal. If smaller companies are trying in good faith to comply with the GDPR, it would be disproportionate to sanction them, Albrecht said, noting that DPAs would more likely assist them to become compliant. The UK DPA's Information Commissioner's Office (ICO) noted that it will prioritize 30 named firms in its investigations under the GDPR.[89] Albrecht's comments underscore the uncertainty created by the GDPR.

B. Empowering Litigants

The GDPR also empowers litigants with a series of new rights, including rights to complain, select representatives,

78 Thomas Hazlett, Jamil Jaffer, Megan Stifel, and Matthew Heiman, *What to do about Facebook: On Data Privacy and the Future of Tech Regulation*, Regulatory Transparency Project Teleforum Podcast (June 7, 2018), https://fedsoc.org/events/RTP_FTC-FB-CamAnalytica (comments of economist Thomas Hazlett).

79 Howard Beales et al., *Government Regulation: The Good, the Bad, & the Ugly*, Regulatory Transparency Project White Paper, June 12, 2017, https://regproject.org/paper/government-regulation-the-good-the-bad-the-ugly/.

80 Leonid Bershidsky, *The EU Doesn't Want to Be More Democratic*, Bloomberg, Feb. 9, 2018, https://www.bloomberg.com/view/articles/2018-02-09/the-eu-doesn-t-want-to-be-more-democratic.

81 Martin Binder, *The Selective Enforcement of Human Rights? The International Response to Violent Humanitarian Crises and Gross Violations of Human Rights in the Post-Cold-War Era*, Discussion Paper, Social Science Research Center Berlin, 2007, https://ideas.repec.org/p/zbw/wzbtci/spiv2007307.html.

82 P. Fenn and C. G. Veljanovski, *A Positive Economic Theory of Regulatory Enforcement*, 98 The Econ. J. 1055 (1988), https://doi.org/10.2307/2233719.

83 Karolina Boiret, *Selective Enforcement of EU Law: Explaining Institutional Choice*, European University Institute Law Department Thesis (2016), https://doi.org/10.2870/496944.

84 *Id.*

85 *GDPR and the Abusive Potential of Selective Enforcement*, Meanwhile in Budapest, May 25, 2018, https://meanwhileinbudapest.com/2018/05/25/gdpr-and-the-power-of-selective-enforcement/. The blog site, *Meanwhile in Budapest*, describes itself as "written from the perspective of Hungarian millennials who are not comfortable with the new authoritarianism."

86 Jan Philipp Albrecht, *Auf zu neuen Ufern: Minister für Digitales und Draußen*, Mar. 3, 2018, https://www.janalbrecht.eu/2018/03/auf-zu-neuen-ufern/.

87 Press Conference by Jan Philipp Albrecht, European Parliament, https://multimedia.europarl.europa.eu/en/albrecht-general-data-protection-regulation_I155149-A_ra (last visited June 24, 2018).

88 *Id.*

89 Alex Hern, *Facebook among 30 Organisations in UK Political Data Inquiry*, The Guardian, April 5, 2018, https://www.theguardian.com/technology/2018/apr/05/facebook-mark-zuckerberg-refuses-to-step-down-or-fire-staff-over-mistakes.

and receive judicial remedy and compensation when firms fail to comply with the GDPR. The representatives of users are encouraged to create non-profit organizations to file class actions,[90] lodge complaints,[91] and collect recompense on behalf of users.[92] These non-profits act as informal agents to surface problems and file complaints with regulatory authorities. Importantly, complaints by non-profits under the GDPR need not allege *actual* injury or harm—which would be required for most class actions in U.S. federal court—but only failure to comply with regulation, even if no harm results. While class actions can offer consumers a convenient, effective remedy for harm, they can also be abused by unscrupulous lawyers and by activists seeking to bypass democratic procedures.[93] By legitimizing regulation by class action in the GDPR, the EU creates an incentive for legal abuse. Historically, Europe has largely eschewed "U.S.-style" class actions,[94] noting that they disproportionately reward lawyers and litigation financiers over consumers.[95] But policymakers have engineered the GDPR so that privacy activists can bring cases without overcoming legal barriers of standing and jurisdiction, which are traditional safeguards against the abuse of the legal system for private gain. Other problems include the ambiguity and politicization surrounding representation,[96] the fact that organizations can deem themselves representatives of users without users' consent, and a lack of clarity on whether consumers can opt out of class actions.[97]

Max Schrems, the Austrian activist and GDPR architect, is the face of EU data protection litigation.[98] He founded NOYB, a non-profit in Austria, expressly to sue Silicon Valley companies under the GDPR. The organization's executive board is the Who's Who of GDPR proponents, including Albrecht, Austrian MP Josef Weidenholzer, Former European Commissioner for Fundamental Rights Paul Nemitz, the City of Vienna, the official consumer associations of Austria and Norway, and the American Electronic Privacy Information Center (EPIC).[99] The board also includes Roland-Prozessfinanz, self-described as "the most experienced litigation funder in Europe," which has financed Schrems' lawsuits since 2014 and takes a 20-40% cut of judicial penalties levied in such cases.[100]

Working with Schrems is Andrea Jelinek,[101] the first Chair of the European Data Protection Board (EDPB)—the pan-European data protection regulator established by the GDPR[102]—and the current chief of the Austrian DPA.[103] Jelinek has prioritized NOYB's complaints against Google, Facebook, Instagram, and WhatsApp in official EU investigations and has incorporated NOYB parlance and arguments such as "forced consent" into her media talking points.[104]

Schrems campaigned and litigated against Facebook long before the GDPR came into effect. Following a study abroad program at California's Santa Clara University, he launched a formal complaint against Facebook in Ireland in 2011, alleging that the company kept information he had tried to delete.[105] He claimed that Facebook refused to hand over his "biometric faceprint," saying it was a trade secret. Though Schrems eventually withdrew his complaint, the Irish Data Protection Commission audited Facebook and ordered it to delete some files and disable its facial recognition software.[106] Schrems filed another complaint against Facebook in Irish court in 2013, which ultimately brought down the 15 year old safe harbor agreement between the U.S. and the EU that had facilitated $250 billion of digital trade annually.[107] The following year, he launched a class action against the company in Austria and invited any Facebook user in the world to participate with a promise of "token" damages of €500 per user.[108] Capped at 25,000 Facebook users, the suit is

90 GDPR, Recital 142.

91 GDPR, Recital 141.

92 GDPR, Recital 143.

93 *See generally* Martin H. Redish, Wholesale Justice (2009).

94 Lisa A. Rickard, *Consumers Are the Losers in EU's Collective Action Proposal*, Politico (Aug. 3, 2018), https://www.politico.eu/article/opinion-consumers-are-the-losers-in-eus-collective-action-proposal-european-commission-collective-action/.

95 *See* Redish, *supra* note 93.

96 For example, different types of organizations can be formed to create complaints and class actions provided that they operate in the "public interest" and in the field of data protection rights. *See* GDPR, Chapter 8, Article 80.

97 *See* Rickard, *supra* note 94.

98 Roslyn Layton, *Europe's Protectionist Privacy Advocates*, Wall St. J. (Mar. 9, 2016), https://www.wsj.com/articles/europes-protectionist-privacy-advocates-1457566423.

99 Executive Board, noyb, https://noyb.eu/team.

100 Arndt Eversberg, *Getting the Deal Through*, https://gettingthedealthrough.com/people/150102/arndt-eversberg/ (last visited Oct. 6, 2018).

101 European Commission, *Citizens' Dialogue in Graz with Ralf Sauer, Deputy Head of Unit DG JUST*, 2018, https://ec.europa.eu/info/events/citizens-dialogues/citizens-dialogue-graz-deputy-head-unit-dg-just-ralf-sauer-2018-mar-01_en.

102 About EDPB, https://edpb.europa.eu/about-edpb/about-edpb_en.

103 Mark Scott and Laurens Cerulus, *Meet Europe's New Chief Regulator of Data Privacy*, Politico, May 25, 2018, https://www.politico.eu/article/andrea-jelinek-gdpr-meet-europes-new-chief-regulator-of-data-privacy/.

104 Suzaane Vranica, *How the EU is implementing its new privacy rules*, Wall St. J., June 18, 2018, https://www.wsj.com/articles/how-the-eu-is-implementing-its-new-privacy-rules-1529342835.

105 Elaine Edwards, *All You Need to Know in the Max Schrems-Facebook Case*, Irish Times, Feb. 6, 2017, https://www.irishtimes.com/business/technology/all-you-need-to-know-in-the-max-schrems-facebook-case-1.2965482.

106 *Id.*

107 Ellen Nakashima, *Top E.U. Court Strikes down Major Data-Sharing Pact between U.S. and Europe*, Wash. Post, October 6, 2015, https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html.

108 *Lawyer Suing Facebook Overwhelmed with Support*, The Guardian (Aug. 6, 2014), https://www.theguardian.com/technology/2014/aug/06/facebook-privacy-action-austria-max-schrems. This amount of proposed damages is absurd, considering that Facebook's average revenue per user in Europe was USD $13.8 in 2014. *See Facebook's average revenue per user as of 4th quarter 2017, by region (in U.S. dollars)*, Statista, https://www.

believed to be the largest class action in Europe to date.[109] Austrian lower courts recognized Schrems' financial and media interest in pursuing the case and rejected it on jurisdictional and procedural grounds.[110] On two separate issues, the Austrian Supreme Court referred the case to the European Court of Justice, which ruled in January that Schrems would be allowed to proceed with the case, but that a class action was not appropriate. An appeal is pending.[111]

NOYB represents the culmination and professionalization of Schrems' effort to "confront tech giants like Facebook, Google & Co. with a team of highly qualified and motivated lawyers and IT experts on equal footing."[112] Not only is the organization positioned to serve those bringing class actions, it also serves data protection regulators, many of whom lack the training and funding to implement the GDPR.[113] NOYB's Kickstarter fundraising campaign raised €300,000 to fund operations, and its Silicon Valley-style business plan boasts that it will offer services such as group actions, collective complaints, mass mandates, abstract lawsuits, help finding favorable jurisdictions, funding of collective enforcement, a testing environment to see whether apps violate the GDPR, public relations and communications services with leading media and advocacy organizations, multilingual information, and "Statistics & Ranking to put pressure on companies and stir public debate."[114]

NOYB has several grievances about Google, Instagram, WhatsApp, and Facebook, including about their online consent processes and the use of data on platforms, but NOYB's underlying concern is market power. NOYB claims that these companies have been so successful that they have become essential for modern life. They say that denying access to these platforms constitutes a serious detriment to people who refuse to accept new privacy policies and terms of service, so consent is essentially coerced. NOYB therefore believes that these companies should be required to provide their services even to users who do not consent to the processing of their personal data (e.g., for targeted advertising), which would effectively compel firms to provide services without compensation. According to NOYB, any consent that these companies have acquired should be viewed as invalid because users had no real choice in the matter; their options were to either consent or be kicked off an essential service. NOYB also asserts that these companies hide consent within the terms of service, making consent to processing a less than fully informed choice.[115] NOYB thinks this is unfair and illegal under Recital 43 of the GDPR,[116] and that essentially any processing under these conditions amounts to "exploitation of personal data." NOYB also alleges that the platforms engage in unfair and deceptive practices to get users to consent to new terms. NOYB highlights "fake" notifications used to trick users into giving consent and requiring users to consent to new terms in order access a profile to delete it.[117] NOYB urges DPAs to find that all consent to new provisions under these conditions is invalid, and it offers additional arguments in case the regulator finds that this does not constitute forced—and therefore invalid—consent. Its list of other reasons to invalidate consent includes a finding that the terms were not specific enough to permit informed consent, and that the consent was not adequately distinguishable from the privacy policy and terms of service. NOYB does not discuss whether companies can or should have any compensation for providing services, which Facebook and similar companies currently receive through targeted advertising.

The idea that Facebook has a coercive level of market power and is an essential service is contradicted by European data. Sixty-five percent of European internet users access social media of some kind,[118] but Facebook's popularity across the EU varies by country, age, gender, device, and other metrics.[119] In any case, if the problem is one of market power, then antitrust is the solution, not data protection regulation. In essence, EU litigants make the same arguments as so-called "hipster" antitrust proponents in the

statista.com/statistics/251328/facebooks-average-revenue-per-user-by-region/.

109 *See* FBClaim, *CJEU Ruling on Facebook Action on Janurary 25, 2018: Class Action, Model Case or No Jurisdiction?*, http://www.europe-v-facebook.org/sk/PA_CJEU_en.pdf (last visited Oct. 2, 2018); Our Team, Members and Partners, noyb, https://noyb.eu/team/ (last visited Oct. 6, 2018).

110 Derek Scally, *Austrian Court Dismisses Schrems' Facebook Privacy Case*, Irish Times, July 1, 2015, https://www.irishtimes.com/business/technology/austrian-court-dismisses-schrems-facebook-privacy-case-1.2269365.

111 Secil Bilgic, *Schrems v. Facebook: CJEU Accepts Facebook User as Consumer but Disallows Class Action Under Special Jurisdiction Rule*, Jolt Digest, Feb. 5, 2018, https://jolt.law.harvard.edu/digest/schrems-v-facebook-cjeu-accepts-facebook-users-as-consumers-but-disallows-class-action-under-special-jurisdiction-rule.

112 Rebecca Hill, *Max Schrems Launches Privacy NGO, Wins €60k Within First 24 Hours*, The Register, Nov. 29, 2017, https://www.theregister.co.uk/2017/11/29/schrems_launches_privacy_enforcement_ngo_pulls_in_nearly_60k_in_first_24_hours/.

113 Douglas Busvine et al., *European Regulators: We're Not Ready for New Privacy Law*, Reuters (May 8, 2018), https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X.

114 Our Detailed Concept, noyb, https://noyb.eu/concept (last visited June 24, 2018).

115 *Noyb.Eu Filed Four Complaints*, *supra* note 1.

116 Recital 43 says:

> In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.
>
> Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

117 *Noyb.Eu Filed Four Complaints*, *supra* note 1.

118 *See Use of Internet Services*, *supra* note 58, at 5.

119 *Number of Facebook Users in Western Europe 2014-2018*, Statista, https://www.statista.com/statistics/283623/western-europe-number-of-facebook-users/ (accessed September 28, 2018).

U.S.[120]—that the evidentiary consumer welfare standard, long a transatlantic touchstone, should be abandoned in favor of the public interest, a German ordoliberal concept that the state should intervene in the market to produce a normative outcome.[121]

Other non-profits have filed major GDPR complaints, including France's LQDN with 19 complaints against "GAFAM" under the GDPR. LQDN's goal is to "reverse the great farce on which GAFAM has built their world: the 'consent' we would give them, so that they probe our spirit and influence our wishes, is worthless."[122] The group vows to take action in European courts—they say "we cannot leave it entirely in the hands of the CNIL," the French DPA—and expects its efforts to have global, not just European, consequences. LQDN argues that proper consent must be "freely" given, that it must be a positive act (i.e., there can be no pre-checked boxes indicating consent), and that it must be specific to different kinds of data processing. The complaints also argue that consent cannot be consideration for a contract to provide services. One of the LQDN's core arguments is that developing personalized user profiles for targeted advertising is not a legitimate interest of service providers like Facebook. According to LQDN, even if the contract makes clear that such a user profile will be developed for that purpose, processing data to support advertising is not necessary for the provision of services and is therefore illegal. Some of the complaints take issue with the passive nature of consent, where check boxes come pre-ticked or ad profiles are created without the user's explicit consent.[123] Additionally, LQDN has brought attention to French DPA rulings against two French startups, Teemo and Fidzup, for data protection violations.[124] This illustrates that the French DPA has no qualms about prosecuting startups,[125] a rebuke of the German policymaker's assurance that enforcement would focus on the big players.

C. Strengthening Bureaucracy

Albrecht argued that enforcement should prioritize the companies that have already been on regulators' radar. But if the regulators already know which companies are causing problems, why require every data processor that serves Europeans to comply with preventative regulations? It could be part of a "make-work" strategy to keep Europe's 29 DPAs in business and require firms to hire data protection officers—another GDPR requirement which is estimated to result in 75,000 new hires.[126] From the beginning of Schrems' lawsuits in 2011 to 2016, the Irish Data Protection Commission ballooned from 22 staff to 64, and its budget increased from $1.7 million to $5.6 million.[127] This illustrates how activist litigation can be a form of de facto policymaking. The regulatory authority had to hire more workers to satisfy the demands of the case. This approach to staffing is different from—and less democratically accountable than—the legislative body setting up the regulator, defining its budget and mandate, and enumerating specific tasks for it to accomplish.

Those seeking to expand the role of regulatory authorities implicitly assume that those authorities have more information and therefore know better than consumers how to order transactions in the marketplace.[128] This assumption is rarely warranted, but it is even less so where regulators do not have expertise in the area they regulate or resources to develop such expertise. The GDPR imposes massive new responsibilities on regulators without a concurrent increase in training, funding, and other resources. EU data supervisors wear many hats, including "ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer."[129] Furthermore, the GDPR widens the gap between the high expectations for data protection and the low level of skills possessed by data supervisors charged with its implementation.[130] There are certainly many talented individuals among these ranks, but the mastery of information and communications technology varies considerably among these professionals, especially as each nation's DPA is constituted differently.

The IAPP surveyed the complaints to the EU's DPAs from May 25-July 31, 2018 and compared it against the same period last year.[131] The volume, frequency, categorization, and length of complaints vary significantly across countries.[132] Whereas Sweden, Denmark, Slovakia, Belgium, and Estonia received only a handful of complaints, others had hundreds, including the

120 Elyse Dorsey, Jan Rybnicek, and Joshua D. Wright, *Hipster Antitrust Meets Public Choice Economics: The Consumer Welfare Standard, Rule of Law, and Rent-Seeking*, George Mason Law & Economics Research Paper No. 18-20, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3165192.

121 Jonathan Rubin and Christian Bergqvist, *Google and the Transatlantic Antitrust Abyss*, Global Comp'n Rev., July 13, 2018, https://globalcompetitionreview.com/article/usa/1171929/google-and-the-transatlantic-antitrust-abyss.

122 *GDPR: La Quadrature du Net Lodges Complaints Against GAFAM*, ArchyWorldys, May 30, 2018, https://www.archyworldys.com/rgpd-la-quadrature-du-net-lodges-complaints-against-gafam/.

123 *Attaquons les GAFAM et leur monde*, *supra* note 2.

124 *Teemo, Fidzup: French Privacy Watchdog Bans Rouge Geolocation, EU Considers Legalizing It*, LQDN, September 4, 2018, https://www.laquadrature.net/en/node/10611.

125 Allison Schiff, *Forget the Duopoly (For Now). It's The Little Guys Taking Heat on GDPR*, AdExchanger (Aug. 7, 2018), https://adexchanger.com/privacy/forget-the-duopoly-for-now-its-the-little-guys-taking-heat-on-gdpr/.

126 Rita Heimes and Sam Pfeifle, *Study: GDPR's Global Reach to Require at Least 75,000 DPO's Worldwide*, IAPP, https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.

127 Müge Fazlioglu, *Analyzing changes in DPA Income and Staff, from 2011 to 2016*, IAPP, Dec. 11, 2017, https://iapp.org/news/a/analyzing-changes-in-dpa-income-and-staff-2011-2016/.

128 *See generally* F.A. Hayek, Economics and Knowledge (1937); F.A. Hayek, The Use of Knowledge in Society (1945).

129 Colin J. Bennett and Charles Raab, The Governance of Privacy: Policy Instruments in Global Perspective (2006).

130 Charles D. Raab and Ivan Szekely, *Data Protection Authorities and Information Technology*, Computer L. & Sec. Rev. (forthcoming), https://ssrn.com/abstract=2994898.

131 *Cataloging GDPR Complaints since May 25*, IAPP, https://iapp.org/news/a/cataloguing-gdpr-complaints-since-may-25/ (accessed September 28, 2018).

132 Jennifer Baker, *What's a GDPR Complaint? No One Really Knows*, IAPP (Aug. 28, 2018), https://iapp.org/news/a/whats-the-definition-of-a-gdpr-complaint-spoiler-alert-no-one-knows/.

Czech Republic (400), France (426), Greece (113), Ireland (933), Netherlands (170), Poland (756), Romania (145), and Slovenia (102). A cursory review shows that the number of complaints is not commensurate with population. Germany, the EU's largest country by population, did not respond to the survey. The UK reports a doubling of complaints from the same period last year (1,124).[133] To manage the increased volume, the ICO requires that all UK data processors pay a significant fee to cover data protection costs, but now many government organizations are in arrears for the payment, including the National Health Service.[134]

Public choice theory suggests that the EU data supervisors' preferences are not necessarily aligned with the public interest.[135] Increasing user knowledge and the quality of data protection technology could make people better off overall, but it could also render data protection authorities less important. While data supervisors will not necessarily reject policies that improve user knowledge and technology design, it is in their interest to promote policies that increase their own resources and legitimacy in conducting compliance and adjudication. It is notable that the GDPR contains no discussion of efforts to improve user education and privacy enhancing behaviors, even though these activities are scientifically documented to improve trust in the online ecosystem.[136]

III. The GPDR's Unintended Consequences

In the months since the GDPR took effect, there have been reports of startups closing,[137] foreign news outlets pulling out of the EU,[138] the disruption of online ad markets,[139] and personal inboxes being flooded with compliance emails.[140] There are related and significant concerns about free speech, security threats, compliance costs, and innovation deterrence.

A. Blocked Data and Content

Since the GDPR went into effect, over 1,000 news sites have gone dark in the EU.[141] EU residents have been unable to access Tronc Media, whose flagship newspapers include the *Los Angeles Times*, the *Chicago Tribune*, *New York Daily News*, the *Hartford Courant* (America's longest running newspaper since 1764), the *Orlando Sentinel*, and the *Baltimore Sun*.[142] Nor can they access more than 60 newspapers of Lee Enterprises covering news across 20 U.S. states.[143] Blocked media is not only a problem for the one million Americans who live in the EU who can no longer read news and information about their hometowns, but for Europeans who wish to learn more about the U.S. from direct sources rather than the state-owned media, which dominate the press and broadcasting in most EU countries.

The GDPR has affected not just American media oulets, but also their advertisers. Given the scope of Google's advertising platform and its affiliates on syndicated networks, its compliance with the GDPR has caused ripple effects in ancillary markets. Independent ad exchanges noted prices plummeting 20 to 40 percent.[144] Some advertisers report being shut out from exchanges.[145] The GDPR's complex and arcane designations for "controllers" and "processors" can ensnare third party chip makers, component suppliers, and software vendors which have never interfaced with end users, as European courts have ruled that any part of the internet ecosystem can be liable for data breaches.[146]

Many American retailers, game companies, and service providers no longer operate in the EU. The websites of Williams-Sonoma and Pottery Barn are dark.[147] The websites of scores of other American retailers are now polluted with pop-ups and disclosures, prompting many customers to click away. The San Francisco-based Klout, an innovative online service that used social media analytics to rate its users according to online social influence, closed down completely.[148] Drawbridge, a San Mateo,

133 Ben Chapman, *Data Breach Complaints up 160% since GDPR Came into Force*, The Independent, August 24, 2018, https://www.independent.co.uk/news/business/news/data-breach-complaints-increase-gdpr-came-into-force-cybersecurity-a8506711.html.

134 *NHS Faces Regulatory Action over Unpaid Data Protection Fees*, IT PRO, September 26, 2018, http://itpro.co.uk/go/31994.

135 James C. Cooper and William E. Kovacic, *Behavioral Economics: Implications for Regulatory Behavior*, SSRN Scholarly Paper, July 21, 2011, https://papers.ssrn.com/abstract=1892078.

136 *See* Roslyn Layton, *How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust*, at 14 (Mar. 31, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944358.

137 Ivana Kottasová, *These Companies Are Getting Killed by GDPR*, CNN (May 11, 2018), http://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.

138 Los Angeles Times, Tronc (last visited June 25, 2018), http://www.tronc.com/gdpr/latimes.com/.

139 Jessica Davies, *'The Google Data Protection Regulation': GDPR is Strafing Ad Sellers*, Digiday (June 4, 2018), https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.

140 Alex Hern, *Most GDPR Emails Unnecessary and Some Illegal, Say Experts*, The Guardian (May 21, 2018), https://www.theguardian.com/technology/2018/may/21/gdpr-emails-mostly-unnecessary-and-in-some-cases-illegal-say-experts.

141 Jeff South, *More than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months after GDPR Took Effect*, Nieman Lab, August 7, 2018, http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

142 Alanna Petroff, *LA Times takes down website in Europe as privacy rules bite*, CNN Money, May 25, 2018, https://money.cnn.com/2018/05/25/media/gdpr-news-websites-la-times-tronc/index.html.

143 Renae Reints, *These Major U.S. News Sites Are Blocked in the EU*, Fortune, August 9, 2018, http://fortune.com/2018/08/09/news-sites-blocked-gdpr/.

144 Davies, *supra* note 139.

145 Catherine Armitage, *Life after GDPR: what next for the advertising industry?*, World Federation of Advertisers, July 10, 2018, https://www.wfanet.org/news-centre/life-after-gdpr-what-next-for-the-advertising-industry/.

146 Judgment of the Court (Grand Chamber), EU, June 5, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0210&qid=1531145885864&from=EN.

147 *Amid Confusion, EU Data Privacy Law Goes into Effect*, WTOP, May 25, 2018, https://wtop.com/news/2018/05/amid-confusion-eu-data-privacy-law-goes-into-effect/.

148 Jon Russel, *RIP Klout*, TechCrunch, May 2018, https://techcrunch.com/2018/05/10/rip-klout/.

California identity management company, exited the EU and sold off its ad tracking business on account of the GDPR.[149] Verve, a leading mobile marketing platform with offices in six U.S. cities, closed its European operation in advance of the GDPR, impacting 15 EU employees.[150] Valve, an award-winning video game company in Bellevue, Washington, shut down an entire game community rather than invest in GDPR compliance.[151] Uber Entertainment, also based in Washington, similarly shut down one of its most popular games entirely after a six year run because upgrading the platform to GDPR compliance was too expensive.[152] California-based Gravity Interactive no longer offers games in the EU and refunded its European customers.[153] The Las Vegas-based Brent Ozar Unlimited, which offers a range of information technology and software support services, stopped serving the EU.[154] San Francisco's Payver, the dashboard camera app that pays drivers to collect road information on potholes, fallen road signs, and other inputs to build maps to improve the safety of self-driving cars, no longer supports the EU.[155] Legal news website *Above the Law* describes the EU closures of Ragnarok Online, Unroll.me, SMNC, Tunngle, and Steel Root, noting that the GPDR is splintering the internet and that GDPR policymakers refused to listen to concerns from startups before the launch and now refuses to fix its problems.[156] Even the website of the Association of National Advertisers is not available in the EU.[157]

149 Allison Schiff, *Drawbridge Sells Its Media Arm And Exits Ad Tech*, AdExchanger, May 8, 2018, https://adexchanger.com/data-exchanges/drawbridge-sells-its-media-arm-and-exits-ad-tech/.

150 Ronan Shields. *Verve to focus on US growth as it plans closure of European offices ahead of GDPR*, The Drum, April 18, 2018, https://www.thedrum.com/news/2018/04/18/verve-focus-us-growth-it-plans-closure-european-offices-ahead-gdpr.

151 *Super Monday Night Combat*, Steam, https://steamcommunity.com/app/104700/allnews/.

152 Owen Good, *Super Monday Night Combat will close down, citing EU's new digital privacy law*, Polygon, April 28, 2018, https://www.polygon.com/2018/4/28/17295498/super-monday-night-combat-shutting-down-gdpr.

153 *Important Notice Regarding European Region Access*, Warportal, http://blog.warpportal.com/?p=10892.

154 *GDPR: Why We Stopped Selling Stuff to Europe*, Brent Ozar, December 18, 2017, https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/.

155 Getpayver, Twitter, April 5, 2018, https://twitter.com/getpayver/status/981992477392437249?lang=en ("Sorry European Payver users! Come May 24th we're discontinuing Payver support in Europe due to #GDPR. Talk to your lawmakers...").

156 Techdirt, *Companies Respond To The GDPR By Blocking All EU Users*, Above the Law, May 11, 2018, https://abovethelaw.com/legal-innovation-center/2018/05/11/companies-respond-to-the-gdpr-by-blocking-all-eu-users/.

157 George P. Slefo, *ANA Doesn't Have GDPR-Compliant Website; Says It Will Be up in 'Two Weeks*,' AdAge, June 7, 2018, https://adage.com/article/digital/ana-misses-deadline-create-gdpr-compliant-website/313775/.

B. Violation of U.S. Free Speech Laws and Norms

GDPR compliance is so costly and cumbersome that these entities self-censor rather than risk violating the GDPR. If the GDPR were adopted in the U.S., it would likely violate the First Amendment, as the requirements for data processing are so onerous that they would be found to limit expression. A related issue with the GDPR is the Right to be Forgotten (RTBF), the notion that information has a finite life and that after a certain period, the information's life is "spent" and can be deleted from the public domain. The EU asserts that the GDPR applies to data controllers anywhere in the world if they process a European citizen's data. Similarly, RTBF proponents such as France's CNIL attempt to force the global removal of public information in the name of data protection. For example, the French DPA has ordered Google to delete certain search results in France, and it believes that the company must therefore delete them for all countries' search engines. Google has appealed this holding to the European Court of Justice. The European Commission, Ireland, and Greece support the company in its appeal, arguing that RTBF stretches the meaning of data protection too far.[158]

Indeed, the GDPR's asserted jurisdiction outside the EU may itself be illegal—at least where the U.S. is concerned.[159] The GDPR is likely unenforceable under U.S. common law, which rejects foreign rulings when they are contrary to American policy.[160] The SPEECH Act, passed in 2010, supplies strong protections for First Amendment freedoms in the context of libel suits brought in foreign jurisdictions.[161]

C. Potentially Blocked Innovation

Many GDPR requirements are fundamentally incompatible with big data, artificial intelligence, blockchain, and machine learning, especially those that require data processors to disclose the purpose of data processing, minimize their use of data, and automate decision-making.[162] For technology developers, engineers, and entrepreneurs, the GDPR creates uncertainty not only in the text of the law and its adjudication, but in that requirements and tenets of the GDPR conflict with the operation of machine learning and artificial intelligence.[163]

Some of the most important recent scientific advances have been the result of processing various sets of information in inventive ways—ways that neither subjects nor controllers

158 *European Commission Sides with Google in RTBF Case*, IAPP, https://iapp.org/news/a/ec-sides-with-google-in-rtbf-case/ (accessed September 28, 2018).

159 Kurt Wimmer, *Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?*, 68 Syracuse L. Rev. 545 (2018), https://ssrn.com/abstract=3188974.

160 *Id.* at 571.

161 *Id.* at 572-73.

162 Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 Seton Hall L. Rev. 995 (2017), https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr.

163 Joel Thayer and Bijan Madhani, *Can a Machine Learn Under the GDPR?*, TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy, December 16, 2018, https://ssrn.com/abstract=3141854.

anticipated, let alone requested. Consider the definitive study on whether the use of mobile phones causes brain cancer.[164] The Danish Cancer Society analyzed 358,403 Danish mobile subscribers by processing social security numbers, mobile phone numbers, and the National Cancer Registry, which records every incidence of cancer by social security number.[165] The study, the most comprehensive investigation of its kind ever conducted, proves that the use of mobile phones is not correlated with brain cancer. But the users' information was not collected for the express purpose of such a study. Therefore, it's possible that, had the GDPR been in effect at the time of the study, consent from the population whose data was analyzed would not have been available, and the GDPR's purpose-specification requirement would have therefore made it impossible to conduct the study. Going forward, it's possible, if not likely, that valuable research will not be conducted because of the GDPR.

Indeed, part of the promise of socialized medicine was the ability to tap the vast pools of data in public health databases to make advances in medicine. However, a privacy panic is threatening to derail some projects,[166] including Iceland's genome warehouse, the oldest and most complete genetic record in the world, which promises groundbreaking therapies for Alzheimer's disease and breast cancer.[167] While many regulatory advocates focus attention on Silicon Valley firms and call for greater regulation, their campaign is backfiring as users turn their ire toward governments and demand erasure of their data from national health care records and other government services, potentially frustrating the operating models of mandated social programs.[168] With the mantra of "if in doubt, opt out," about half a million Australians rejected the country's national electronic health record, causing the computer system to crash in July 2018.[169]

For centuries, European state churches have collected and published information on births, deaths, weddings, baptisms, and more. In Denmark and Sweden, these institutions retain the official register for this information. Because of the GDPR, many churches have stopped printing announcements in the bulletins for their local congregations unless they obtain consent first.[170] GDPR risks have also been identified with respect to convicted felons successfully removing information about their crimes from search engines,[171] the exchange of business cards,[172] the taking of pictures in public,[173] and disclosures of health and injury information in the trade of soccer players.[174]

D. Security Concerns

A key unintended consequence of the GDPR is that it undermines the transparency of the international systems and architecture that organize the internet. The WHOIS query and response protocol for internet domain names, IP addresses, and autonomous systems is used by law enforcement, cybersecurity professionals and researchers, and trademark and intellectual property rights holders.[175] The Internet Corporation for Assigned Names and Numbers (ICANN) recently announced a Temporary Specification that allows registries and registrars to obscure WHOIS information they were previously required to make public, ostensibly in order to comply with the GDPR.[176] This could hinder efforts to combat unlawful activity online, including identity theft, cyber-attacks, online espionage, theft of intellectual property, fraud, unlawful sale of drugs, human trafficking, and other criminal behavior, and it is not even required by the GDPR.

The GDPR does not apply at all to non-personal information and states that disclosure of even personal information can be warranted for matters such as consumer protection, public

164 Patrizia Frei et al., *Use of Mobile Phones and Risk of Brain Tumours: Update of Danish Cohort Study*," BMJ, October 20, 2011, https://www.cancer.dk/dyn/resources/File/file/9/1859/1385432841/1_bmj_2011_pdf.pdf.

165 *Id.*

166 Daniel Castro and Alan McQuinn, *The Privacy Panic Cycle: A Guide to Public Fears About New Technologies*, Information Technology and Innovation Foundation, September 10, 2015, https://itif.org/events/2015/09/10/sky-not-falling-understanding-privacy-panic-cycle.

167 Jeremy Hsu, *Iceland's Giant Genome Project Points to Future of Medicine*, IEEE Spectrum, March 25, 2015, https://spectrum.ieee.org/the-human-os/biomedical/diagnostics/icelands-giant-genome-project-points-to-future-of-medicine.

168 Howell, *supra* note 10.

169 *Id.*

170 *Minister: Krav om GDPR-samtykke til kirkeblade er absurd*, Version2, September 11, 2018, https://www.version2.dk/artikel/minister-krav-gdpr-samtykke-kirkeblade-absurd-1086182; *Kirkeblade opgiver at bringe navne på døbte og døde*, B.T., August 3, 2018, https://www.bt.dk/content/item/1203799; Jens Peder Østergaard, *Konsekvens af EU-lov: Slut med at læse om døbte, gifte og døde*, Viborg Stifts Folkeblade, May 22, 2018, https://viborg-folkeblad.dk/rundtomviborg/Konsekvens-af-EU-lov-Slut-med-at-laese-om-doebte-gifte-og-doede/artikel/376140.

171 Daniel Castro, *The EU's Right to be Forgotten is Now Being Used to Protect Murderers*, Center for Data Innovation (Sep. 21, 2018), https://www.datainnovation.org/2018/09/the-eus-right-to-be-forgotten-is-now-being-used-to-protect-murderers/ ("According to the company (Google), almost one-fifth of the news articles it received requests to remove related to crime, and it removes roughly one-third of the right to be forgotten requests that it receives relating to news articles.").

172 Stephen White, *How Do Business Cards Sit with GDPR?*, GDPR.Report, February 8, 2018, https://gdpr.report/news/2018/02/08/business-cards-sit-gdpr/.

173 Kevin Sullivan, *What Photographers Need to Know About GDPR*, PDNPulse, June 12, 2018, https://pdnpulse.pdnonline.com/2018/06/gdpr-how-bad-is-it-for-photographers.html; Soraya Sahhaddi Nelson, *New EU Data Protection Law Could Affect People Who Take Pictures With Their Phones*, NPR, May 24, 2018, https://www.npr.org/2018/05/24/614195844/new-eu-data-protection-law-could-affect-people-who-take-pictures-with-their-phon?t=1538121870256.

174 Thomas Idskov, *Mundkurv! Derfor holdes omfanget af FCK-spillers skade hemmelig*, B.T., July 12, 2018, https://www.bt.dk/content/item/1197424.

175 Shane Tews, *How European data protection law is upending the Domain Name System*, AEI, Feb. 26, 2018, https://www.aei.org/publication/how-european-data-protection-law-is-upending-the-domain-name-system/.

176 Temporary Specification for gTLD Registration Data, ICANN (adopted May 17, 2018), https://www.icann.org/resources/pages/gtld-registration-data-specs-en.

safety, law enforcement, enforcement of rights, cybersecurity, and combating fraud. Moreover, the GDPR does not apply to domain names registered to U.S. registrants by American registrars and registries. Nor does it apply to domain name registrants that are companies, businesses, or other legal entities, rather than "natural persons." All the same, actors including ICANN are practicing voluntary censorship because the GDPR's provisions are so vague and the potential penalties so high. GDPR proponents have likely contributed to the impression that the GDPR urges measures like the Temporary Specification. For example, in her role in the Article 29 Working Party, the group that drove the promulgation of the GDPR, Jelinek said that the elimination and masking of WHOIS information is justified under the GDPR.[177]

The WHOIS problem can be described as the conflict between the individual's right to privacy and the public's right to know.[178] It can also be understood within the context of the problem of "privacy overreach,"[179] in which the drive to protect privacy becomes absolute, lacks balance with other rights, and unwittingly brings worse outcomes for privacy and data protection.[180] The situation harkens back to a key fallacy of privacy activists who attempted to block the rollout of caller ID because it violated the privacy rights of intrusive callers. Today, the receiver's right to know who is calling is prioritized over the caller's right to remain anonymous.[181] Similarly it is understood that the needs of public safety will supersede data protection, particularly in situations of danger to human life. Moreover, one should expect intellectual property to be in balance with data protection, not in conflict as it is under the GDPR. The pace of development of privacy and data protection law is significantly faster than that of other kinds of law, leading one scholar to suggest that it threatens to upend the balance with other fundamental rights.[182] This point is eloquently underscored by Richard Epstein in his critique of the idea of privacy rights established by the Warren Court. This Progressive theory assumes that it is "always easy, if not inevitable, to expand the set of rights without adverse social consequences," but never stops to consider that, when rights are expanded, correlative duties are imposed on others.[183]

E. Compliance Costs

To do business in the EU and comply with the GDPR, firms with 500 employees or more will likely have to spend between $1 and $10 million each.[184] With over 19,000 U.S. firms of this size,[185] total GDPR compliance costs for U.S. firms alone could reach $150 billion, twice what the U.S. spends on network investment[186] and one-third of annual e-commerce revenue in the U.S.[187] Economist Hosuk Lee-Makiyama calculates that the GDPR's requirements on cross-border trade flows will increase prices, amounting to a direct welfare loss of €260 per European citizen.[188] The net effect is that those companies that can afford to comply will do so, and the rest will exit. Hence the GDPR will become a barrier to market entry, punishing small firms, rewarding the largest players, and creating a codependent relationship between regulators and the firms they regulate. This is a perverse outcome for a regulation that promised to level the playing field on data protection.

IV. Conclusion

Many American policymakers have wisely recognized that the GDPR is not appropriate for the U.S. However, they are seeking to review and update existing information privacy laws to ensure consistency and effectiveness while avoiding fragmentation with state level rules.[189] The Trump administration has tasked the NTIA to develop—through public comment and scientific inquiry—a set of principles that will provide a high level of protection for individuals while giving organizations

177 Letter from Andrea Jelinek, Chairperson of Article 29 Data Protection Working Party, to Göran Marby, President of ICANN, April 11, 2018, https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf.

178 Shane Tews, *Privacy and Europe's data protection law: Problems and implications for the US*, AEI, May 8, 2018, http://www.aei.org/publication/privacy-and-europes-data-protection-law-problems-and-implications-for-the-us/.

179 *See* Justin "Gus" Hurwitz and Jamil N. Jaffer, *Modern Privacy Advocacy: An Approach at War with Privacy Itself?*, Regulatory Transparency Project White Paper, June 12, 2018, https://regproject.org/paper/modern-privacy-advocacy-approach-war-privacy/.

180 *See* Maja Brkan, *The Unstoppable Expansion of the EU Fundamental Right to Data Protection*, 23 Maastricht J. of Euro. & Comp. Law 812 (2016), http://journals.sagepub.com/doi/abs/10.1177/1023263X1602300505?journalCode=maaa.

181 *See* Hurwitz and Jaffer, *supra* note 179.

182 *See* Brkan, *supra* note 180.

183 Richard Epstein, *A Not Quite Contemporary View of Privacy*, 41 Harv. J. of Pub. Pol. 95 (2018), http://www.harvard-jlpp.com/wp-content/uploads/2018/01/EpsteinPanel_FINAL.pdf.

184 PricewaterhouseCoopers, *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey*, January 23, 2017, https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html.

185 U.S. Census Bureau, *2015 SUSB Annual Data Tables by Establishment Industry*, January 2018, https://www.census.gov/data/tables/2015/econ/susb/2015-susb-annual.html.

186 Jonathan Spalter, *Broadband CapEx Investment Looking Up in 2017*, USTelecom, July 25, 2018, https://www.ustelecom.org/blog/broadband-capex-investment-looking-2017.

187 U.S. Census Bureau, *Quarterly Retail E-Commerce Sales 1st Quarter 2018*, May 17, 2018, https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

188 Hosuk Lee-Makiyama, *The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs*, in Protection of Information and the Right to Privacy: A New Equilibrium? 85–94 (2014). This methodology is expanded in Erik Van der Marel et al., *A Methodology to Estimate the Costs of Data Regulations*, 146 Int'l Econ. 12 (2016).

189 Roslyn Layton, *Keys for a Consumer-Centric Approach to Online Privacy*, AEI (Sep. 26, 2018), http://www.aei.org/publication/keys-for-a-consumer-centric-approach-to-online-privacy/.

legal clarity and the flexibility to innovate.[190] These principles can inform bipartisan efforts for consumer online privacy legislation under consideration in Congress. The scientific research on data protection and privacy suggests that consumer education and privacy enhancing technologies are essential to creating trust online,[191] but these inputs are ignored in both the GDPR and the California Consumer Privacy Act.[192] Congress can foster the continued prosperity of the information economy by ensuring that consumers can access privacy education to make informed choices, that safe harbors for privacy-enhancing innovation protect the testing and learning of new technologies, and that common standards for competition and consumer protection online are equally guaranteed for all Americans and delivered by the FTC.[193]

This paper has reviewed perspectives on the GDPR, misconceptions about the policy, legal risks, and the GDPR's unintended consequences. The purpose of the GDPR is not to protect privacy, but rather to regulate data processing. In the past decade, the increasing data protection rules have not resulted in improved trust or increased cross-border commerce in the EU. The likelihood of selective enforcement of the GDPR, the empowerment of litigants to bring class action lawsuits, and the strengthening of the EU administrative state all suggest that the GDPR is more than the humanitarian effort it purports to be. The GDPR's unintended consequences include violations of the freedom of speech, closures of startups, blocked foreign news outlets, the disruption of online ad markets, the compromising of the WHOIS database, and the hampering of innovation. These are important realities which U.S. policymakers should consider as they evaluate whether and how to regulate online data in the U.S.

190 *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, National Telecommunications and Information Administration (Sep. 25, 2018), https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.

191 Roslyn Layton, *Statement before the Federal Trade Commission on Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, Market Solutions for Online Privacy*, AEI (Aug. 20, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf.

192 Cal. Civ. Code § 1798.100 et seq. Many compare this new state law to the GDPR because of its heavyhanded approach and potentially negative impact for enterprise. *See* Lothar Determan, *Analysis: California Consumer Privacy Act of 2018*, IAPP, July 2, 2018, https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

193 Specific recommendations can be found in Layton, *supra* note 191.